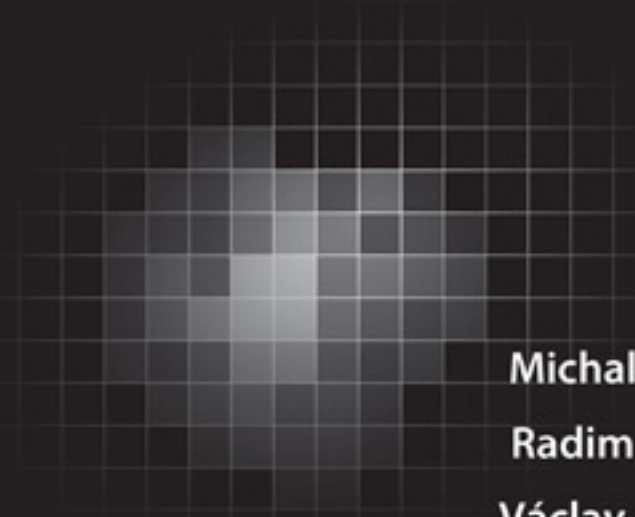




European ICT Law

10th edition



Michal Koščík

Radim Polčák

Václav Stupka

Matěj Myška

Pavel Loutocký

Libor Kyncl

European ICT Law Texts, Cases, Materials 10th edition

Michal Koščík

Radim Polčák

Václav Stupka

Matěj Myška

Pavel Loutocký

Libor Kyncl

This publication was created by the members of the Institute of Law and Technology (Faculty of Law, Masaryk University).

Graphic design of the cover Petr Šavelka

Contents – summary

I.	E-Commerce and Consumer protection.....	9
II.	Competition Law	65
III.	Law of domain names	70
IV.	Public Sector Information	106
V.	ISP Liability	118
VI.	Cybercrime and Cybersecurity.....	130
VII.	Copyright Law	166
VIII.	Electronic documents.....	206
IX.	Data protection.....	229
X.	E-Finance.....	329
XI.	Jurisdiction	389

Contents

Contents – summary	3
I. E-Commerce and Consumer protection	9
Treaty on the functioning of the European Union (relevant provisions)	9
Principles	9
Free Movement of Goods	10
Free Movement of Persons, Services and Capital	11
Consumer Protection	12
Relevant Case-Law on free movement of goods and services (on-line or via telecommunication)	13
C-322/01, Deutscher Apothekerverband eV and 0800 DocMorris NV,	13
C-243/01 Criminal proceedings against Piergiorgio Gambelli and Others	13
C-42/07 Liga Portuguesa de Futebol Profissional and Bwin International Ltd, formerly Baw International Ltd v Departamento de Jogos da Santa Casa da Misericórdia de Lisboa	13
C-156/13, Digibet Ltd, Gert Albers v Westdeutsche Lotterie GmbH & Co. OHG,	14
C-475/12 - UPC DTH	14
Directive 2011/83/EU of the European parliament and of the Council of 25 October 2011 on consumer rights	15
Directive 2013/11/EU of the European parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR)	31
Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts	41
Relevant case law on unfair terms in consumer contracts	44
C-243/08, Pannon GSM Zrt. v Erzsébet Sustikné Gyórfi,	44
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)	45
Relevant Case Law on Directive 2000/31/EC on electronic commerce	54
C-244/06, Dynamic Medien Vertriebs GmbH v Avides Media AG, THE COURT (Third Chamber),	54
C-298/07, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v deutsche internet versicherung AG,	54
C-509/09 and C-161/10 (Joined Cases) eDate Advertising GmbH v X, Olivier Martinez, Robert Martinez v MGN Limited	54
C-292/10, G v Cornelius de Visser,	54
C-291/13 Sotiris Papasavvas v O Fileleftheros Dimosia Etaireia Ltd, Takis Kounnafi, Giorgos Sertis	55
C-322/01 - Deutscher Apothekerverband	55
C-244/06 - Dynamic Medien	55
C-275/06 – Promusicae	55
C-298/07 - Deutsche internet versicherung	55
Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market ("Unfair Commercial Practices Directive")	55
Relevant Case Law on Unfair Commercial Practices Directive	63
C-122/10, Konsumentombudsmannen v Ving Sverige AB,	63
II. Competition Law	65
Treaty on the Functioning of the European Union (101 – 109)	65
Relevant case-law to the Treaty on the Functioning of the EU Art 101-102	66
C-418/01 IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG	66

T-201/04 Microsoft Corp. v Commission of the European Communities	67
C-52/07- Kanal 5 Ltd and TV 4 AB v Föreningen Svenska Tonsättares Internationella Musikbyrå (STIM) upa.....	67
C-425/07 P AEPI Elliniki Etaireia pros Prostatian tis Pnevmatikis Idioktiasias AE v Commission of the European Communities	68
COMP/39.530 Summary of Commission Decision - Microsoft - Webbrowser	68
III. Law of domain names	70
Uniform Domain Name Dispute Resolution Policy	70
Rules for Uniform Domain Name Dispute Resolution Policy.....	72
Uniform Domain Name Resolution Policy – Relevant Case Law	76
America Online, Inc. v. Johuathan Investments, Inc., and AOLNEWS.COM Case No. D 2001-0918.....	76
Wal-Mart Stores, Inc. v. Richard MacLeod d/b/a For Sale Case No. D2000-0662	79
Dr. Michael Crichton v. In Stealth Mode Case No: D2002-0874	82
Uniform Rapid Suspension System ("URS") Rules	84
Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trade marks	87
Regulation (EC) No 733/2002 of the European Parliament and of the council of 22 April 2002 on the implementation of the .eu Top Level Domain	93
Relevant case law on Regulation no. 733/2002 - on the implementation of the .eu Top Level Domain	96
C-483/07 P - Galileo Lebensmittel v Commission	96
C-569/08 - Internetportal und Marketing.....	98
C-376/11 - Pie Optiek	98
Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration	99
IV. Public Sector Information	106
Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.....	106
Relevant Case Law on Public Sector Information	111
C-343/95, Diego Cali & Figli Srl v. Servizi Ecologici Porto di Genova SpA (SEPG)	111
C-7/13, Creditinfo Lánstraust hf. and Registers Iceland and the Icelandic State	112
C-117/13, Technische Universität Darmstadt v Eugen Ulmer KG.....	114
V. ISP Liability	118
Convention on Information and Legal Co-operation concerning "Information Society Services"	118
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'	120
Relevant Case law concerning Directive 2000/31/EC	121
C-324/09, L'Oréal SA and others v. eBay International AG and others	121
C-314/12 UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH.....	125
Case of Delfi AS v. Estonia (ECHR Application No. 64569/09, Grand Chamber)	126
C-291/13 Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis.....	129
*Text contained in relevant case law to Directive 2000/31/EC on Electronic commerce	129
VI. Cybercrime and Cybersecurity	130
Convention on Cybercrime	130
Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems	140
For further interpretation see - Convention on Cybercrime – Explanatory report.....	142
98/560/EC: Council Recommendation on the development of the competitiveness of the European audiovisual and information services industry.....	142

Regulation (EC) No 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency	146
Directive 2013/40/EU of 12 August 2013 on attacks against information systems	153
See also: 158	
2013/0027 (COD) Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union	158
Explanatory Memorandum - Directive concerning measures to ensure a high common level of network and information security across the Union	158
Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace	159
VII. Copyright Law	166
Berne Convention for the Protection of Literary and Artistic Works	166
Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations	170
WIPO Copyright Treaty	174
WIPO Performances and Phonograms Treaty	176
Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society	178
Relevant Case-Law on Directive 2001/29/EC	185
C-5/08 Infopaq International	185
C-467/08 Padawan	185
C-462/09 Stichting de Thuiskopie	185
C-135/10 SCF ("Del Corso")	186
C-145/10 Painer	186
C-277/10 Luksan	186
C-360/10 SABAM	187
C-607/11 ITV Broadcasting and Others	187
C-351/12 OSA	187
C-355/12 Nintendo and Others	187
C-435/12 ACI Adam BV and Others	188
C-463/12 Copydan Båndkopi	188
C-466/12 Svensson and Others	188
C-117/13 Eugen Ulmer ("TU Darmstadt")	188
C-201/13 Deckmyn and Vrijheidsfonds	189
C-279/13 C More Entertainment	189
C-360/13 Public Relations Consultants Association ("Meltwater")	189
C-419/13 Art & Allposters International	189
C-516/13 Dimensione Direct Sales and Labianca	189
Directive 2009/24/EC on the legal protection of computer programs	189
Relevant Case-Law on Directive 2009/24/EC	192
C-393/09 Bezpečnostní softwarová asociace	192
C-406/10 SAS Institute	192
C-128/11 UsedSoft	192
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases ..	192
Relevant Case-Law on Directive 96/9/EC	197
C-203/02 The British Horseracing Board Ltd and Others	197
C-444/02 Fixtures Marketing ("OPAP")	197

C-338/02 Fixtures Marketing (“Svenska Spel AB”).....	197
C-304/07 Directmedia Publishing	198
C-545/07 Apis-Hristovich	198
C-604/10 Football Dataco and Others	198
C-202/12 Innoweb	198
C-30/14 Ryanair.....	198
Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights.....	199
Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version).....	202
VIII. Electronic documents	206
Directive 1999/93/EC of the European Parliament and of the council of 13 December 1999 on a Community framework for electronic signatures	206
Regulation (EU) No 910/2014 Of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	211
IX. Data protection	229
Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14.....	229
Charter of Fundamental Rights of the European Union (2007/C 303/01)	230
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	231
Relevant Case-Law on Convention for the Protection of Human Rights and Fundamental Freedoms	234
• CASE OF KLASS AND OTHERS v. GERMANY (Application no. 5029/71) 6 September 1978.....	234
• CASE OF MALONE v. THE UNITED KINGDOM (Application no. 8691/79) 2 August 1984.....	234
• CASE OF NIEMIETZ v. GERMANY (Application no. 13710/88) 16 December 1992	234
• CASE OF ROTARU v. ROMANIA (Application no. 28341/95) 4 May 2000	234
• COPLAND v. THE UNITED KINGDOM (Application no. 62617/00) 3 April 2007	234
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data	235
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	247
Relevant Case Law on the Directives 95/46/EC; 2002/58/EC	257
C-101/01 Criminal proceedings against Bodil Lindqvist).....	257
C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU	258
C-557/07 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH vTele2 Telecommunication GmbH.....	258
C-461/10 Bonnier Audio AB et al. v Perfect Communication Sweden AB	258
Joined Cases C-293/12 and C-594/12, (Digital Rights Ireland Ltd, Kämtner Landesregierung)	259
C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González.....	259
C-212/13, František Ryneš v Úřad pro ochranu osobních údajů,	260
Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	261
Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA	306
X. E-Finance	329
Treaty on the Functioning of the European Union (relevant provisions connected with E-Finance).....	329

Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services (“DMFS” Directive)	330
Relevant Case Law on Durable Medium and Information Providing in e-Finance	335
E-4/09 Inconsult Anstalt vs the Financial Market Authority (Finanzmarktaufsicht, Liechtenstein)	336
Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (“PSD2” Directive).....	340
Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (“PAD” Directive).....	358
Relevant Case-Law on Payments and Payment Frauds.....	366
C-616/11 T-Mobile Austria	366
C-494/12 Dixons Retail plc v Commissioners for Her Majesty’s Revenue and Customs	367
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE COMP/34.579 — MasterCard, Case COMP/36.518 — EuroCommerce, Case COMP/38.580 — Commercial Cards	367
Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (4 th Anti-Money Laundering = “4AML” Directive)	369
Relevant Case-Law on Anti-Money Laundering.....	383
Joined cases C-478/11 P to C-482/11 P – Laurent Gbagbo (C-478/11 P), Katinan Justin Koné (C-479/11 P), Akissi Danièle Boni-Claverie (C-480/11 P), Alcide Djédjé (C-481/11 P) and Affi Pascal N’Guessan (C-482/11 P) v Council of the European Union	383
C- 212/11, Jyske Bank Gibraltar Ltd v Administración del Estado.....	388
Relevant EU Regulations on EU Supervisory Authorities	388
XI. Jurisdiction	389
Regulation (EU) No 1215/2012 European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast).....	389
(16) OJ L 174, 27.6.2001, p. 25.	400
Relevant Case Law on the repealed council Regulation no 44/2001	401
C-478/12 Maletic.....	401
Joined Cases C-509/09 and C-161/10 eDate Advertising GmbH v X, Olivier Martinez, Robert Martinez v MGN Limited	401
Joined Cases C-585/08 and C-144/09, Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09),.....	401
C-523/10, Wintersteiger AG v Products 4U Sondermaschinenbau GmbH,	402
C-170/12, Peter Pinckney v KDG Mediatech AG,	402
C-190/11, Daniela Mühlleitner v Ahmad Yusufi, Wadat Yusufi,	402
Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).....	403
Regulation (EC) No 864/2007 of the European parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II).....	410

I.E-Commerce and Consumer protection

Treaty on the functioning of the European Union (relevant provisions)

Principles **Article 1**

1. This Treaty organises the functioning of the Union and determines the areas of, delimitation of, and arrangements for exercising its competences.
2. This Treaty and the Treaty on European Union constitute the Treaties on which the Union is founded. These two Treaties, which have the same legal value, shall be referred to as "the Treaties".

TITLE I **CATEGORIES AND AREAS OF UNION COMPETENCE**

Article 2

1. When the Treaties confer on the Union exclusive competence in a specific area, only the Union may legislate and adopt legally binding acts, the Member States being able to do so themselves only if so empowered by the Union or for the implementation of Union acts.
2. When the Treaties confer on the Union a competence shared with the Member States in a specific area, the Union and the Member States may legislate and adopt legally binding acts in that area. The Member States shall exercise their competence to the extent that the Union has not exercised its competence. The Member States shall again exercise their competence to the extent that the Union has decided to cease exercising its competence.
3. The Member States shall coordinate their economic and employment policies within arrangements as determined by this Treaty, which the Union shall have competence to provide.
4. The Union shall have competence, in accordance with the provisions of the Treaty on European Union, to define and implement a common foreign and security policy, including the progressive framing of a common defence policy.
5. In certain areas and under the conditions laid down in the Treaties, the Union shall have competence to carry out actions to support, coordinate or supplement the actions of the Member States, without thereby superseding their competence in these areas.
Legally binding acts of the Union adopted on the basis of the provisions of the Treaties relating to these areas shall not entail harmonisation of Member States' laws or Regulations.
6. The scope of and arrangements for exercising the Union's competences shall be determined by the provisions of the Treaties relating to each area.

Article 3

1. The Union shall have exclusive competence in the following areas:
 - (a) customs union;
 - (b) the establishing of the competition rules necessary for the functioning of the internal market;
 - (c) monetary policy for the Member States whose currency is the euro;

- (d) the conservation of marine biological resources under the common fisheries policy;
- (e) common commercial policy.

2. The Union shall also have exclusive competence for the conclusion of an international agreement when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope.

Article 4

1. The Union shall share competence with the Member States where the Treaties confer on it a competence which does not relate to the areas referred to in Articles 3 and 6.
2. Shared competence between the Union and the Member States applies in the following principal areas:

- (a) internal market;
- (b) social policy, for the aspects defined in this Treaty;
- (c) economic, social and territorial cohesion;
- (d) agriculture and fisheries, excluding the conservation of marine biological resources;
- (e) environment;
- (f) consumer protection;
- (g) transport;
- (h) trans-European networks;
- (i) energy;
- (j) area of freedom, security and justice;
- (k) common safety concerns in public health matters, for the aspects defined in this Treaty.

3. In the areas of research, technological development and space, the Union shall have competence to carry out activities, in particular to define and implement programmes; however, the exercise of that competence shall not result in Member States being prevented from exercising theirs.
4. In the areas of development cooperation and humanitarian aid, the Union shall have competence to carry out activities and conduct a common policy; however, the exercise of that competence shall not result in Member States being prevented from exercising theirs.

Article 5

1. The Member States shall coordinate their economic policies within the Union. To this end, the Council shall adopt measures, in particular broad guidelines for these policies. Specific provisions shall apply to those Member States whose currency is the euro.

2. The Union shall take measures to ensure coordination of the employment policies of the Member States, in particular by defining guidelines for these policies.

3. The Union may take initiatives to ensure coordination of Member States' social policies.

Article 6

The Union shall have competence to carry out actions to support, coordinate or supplement the actions of the Member States. The areas of such action shall, at European level, be:

- (a) protection and improvement of human health;
- (b) industry;
- (c) culture;
- (d) tourism;
- (e) education, vocational training, youth and sport;
- (f) civil protection;
- (g) administrative cooperation.

TITLE II PROVISIONS HAVING GENERAL APPLICATION

Article 7

The Union shall ensure consistency between its policies and activities, taking all of its objectives into account and in accordance with the principle of conferral of powers.

Article 8

In all its activities, the Union shall aim to eliminate inequalities, and to promote equality, between men and women.

Article 9

In defining and implementing its policies and activities, the Union shall take into account requirements linked to the promotion of a high level of employment, the guarantee of adequate social protection, the fight against social exclusion, and a high level of education, training and protection of human health.

Article 10

In defining and implementing its policies and activities, the Union shall aim to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.

Article 11

Environmental protection requirements must be integrated into the definition and implementation of the Union's policies and activities, in particular with a view to promoting sustainable development.

Article 12

Consumer protection requirements shall be taken into account in defining and implementing other Union policies and activities.

Article 13

In formulating and implementing the Union's agriculture, fisheries, transport, internal market, research and technological development and space policies, the Union and the Member States shall, since animals are sentient beings, pay full regard to the welfare requirements of animals, while respecting the legislative or administrative provisions and customs of the Member States relating in particular to religious rites, cultural traditions and regional heritage.

Article 14

Without prejudice to Article 4 of the Treaty on European Union or to Articles 93, 106 and 107 of this Treaty, and given the place occupied by services of general economic interest in the shared values of the Union as well as their role in promoting social and territorial cohesion, the Union and the Member States, each within their respective powers and within the scope of application of the Treaties, shall take care that such services operate on the basis of principles and conditions, particularly economic and financial conditions, which enable them to fulfil their missions. The European Parliament and the Council, acting by means of Regulations in accordance with the ordinary legislative procedure, shall establish these principles and set these conditions without prejudice to the competence of

Member States, in compliance with the Treaties, to provide, to commission and to fund such services.

Article 15

1. In order to promote good governance and ensure the participation of civil society, the Union's institutions, bodies, offices and agencies shall conduct their work as openly as possible.

2. The European Parliament shall meet in public, as shall the Council when considering and voting on a draft legislative act.

3. Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, shall have a right of access to documents of the Union's institutions, bodies, offices and agencies, whatever their medium, subject to the principles and the conditions to be defined in accordance with this paragraph.

General principles and limits on grounds of public or private interest governing this right of access to documents shall be determined by the European Parliament and the Council, by means of Regulations, acting in accordance with the ordinary legislative procedure.

Each institution, body, office or agency shall ensure that its proceedings are transparent and shall elaborate in its own Rules of Procedure specific provisions regarding access to its documents, in accordance with the Regulations referred to in the second subparagraph.

The Court of Justice of the European Union, the European Central Bank and the European Investment Bank shall be subject to this paragraph only when exercising their administrative tasks.

The European Parliament and the Council shall ensure publication of the documents relating to the legislative procedures under the terms laid down by the Regulations referred to in the second subparagraph.

Article 16

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Article 17

1. The Union respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States.

2. The Union equally respects the status under national law of philosophical and non-confessional organisations.

3. Recognising their identity and their specific contribution, the Union shall maintain an open, transparent and regular dialogue with these churches and organisations.

Free Movement of Goods

Article 28

1. The Union shall comprise a customs union which shall cover all trade in goods and which shall involve the prohibition between Member States of customs duties on imports and exports and of all charges having equivalent effect, and the adoption of a common customs tariff in their relations with third countries. In Member States and to products coming from third countries which are in free circulation in Member States.

Article 29

Products coming from a third country shall be considered to be in free circulation in a Member State if the import formalities have been complied with and any customs duties or charges having equivalent effect which are payable have been levied in that Member State, and if they have not benefited from a total or partial drawback of such duties or charges.

CHAPTER 1 THE CUSTOMS UNION

Article 30

Customs duties on imports and exports and charges having equivalent effect shall be prohibited between Member States. This prohibition shall also apply to customs duties of a fiscal nature.

Article 31

Common Customs Tariff duties shall be fixed by the Council on a proposal from the Commission.

Article 32

In carrying out the tasks entrusted to it under this Chapter the Commission shall be guided by:

- (a) the need to promote trade between Member States and third countries;
- (b) developments in conditions of competition within the Union in so far as they lead to an improvement in the competitive capacity of undertakings;
- (c) the requirements of the Union as regards the supply of raw materials and semi-finished goods; in this connection the Commission shall take care to avoid distorting conditions of competition between Member States in respect of finished goods;
- (d) the need to avoid serious disturbances in the economies of Member States and to ensure rational development of production and an expansion of consumption within the Union.

CHAPTER 2 CUSTOMS COOPERATION

Article 33

Within the scope of application of the Treaties, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall take measures in order to strengthen customs cooperation between Member States and between the latter and the Commission.

CHAPTER 3 PROHIBITION OF QUANTITATIVE RESTRICTIONS BETWEEN MEMBER STATES

Article 34

Quantitative restrictions on imports and all measures having equivalent effect shall be prohibited between Member States.

Article 35

Quantitative restrictions on exports, and all measures having equivalent effect, shall be prohibited between Member States.

Article 36

The provisions of Articles 34 and 35 shall not preclude prohibitions or restrictions on imports, exports or goods in transit justified on grounds of public morality, public policy or public security; the protection of health and life of humans, animals or plants; the protection of national treasures possessing artistic, historic or archaeological value; or the protection of industrial and commercial property. Such prohibitions or restrictions shall not, however, constitute a means of arbitrary discrimination or a disguised restriction on trade between Member States.

Article 37

1. Member States shall adjust any State monopolies of a commercial character so as to ensure that no discrimination

regarding the conditions under which goods are procured and marketed exists between nationals of Member States.

fact, either directly or indirectly supervises, determines or appreciably influences imports or exports between Member States. These provisions shall likewise apply to monopolies delegated by the State to others.

2. Member States shall refrain from introducing any new measure which is contrary to the principles laid down in paragraph 1 or which restricts the scope of the articles dealing with the prohibition of customs duties and quantitative restrictions between Member States.

3. If a State monopoly of a commercial character has rules which are designed to make it easier to dispose of agricultural products or obtain for them the best return, steps should be taken in applying the rules contained in this Article to ensure equivalent safeguards for the employment and standard of living of the producers concerned.

Free Movement of Persons, Services and Capital

CHAPTER 2 RIGHT OF ESTABLISHMENT

Article 49

Within the framework of the provisions set out below, restrictions on the freedom of establishment of nationals of a Member State in the territory of another Member State shall be prohibited. Such prohibition shall also apply to restrictions on the setting-up of agencies, branches or subsidiaries by nationals of any Member State established in the territory of any Member State.

Freedom of establishment shall include the right to take up and pursue activities as self-employed persons and to set up and manage undertakings, in particular companies or firms within the meaning of the second paragraph of Article 54, under the conditions laid down for its own nationals by the law of the country where such establishment is effected, subject to the provisions of the Chapter relating to capital.

Article 50

1. In order to attain freedom of establishment as regards a particular activity, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, shall act by means of Directive.

2. The European Parliament, the Council and the Commission shall carry out the duties devolving upon them under the preceding provisions, in particular:

- (a) by according, as a general rule, priority treatment to activities where freedom of establishment makes a particularly valuable contribution to the development of production and trade;
- (b) by ensuring close cooperation between the competent authorities in the Member States in order to ascertain the particular situation within the Union of the various activities concerned;
- (c) by abolishing those administrative procedures and practices, whether resulting from national legislation or from agreements previously concluded between Member States, the maintenance of which would form an obstacle to freedom of establishment;
- (d) by ensuring that workers of one Member State employed in the territory of another Member State may remain in that territory for the purpose of taking up activities therein as self-employed persons, where they satisfy the conditions which they would be required to satisfy if they were entering that State at the time when they intended to take up such activities;
- (e) by enabling a national of one Member State to acquire and use land and buildings situated in the territory of another Member State, in so far as this does not conflict with the principles laid down in Article 39(2);
- (f) by effecting the progressive abolition of restrictions on freedom of establishment in every branch of activity under consideration, both as regards the conditions for setting up

agencies, branches or subsidiaries in the territory of a Member State and as regards the subsidiaries in the territory of a Member State and as regards the conditions governing the entry of personnel belonging to the main establishment into managerial or supervisory posts in such agencies, branches or subsidiaries;

(g) by coordinating to the necessary extent the safeguards which, for the protection of the interests of members and others, are required by Member States of companies or firms within the meaning of the second paragraph of Article 54 with a view to making such safeguards equivalent throughout the Union;

(h) by satisfying themselves that the conditions of establishment are not distorted by aids granted by Member States.

Article 51

The provisions of this Chapter shall not apply, so far as any given Member State is concerned, to activities which in that State are connected, even occasionally, with the exercise of official authority. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may rule that the provisions of this Chapter shall not apply to certain activities.

Article 52

1. The provisions of this Chapter and measures taken in pursuance thereof shall not prejudice the applicability of provisions laid down by law, Regulation or administrative action providing for special treatment for foreign nationals on grounds of public policy, public security or public health.

2. The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure, issue Directives for the coordination of the abovementioned provisions.

Article 53

1. In order to make it easier for persons to take up and pursue activities as self-employed persons, the European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure, issue Directives for the mutual recognition of diplomas, certificates and other evidence of formal qualifications and for the coordination of the provisions laid down by law, Regulation or administrative action in Member States concerning the taking-up and pursuit of activities as self-employed persons.

2. In the case of the medical and allied and pharmaceutical professions, the progressive abolition of restrictions shall be dependent upon coordination of the conditions for their exercise in the various Member States.

Article 54

Companies or firms formed in accordance with the law of a Member State and having their registered office, central administration or principal place of business within the Union shall, for the purposes of this Chapter, be treated in the same way as natural persons who are nationals of Member States. 'Companies or firms' means companies or firms constituted under civil or commercial law, including cooperative societies, and other legal persons governed by public or private law, save for those which are non-profit-making.

Article 55

Member States shall accord nationals of the other Member States the same treatment as their own nationals as regards participation in the capital of companies or firms within the meaning of Article 54, without prejudice to the application of the other provisions of the Treaties.

CHAPTER 3 SERVICES

Article 56

Within the framework of the provisions set out below, restrictions on freedom to provide services within the Union

shall be prohibited in respect of nationals of Member States who are established in a Member State other than that of the person for whom the services are intended.

The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may extend the provisions of the Chapter to nationals of a third country who provide services and who are established within the Union.

Article 57

Services shall be considered to be 'services' within the meaning of the Treaties where they are normally provided for remuneration, in so far as they are not governed by the provisions relating to freedom of movement for goods, capital and persons.

'Services' shall in particular include:

(a) activities of an industrial character;

(b) activities of a commercial character;

(c) activities of craftsmen;

(d) activities of the professions.

Without prejudice to the provisions of the Chapter relating to the right of establishment, the person providing a service may, in order to do so, temporarily pursue his activity in the Member State where the service is provided, under the same conditions as are imposed by that State on its own nationals.

Article 58

1. Freedom to provide services in the field of transport shall be governed by the provisions of the Title relating to transport.

2. The liberalisation of banking and insurance services connected with movements of capital shall be effected in step with the liberalisation of movement of capital.

Article 59

1. In order to achieve the liberalisation of a specific service, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, shall issue Directives.

2. As regards the Directives referred to in paragraph 1, priority shall as a general rule be given to those services which directly affect production costs or the liberalisation of which helps to promote trade in goods.

Article 60

The Member States shall endeavour to undertake the liberalisation of services beyond the extent required by the Directives issued pursuant to Article 59(1), if their general economic situation and the situation of the economic sector concerned so permit.

To this end, the Commission shall make recommendations to the Member States concerned.

Article 61

As long as restrictions on freedom to provide services have not been abolished, each Member State shall apply such restrictions without distinction on grounds of nationality or residence to all persons providing services within the meaning of the first paragraph of Article 56.

Article 62

The provisions of Articles 51 to 54 shall apply to the matters covered by this Chapter.

Consumer Protection

Article 169

1. In order to promote the interests of consumers and to ensure a high level of consumer protection, the Union shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests.

2. The Union shall contribute to the attainment of the objectives referred to in paragraph 1 through:

(a) measures adopted pursuant to Article 114 in the context of the completion of the internal market;

(b) measures which support, supplement and monitor the policy pursued by the Member States.

3. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure and after

consulting the Economic and Social Committee, shall adopt the measures referred to in paragraph 2(b).

4. Measures adopted pursuant to paragraph 3 shall not prevent any Member State from maintaining or introducing more stringent protective measures. Such measures must be compatible with the Treaties. The Commission shall be notified of them.

Relevant Case-Law on free movement of goods and services (on-line or via telecommunication)

C-322/01, Deutscher Apothekerverband eV and 0800 DocMorris NV,

Ruling:

1 (a) A national prohibition on the sale by mail order of medicinal products the sale of which is restricted to pharmacies in the Member State concerned, such as the prohibition laid down in Paragraph 43(1) of the Arzneimittelgesetz (Law on medicinal products) in the version of 7 September 1998, is a measure having an effect equivalent to a quantitative restriction for the purposes of Article 28 EC.

(b) Article 30 EC may be relied on to justify a national prohibition on the sale by mail order of medicinal products which may be sold only in pharmacies in the Member State concerned in so far as the prohibition covers medicinal products subject to prescription. However, Article 30 EC cannot be relied on to justify an absolute prohibition on the sale by mail order of medicinal products which are not subject to prescription in the Member State concerned.

(c) Questions 1(a) and 1(b) do not need to be assessed differently where medicinal products are imported into a Member State in which they are authorised, having been previously obtained by a pharmacy in another Member State from a wholesaler in the importing Member State.

2. Article 88(1) of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use precludes a national prohibition on advertising the sale by mail order of medicinal products which may be supplied only in pharmacies in the Member State concerned, such as the prohibition laid down in Paragraph 8(1) of the Heilmittelwerbegesetz (Law on the advertising of medicinal products), in so far as the prohibition covers medicinal products which are not subject to prescription.

C-243/01 Criminal proceedings against Piergiorgio Gambelli and Others

Ruling

National legislation which prohibits on pain of criminal penalties the pursuit of the activities of collecting, taking, booking and forwarding offers of bets, in particular bets on sporting events, without a licence or authorisation from the Member State concerned constitutes a restriction on the freedom of establishment and the freedom to provide services provided for in Articles 43 and 49 EC respectively. It is for the national court to determine whether such legislation, taking account of the detailed rules for its application, actually serves the aims which might justify it, and whether the restrictions it imposes are disproportionate in the light of those objectives.

C-42/07 Liga Portuguesa de Futebol Profissional and Bwin International Ltd, formerly Baw International Ltd v Departamento de Jogos da Santa Casa da Misericórdia de Lisboa

Summary of the Judgment

1. Freedom to provide services – Provisions of the Treaty – Scope

(Arts 49 EC and 56 EC)

2. Freedom to provide services – Restrictions

(Art. 49 EC)

1. Any restrictive effects which the legislation of a Member State, which prohibits operators established in other Member States in which they lawfully provide similar services from offering games of chance via the internet within the territory of that Member State, might have on the free movement of capital and payments would be no more than the inevitable consequence of any restrictions on the freedom to provide services. Where a national measure relates to several fundamental freedoms at the same time, the Court will in principle examine the measure in relation to only one of those freedoms if it appears, in the circumstances of the case, that the other freedoms are entirely secondary in relation to the first and may be considered together with it.
(see para. 47)

2. Article 49 EC does not preclude legislation of a Member State which prohibits private operators established in other Member States, in which they lawfully provide similar services, from offering games of chance via the internet within the territory of that Member State.

Admittedly, such legislation gives rise to a restriction of the freedom to provide services enshrined in Article 49 EC, by also imposing a restriction on the freedom of the residents of the Member State concerned to enjoy, via the internet, services which are offered in other Member States.

However, in the light of the specific features associated with the provision of games of chance via the internet, the restriction at issue may be regarded as justified by the objective of combating fraud and crime. The grant of exclusive rights to operate games of chance via the internet to a single operator which is subject to strict control by the public authorities may confine the operation of gambling within controlled channels and be regarded as appropriate for the purpose of protecting consumers against fraud on the part of operators.

As to whether the system in dispute is necessary, the sector involving games of chance offered via the internet has not been the subject of Community harmonisation. A Member State is therefore entitled to take the view that the mere fact that a private operator lawfully offers services in that sector via the internet in another Member State, in which it is established and where it is in principle already subject to statutory conditions

and controls on the part of the competent authorities in that State, cannot be regarded as amounting to a sufficient assurance that national consumers will be protected against the risks of fraud and crime, in the light of the difficulties liable to be encountered in such a context by the authorities of the Member State of establishment in assessing the professional qualities and integrity of operators. In addition, because of the lack of direct contact between consumer and operator, games of chance accessible via the internet involve different and more substantial risks of fraud by operators against consumers compared with the traditional markets for such games. Moreover, the possibility cannot be ruled out that an operator which sponsors some of the sporting competitions on which it accepts bets and some of the teams taking part in those competitions may be in a position to influence their outcome directly or indirectly, and thus increase its profits. (see paras 53-54, 67-73, operative part).

C-156/13, Digibet Ltd, Gert Albers v Westdeutsche Lotterie GmbH & Co. OHG,

1. This request for a preliminary ruling concerns the interpretation of Article 56 EC.

18. In those circumstances, the Bundesgerichtshof decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. Does it represent an inconsistent restriction on gaming and betting activities where, on the one hand, in a Member State organised as a federal State, the organisation and facilitation of public games of chance on the internet is, in principle, prohibited by the law in force in the overwhelming majority of the Länder and — without an established right — can be allowed, exceptionally, only for lotteries and sporting bets in order to provide a suitable alternative to the illegal supply of games of chance as well as to combat the development and spread thereof, but — on the other hand, under the law in force in one of that Member State's Länder, subject to certain specified objective conditions, an authorisation for the marketing of sporting bets on the internet must be issued to any EU citizen or equivalent legal person, thereby undermining the effectiveness of the restriction on the marketing of games of chance on the internet in force in the rest of the Federal Republic in achieving the legitimate public interest objectives which it pursues?

2. Does the answer to the first question depend on whether the different legal position in one Land removes altogether or significantly undermines the effectiveness of the restrictions on the marketing of games of chance on the internet in force in the other Länder in achieving the legitimate public interest objectives which they pursue?

If the answer to the first question is in the affirmative:

3. Is the inconsistency avoided by the Land with the divergent legislation adopting the restrictions on games of chance in force in the rest of the Länder, even where, in relation to the administrative licensing contracts already concluded there, the previous more generous rules on internet games of chance in that Land remain in force for a transitional period of several years because those authorisations cannot be revoked, or cannot be revoked without incurring compensation payments which the Land would find difficult to bear?

4. Does the answer to the third question depend on whether, during the transition period of several years, the effectiveness of the restrictions on games of chance in force in the other Länder is affected or significantly undermined?

Ruling: Article 56 TFEU must be interpreted as meaning that it does not preclude legislation common to the majority of the federal entities of a Member State having a federal structure which prohibits, in principle, the organisation and facilitation of games of chance via the internet, where, for a limited period, a single federal entity has maintained in force more liberal legislation coexisting with the restrictive legislation of the other federal entities, provided that such legislation is able to satisfy the conditions of proportionality laid down by the case-law of the Court, which is for the national court to ascertain.

C-475/12 - UPC DTH

Questions to the Court of Justice for a preliminary ruling:

'1. May Article 2(c) of the Framework Directive ... be interpreted as meaning that a service by which a service provider supplies, for consideration, conditional access to a package of programmes which contains radio and television broadcast services and is retransmitted by satellite is to be classified as an electronic communications service?

2. May the [FEU Treaty] be interpreted as meaning that the principle of the free movement of services is applicable to the service described in the first question, in the case of a service supplied from Luxembourg to Hungary?

3. May the [FEU Treaty] be interpreted as meaning that, in the case of the service described in the first question, the country of destination, to which the service is sent, is entitled to limit the supply of that type of services by requiring that the [supplier of the] service has to be registered in that Member State and has to be established as a branch or separate legal entity, and allowing this type of services to be supplied only through the establishment of a branch or separate legal entity?

4. May the [FEU Treaty] be interpreted as meaning that administrative proceedings relating to the services described in the first question, regardless of the Member State in which the undertaking supplying that service operates or is registered, will be subject to the administrative authority of the Member State which has jurisdiction on the basis of the place in which the service is supplied?

5. May Article 2(c) of the [Framework Directive] be interpreted as meaning that the service described in the first question must be classified as an electronic communications service, or must such a service be classified as a conditional access service supplied using the conditional access system defined in Article 2(f) of the Framework Directive?

6. On the basis of all the foregoing, may the relevant provisions be interpreted as meaning that the service provider described in the first question must be classified as a provider of electronic communications services pursuant to [EU] law?

Ruling:

1. Article 2(c) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, must be interpreted as meaning that a service consisting in the supply, for consideration, of conditional access to a package of programmes which contains radio and television broadcast services and is retransmitted by satellite falls within the definition of 'electronic communications service' within the meaning of that provision.

The fact that that service includes a conditional access system within the meaning of Article 2(ea) and (f) of Directive 2002/21, as amended by Directive 2009/140, is irrelevant in that regard.

An operator supplying a service such as that at issue in the main proceedings must be regarded as a provider of electronic communications services under Directive 2002/21, as amended by Directive 2009/140.

2. In circumstances such as those at issue in the main proceedings, a service consisting in the supply, for consideration, of conditional access to a package of programmes which contains radio and audio-visual broadcast services and is retransmitted by satellite constitutes a provision of services for the purposes of Article 56 TFEU.

3. Surveillance proceedings relating to electronic communications services, such as that at issue in the main proceedings, will be subject to the authorities of the Member State in which the recipients of those services are resident.

4. Article 56 TFEU must be interpreted as meaning that:

– Member States are not precluded from requiring undertakings which supply electronic communications services, such as that at issue in the main proceedings, in their territory to register those services, provided that Member States act in compliance with the requirements set out in Article 3 of Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), as amended by Directive 2009/140; and

– on the other hand, undertakings wishing to supply electronic communications services, such as that at issue in the main proceedings, in a Member State other than that in which they are established cannot be required to establish in that State a branch or a legal entity separate from that located in the Member State of transmission.

Directive 2011/83/EU of the European parliament and of the Council of 25 October 2011 on consumer rights

Full name: Directive 2011/83/EU of the European parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises (4) and Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (5) lay down a number of contractual rights for consumers.

(2) Those Directives have been reviewed in the light of experience with a view to simplifying and updating the applicable rules, removing inconsistencies and closing unwanted gaps in the rules. That review has shown that it is appropriate to replace those two Directives by a single Directive. This Directive should therefore lay down standard rules for the common aspects of distance and off-premises contracts, moving away from the minimum harmonisation approach in the former Directives whilst allowing Member States to maintain or adopt national rules in relation to certain aspects.

(3) Article 169(1) and point (a) of Article 169(2) of the Treaty on the Functioning of the European Union (TFEU) provide that the Union is to contribute to the attainment of a high level of consumer protection through the measures adopted pursuant to Article 114 thereof.

(4) In accordance with Article 26(2) TFEU, the internal market is to comprise an area without internal frontiers in which the free movement of goods and services and freedom of establishment are ensured. The harmonisation of certain aspects of consumer distance and off-premises contracts is necessary for the promotion of a real consumer internal market striking the right balance between a high level of consumer protection and the competitiveness of enterprises, while ensuring respect for the principle of subsidiarity.

(5) The cross-border potential of distance selling, which should be one of the main tangible results of the internal market, is not fully exploited. Compared with the significant growth of domestic distance sales over the last few years, the growth in cross-border distance sales has been limited. This discrepancy is particularly significant for Internet sales for which the potential for further growth is high. The cross-border potential of contracts negotiated away from business premises (direct selling) is constrained by a number of factors including the different national consumer protection rules imposed upon the industry. Compared with the growth of domestic direct selling over the last few years, in particular in the services sector, for instance utilities, the number of consumers using this channel for cross-border purchases has remained flat. Responding to increased business opportunities in many Member States, small and medium-sized enterprises (including individual traders) or agents of direct selling companies should be more inclined to seek business opportunities in other Member States, in particular in border regions. Therefore the full harmonisation of consumer information and the right of withdrawal in distance and off-premises contracts will contribute to a high level of consumer protection and a better functioning of the business-to-consumer internal market.

(6) Certain disparities create significant internal market barriers affecting traders and consumers. Those disparities increase compliance costs to traders wishing to engage in the cross-border sale of goods or provision of services. Disproportionate fragmentation also undermines consumer confidence in the internal market.

(7) Full harmonisation of some key regulatory aspects should considerably increase legal certainty for both consumers and traders. Both consumers and traders should be able to rely on a single regulatory framework based on clearly defined legal concepts regulating certain aspects of business-to-consumer contracts across the Union. The effect of such harmonisation

should be to eliminate the barriers stemming from the fragmentation of the rules and to complete the internal market in this area. Those barriers can only be eliminated by establishing uniform rules at Union level. Furthermore consumers should enjoy a high common level of protection across the Union.

(8) The regulatory aspects to be harmonised should only concern contracts concluded between traders and consumers. Therefore, this Directive should not affect national law in the area of contracts relating to employment, contracts relating to succession rights, contracts relating to family law and contracts relating to the incorporation and organisation of companies or partnership agreements.

(9) This Directive establishes rules on information to be provided for distance contracts, off-premises contracts and contracts other than distance and off-premises contracts. This Directive also regulates the right of withdrawal for distance and off-premises contracts and harmonises certain provisions dealing with the performance and some other aspects of business-to-consumer contracts.

(10) This Directive should be without prejudice to Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (6).

(11) This Directive should be without prejudice to Union provisions relating to specific sectors, such as medicinal products for human use, medical devices, privacy and electronic communications, patients' rights in cross-border healthcare, food labelling and the internal market for electricity and natural gas.

(12) The information requirements provided for in this Directive should complete the information requirements of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (7) and Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (8). Member States should retain the possibility to impose additional information requirements applicable to service providers established in their territory.

(13) Member States should remain competent, in accordance with Union law, to apply the provisions of this Directive to areas not falling within its scope. Member States may therefore maintain or introduce national legislation corresponding to the provisions of this Directive, or certain of its provisions, in relation to contracts that fall outside the scope of this Directive. For instance, Member States may decide to extend the application of the rules of this Directive to legal persons or to natural persons who are not consumers within the meaning of this Directive, such as non-governmental organisations, start-ups or small and medium-sized enterprises. Similarly, Member States may apply the provisions of this Directive to contracts that are not distance contracts within the meaning of this Directive, for example because they are not concluded under an organised distance sales or service-provision scheme. Moreover, Member States may also maintain or introduce national provisions on issues not specifically addressed in this Directive, such as additional rules concerning sales contracts, including in relation to the delivery of goods, or requirements for the provision of information during the existence of a contract.

(14) This Directive should not affect national law in the area of contract law for contract law aspects that are not regulated by this Directive. Therefore, this Directive should be without prejudice to national law regulating for instance the conclusion or the validity of a contract (for instance in the case of lack of consent). Similarly, this Directive should not affect national law in relation to the general contractual legal remedies, the rules on public economic order, for instance rules on excessive or extortionate prices, and the rules on unethical legal transactions.

(15) This Directive should not harmonise language requirements applicable to consumer contracts. Therefore,

Member States may maintain or introduce in their national law language requirements regarding contractual information and contractual terms.

(16) This Directive should not affect national laws on legal representation such as the rules relating to the person who is acting in the name of the trader or on his behalf (such as an agent or a trustee). Member States should remain competent in this area. This Directive should apply to all traders, whether public or private.

(17) The definition of consumer should cover natural persons who are acting outside their trade, business, craft or profession. However, in the case of dual purpose contracts, where the contract is concluded for purposes partly within and partly outside the person's trade and the trade purpose is so limited as not to be predominant in the overall context of the contract, that person should also be considered as a consumer.

(18) This Directive does not affect the freedom of Member States to define, in conformity with Union law, what they consider to be services of general economic interest, how those services should be organised and financed, in compliance with State aid rules, and which specific obligations they should be subject to.

(19) Digital content means data which are produced and supplied in digital form, such as computer programs, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through any other means. Contracts for the supply of digital content should fall within the scope of this Directive. If digital content is supplied on a tangible medium, such as a CD or a DVD, it should be considered as goods within the meaning of this Directive. Similarly to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating, contracts for digital content which is not supplied on a tangible medium should be classified, for the purpose of this Directive, neither as sales contracts nor as service contracts. For such contracts, the consumer should have a right of withdrawal unless he has consented to the beginning of the performance of the contract during the withdrawal period and has acknowledged that he will consequently lose the right to withdraw from the contract. In addition to the general information requirements, the trader should inform the consumer about the functionality and the relevant interoperability of digital content. The notion of functionality should refer to the ways in which digital content can be used, for instance for the tracking of consumer behaviour; it should also refer to the absence or presence of any technical restrictions such as protection via Digital Rights Management or region coding. The notion of relevant interoperability is meant to describe the information regarding the standard hardware and software environment with which the digital content is compatible, for instance the operating system, the necessary version and certain hardware features. The Commission should examine the need for further harmonisation of provisions in respect of digital content and submit, if necessary, a legislative proposal for addressing this matter.

(20) The definition of distance contract should cover all cases where a contract is concluded between the trader and the consumer under an organised distance sales or service-provision scheme, with the exclusive use of one or more means of distance communication (such as mail order, Internet, telephone or fax) up to and including the time at which the contract is concluded. That definition should also cover situations where the consumer visits the business premises merely for the purpose of gathering information about the goods or services and subsequently negotiates and concludes the contract at a distance. By contrast, a contract which is negotiated at the business premises of the trader and finally concluded by means of distance communication should not be considered a distance contract. Neither should a contract initiated by means of distance communication, but finally concluded at the business premises of the trader be

considered a distance contract. Similarly, the concept of distance contract should not include reservations made by a consumer through a means of distance communications to request the provision of a service from a professional, such as in the case of a consumer phoning to request an appointment with a hairdresser. The notion of an organised distance sales or service-provision scheme should include those schemes offered by a third party other than the trader but used by the trader, such as an online platform. It should not, however, cover cases where websites merely offer information on the trader, his goods and/or services and his contact details.

(21) An off-premises contract should be defined as a contract concluded with the simultaneous physical presence of the trader and the consumer, in a place which is not the business premises of the trader, for example at the consumer's home or workplace. In an off-premises context, the consumer may be under potential psychological pressure or may be confronted with an element of surprise, irrespective of whether or not the consumer has solicited the trader's visit. The definition of an off-premises contract should also include situations where the consumer is personally and individually addressed in an off-premises context but the contract is concluded immediately afterwards on the business premises of the trader or through a means of distance communication. The definition of an off-premises contract should not cover situations in which the trader first comes to the consumer's home strictly with a view to taking measurements or giving an estimate without any commitment of the consumer and where the contract is then concluded only at a later point in time on the business premises of the trader or via means of distance communication on the basis of the trader's estimate. In those cases, the contract is not to be considered as having been concluded immediately after the trader has addressed the consumer if the consumer has had time to reflect upon the estimate of the trader before concluding the contract. Purchases made during an excursion organised by the trader during which the products acquired are promoted and offered for sale should be considered as off-premises contracts.

(22) Business premises should include premises in whatever form (such as shops, stalls or lorries) which serve as a permanent or usual place of business for the trader. Market stalls and fair stands should be treated as business premises if they fulfil this condition. Retail premises where the trader carries out his activity on a seasonal basis, for instance during the tourist season at a ski or beach resort, should be considered as business premises as the trader carries out his activity in those premises on a usual basis. Spaces accessible to the public, such as streets, shopping malls, beaches, sports facilities and public transport, which the trader uses on an exceptional basis for his business activities as well as private homes or workplaces should not be regarded as business premises. The business premises of a person acting in the name or on behalf of the trader as defined in this Directive should be considered as business premises within the meaning of this Directive.

(23) Durable media should enable the consumer to store the information for as long as it is necessary for him to protect his interests stemming from his relationship with the trader. Such media should include in particular paper, USB sticks, CD-ROMs, DVDs, memory cards or the hard disks of computers as well as e-mails.

(24) A public auction implies that traders and consumers attend or are given the possibility to attend the auction in person. The goods or services are offered by the trader to the consumer through a bidding procedure authorised by law in some Member States, to offer goods or services at public sale. The successful bidder is bound to purchase the goods or services. The use of online platforms for auction purposes which are at the disposal of consumers and traders should not be considered as a public auction within the meaning of this Directive.

(25) Contracts related to district heating should be covered by this Directive, similarly to the contracts for the supply of water, gas or electricity. District heating refers to the supply

of heat, inter alia, in the form of steam or hot water, from a central source of production through a transmission and distribution system to multiple buildings, for the purpose of heating.

(26) Contracts related to the transfer of immovable property or of rights in immovable property or to the creation or acquisition of such immovable property or rights, contracts for the construction of new buildings or the substantial conversion of existing buildings as well as contracts for the rental of accommodation for residential purposes are already subject to a number of specific requirements in national legislation. Those contracts include for instance sales of immovable property still to be developed and hire-purchase. The provisions of this Directive are not appropriate to those contracts, which should be therefore excluded from its scope. A substantial conversion is a conversion comparable to the construction of a new building, for example where only the façade of an old building is retained. Service contracts in particular those related to the construction of annexes to buildings (for example a garage or a veranda) and those related to repair and renovation of buildings other than substantial conversion, should be included in the scope of this Directive, as well as contracts related to the services of a real estate agent and those related to the rental of accommodation for non-residential purposes.

(27) Transport services cover passenger transport and transport of goods. Passenger transport should be excluded from the scope of this Directive as it is already subject to other Union legislation or, in the case of public transport and taxis, to Regulation at national level. However, the provisions of this Directive protecting consumers against excessive fees for the use of means of payment or against hidden costs should apply also to passenger transport contracts. In relation to transport of goods and car rental which are services, consumers should benefit from the protection afforded by this Directive, with the exception of the right of withdrawal.

(28) In order to avoid administrative burden being placed on traders, Member States may decide not to apply this Directive where goods or services of a minor value are sold off-premises. The monetary threshold should be established at a sufficiently low level as to exclude only purchases of small significance. Member States should be allowed to define this value in their national legislation provided that it does not exceed EUR 50. Where two or more contracts with related subjects are concluded at the same time by the consumer, the total cost thereof should be taken into account for the purpose of applying this threshold.

(29) Social services have fundamentally distinct features that are reflected in sector-specific legislation, partially at Union level and partially at national level. Social services include, on the one hand, services for particularly disadvantaged or low income persons as well as services for persons and families in need of assistance in carrying out routine, everyday tasks and, on the other hand, services for all people who have a special need for assistance, support, protection or encouragement in a specific life phase. Social services cover, inter alia, services for children and youth, assistance services for families, single parents and older persons, and services for migrants. Social services cover both short-term and long-term care services, for instance services provided by home care services or provided in assisted living facilities and residential homes or housing ('nursing homes'). Social services include not only those provided by the State at a national, regional or local level by providers mandated by the State or by charities recognised by the State but also those provided by private operators. The provisions of this Directive are not appropriate to social services which should be therefore excluded from its scope.

(30) Healthcare requires special Regulations because of its technical complexity, its importance as a service of general interest as well as its extensive public funding. Healthcare is defined in Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (9) as 'health

services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices'. Health professional is defined in that Directive as a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (10) or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in point (a) of Article 3(1) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment. The provisions of this Directive are not appropriate to healthcare which should be therefore excluded from its scope.

(31) Gambling should be excluded from the scope of this Directive. Gambling activities are those which involve wagering at stake with pecuniary value in games of chance, including lotteries, gambling in casinos and betting transactions. Member States should be able to adopt other, including more stringent, consumer protection measures in relation to such activities.

(32) The existing Union legislation, *inter alia*, relating to consumer financial services, package travel and timeshare contains numerous rules on consumer protection. For this reason, this Directive should not apply to contracts in those areas. With regard to financial services, Member States should be encouraged to draw inspiration from existing Union legislation in that area when legislating in areas not regulated at Union level, in such a way that a level playing field for all consumers and all contracts relating to financial services is ensured.

(33) The trader should be obliged to inform the consumer in advance of any arrangement resulting in the consumer paying a deposit to the trader, including an arrangement whereby an amount is blocked on the consumer's credit or debit card.

(34) The trader should give the consumer clear and comprehensible information before the consumer is bound by a distance or off-premises contract, a contract other than a distance or an off-premises contract, or any corresponding offer. In providing that information, the trader should take into account the specific needs of consumers who are particularly vulnerable because of their mental, physical or psychological infirmity, age or credulity in a way which the trader could reasonably be expected to foresee. However, taking into account such specific needs should not lead to different levels of consumer protection.

(35) The information to be provided by the trader to the consumer should be mandatory and should not be altered. Nevertheless, the contracting parties should be able to expressly agree to change the content of the contract subsequently concluded, for instance the arrangements for delivery.

(36) In the case of distance contracts, the information requirements should be adapted to take into account the technical constraints of certain media, such as the restrictions on the number of characters on certain mobile telephone screens or the time constraint on television sales spots. In such cases the trader should comply with a minimum set of information requirements and refer the consumer to another source of information, for instance by providing a toll free telephone number or a hypertext link to a webpage of the trader where the relevant information is directly available and easily accessible. As to the requirement to inform the consumer of the cost of returning goods which by their nature cannot normally be returned by post, it will be considered to have been met, for example, if the trader specifies one carrier (for instance the one he assigned for the delivery of the good) and one price concerning the cost of returning the goods. Where the cost of returning the goods cannot reasonably be calculated in advance by the trader, for example because the trader does not offer to arrange for the return of the goods himself, the trader should provide a statement that such a cost

will be payable, and that this cost may be high, along with a reasonable estimation of the maximum cost, which could be based on the cost of delivery to the consumer.

(37) Since in the case of distance sales, the consumer is not able to see the goods before concluding the contract, he should have a right of withdrawal. For the same reason, the consumer should be allowed to test and inspect the goods he has bought to the extent necessary to establish the nature, characteristics and the functioning of the goods. Concerning off-premises contracts, the consumer should have the right of withdrawal because of the potential surprise element and/or psychological pressure. Withdrawal from the contract should terminate the obligation of the contracting parties to perform the contract.

(38) Trading websites should indicate clearly and legibly at the latest at the beginning of the ordering process whether any delivery restrictions apply and which means of payment are accepted.

(39) It is important to ensure for distance contracts concluded through websites that the consumer is able to fully read and understand the main elements of the contract before placing his order. To that end, provision should be made in this Directive for those elements to be displayed in the close vicinity of the confirmation requested for placing the order. It is also important to ensure that, in such situations, the consumer is able to determine the moment at which he assumes the obligation to pay the trader. Therefore, the consumer's attention should specifically be drawn, through an unambiguous formulation, to the fact that placing the order entails the obligation to pay the trader.

(40) The current varying lengths of the withdrawal periods both between the Member States and for distance and off-premises contracts cause legal uncertainty and compliance costs. The same withdrawal period should apply to all distance and off-premises contracts. In the case of service contracts, the withdrawal period should expire after 14 days from the conclusion of the contract. In the case of sales contracts, the withdrawal period should expire after 14 days from the day on which the consumer or a third party other than the carrier and indicated by the consumer, acquires physical possession of the goods. In addition the consumer should be able to exercise the right to withdraw before acquiring physical possession of the goods. Where multiple goods are ordered by the consumer in one order but are delivered separately, the withdrawal period should expire after 14 days from the day on which the consumer acquires physical possession of the last good. Where goods are delivered in multiple lots or pieces, the withdrawal period should expire after 14 days from the day on which the consumer acquires the physical possession of the last lot or piece.

(41) In order to ensure legal certainty, it is appropriate that Council Regulation (EEC, Euratom) No 1182/71 of 3 June 1971 determining the rules applicable to periods, dates and time limits (11) should apply to the calculation of the periods contained in this Directive. Therefore, all periods contained in this Directive should be understood to be expressed in calendar days. Where a period expressed in days is to be calculated from the moment at which an event occurs or an action takes place, the day during which that event occurs or that action takes place should not be considered as falling within the period in question.

(42) The provisions relating to the right of withdrawal should be without prejudice to the Member States' laws and Regulations governing the termination or unenforceability of a contract or the possibility for the consumer to fulfil his contractual obligations before the time determined in the contract.

(43) If the trader has not adequately informed the consumer prior to the conclusion of a distance or off-premises contract, the withdrawal period should be extended. However, in order to ensure legal certainty as regards the length of the withdrawal period, a 12-month limitation period should be introduced.

(44) Differences in the ways in which the right of withdrawal is exercised in the Member States have caused costs for traders selling cross-border. The introduction of a harmonised model withdrawal form that the consumer may use should simplify the withdrawal process and bring legal certainty. For these reasons, Member States should refrain from adding any presentational requirements to the Union-wide model form relating for example to the font size. However, the consumer should remain free to withdraw in his own words, provided that his statement setting out his decision to withdraw from the contract to the trader is unequivocal. A letter, a telephone call or returning the goods with a clear statement could meet this requirement, but the burden of proof of having withdrawn within the time limits fixed in the Directive should be on the consumer. For this reason, it is in the interest of the consumer to make use of a durable medium when communicating his withdrawal to the trader.

(45) As experience shows that many consumers and traders prefer to communicate via the trader's website, there should be a possibility for the trader to give the consumer the option of filling in a web-based withdrawal form. In this case the trader should provide an acknowledgement of receipt for instance by e-mail without delay.

(46) In the event that the consumer withdraws from the contract, the trader should reimburse all payments received from the consumer, including those covering the expenses borne by the trader to deliver goods to the consumer. The reimbursement should not be made by voucher unless the consumer has used vouchers for the initial transaction or has expressly accepted them. If the consumer expressly chooses a certain type of delivery (for instance 24-hour express delivery), although the trader had offered a common and generally acceptable type of delivery which would have incurred lower delivery costs, the consumer should bear the difference in costs between these two types of delivery.

(47) Some consumers exercise their right of withdrawal after having used the goods to an extent more than necessary to establish the nature, characteristics and the functioning of the goods. In this case the consumer should not lose the right to withdraw but should be liable for any diminished value of the goods. In order to establish the nature, characteristics and functioning of the goods, the consumer should only handle and inspect them in the same manner as he would be allowed to do in a shop. For example, the consumer should only try on a garment and should not be allowed to wear it. Consequently, the consumer should handle and inspect the goods with due care during the withdrawal period. The obligations of the consumer in the event of withdrawal should not discourage the consumer from exercising his right of withdrawal.

(48) The consumer should be required to send back the goods not later than 14 days after having informed the trader about his decision to withdraw from the contract. In situations where the trader or the consumer does not fulfil the obligations relating to the exercise of the right of withdrawal, penalties provided for by national legislation in accordance with this Directive should apply as well as contract law provisions.

(49) Certain exceptions from the right of withdrawal should exist, both for distance and off-premises contracts. A right of withdrawal could be inappropriate for example given the nature of particular goods or services. That is the case for example with wine supplied a long time after the conclusion of a contract of a speculative nature where the value is dependent on fluctuations in the market ("vin en primeur"). The right of withdrawal should neither apply to goods made to the consumer's specifications or which are clearly personalised such as tailor-made curtains, nor to the supply of fuel, for example, which is a good, by nature inseparably mixed with other items after delivery. The granting of a right of withdrawal to the consumer could also be inappropriate in the case of certain services where the conclusion of the contract implies the setting aside of capacity which, if a right of withdrawal were exercised, the trader may find difficult to

fill. This would for example be the case where reservations are made at hotels or concerning holiday cottages or cultural or sporting events.

(50) On the one hand, the consumer should benefit from his right of withdrawal even in case he has asked for the provision of services before the end of the withdrawal period. On the other hand, if the consumer exercises his right of withdrawal, the trader should be assured to be adequately paid for the service he has provided. The calculation of the proportionate amount should be based on the price agreed in the contract unless the consumer demonstrates that that total price is itself disproportionate, in which case the amount to be paid shall be calculated on the basis of the market value of the service provided. The market value should be defined by comparing the price of an equivalent service performed by other traders at the time of the conclusion of the contract. Therefore the consumer should request the performance of services before the end of the withdrawal period by making this request expressly and, in the case of off-premises contracts, on a durable medium. Similarly, the trader should inform the consumer on a durable medium of any obligation to pay the proportionate costs for the services already provided. For contracts having as their object both goods and services, the rules provided for in this Directive on the return of goods should apply to the goods aspects and the compensation regime for services should apply to the services aspects.

(51) The main difficulties encountered by consumers and one of the main sources of disputes with traders concern delivery of goods, including goods getting lost or damaged during transport and late or partial delivery. Therefore it is appropriate to clarify and harmonise the national rules as to when delivery should occur. The place and modalities of delivery and the rules concerning the determination of the conditions for the transfer of the ownership of the goods and the moment at which such transfer takes place, should remain subject to national law and therefore should not be affected by this Directive. The rules on delivery laid down in this Directive should include the possibility for the consumer to allow a third party to acquire on his behalf the physical possession or control of the goods. The consumer should be considered to have control of the goods where he or a third party indicated by the consumer has access to the goods to use them as an owner, or the ability to resell the goods (for example, when he has received the keys or possession of the ownership documents).

(52) In the context of sales contracts, the delivery of goods can take place in various ways, either immediately or at a later date. If the parties have not agreed on a specific delivery date, the trader should deliver the goods as soon as possible, but in any event not later than 30 days from the day of the conclusion of the contract. The rules regarding late delivery should also take into account goods to be manufactured or acquired specially for the consumer which cannot be reused by the trader without considerable loss. Therefore, a rule which grants an additional reasonable period of time to the trader in certain circumstances should be provided for in this Directive. When the trader has failed to deliver the goods within the period of time agreed with the consumer, before the consumer can terminate the contract, the consumer should call upon the trader to make the delivery within a reasonable additional period of time and be entitled to terminate the contract if the trader fails to deliver the goods even within that additional period of time. However, this rule should not apply when the trader has refused to deliver the goods in an unequivocal statement. Neither should it apply in certain circumstances where the delivery period is essential such as, for example, in the case of a wedding dress which should be delivered before the wedding. Nor should it apply in circumstances where the consumer informs the trader that delivery on a specified date is essential. For this purpose, the consumer may use the trader's contact details given in accordance with this Directive. In these specific cases, if the trader fails to deliver the goods on time, the consumer should be entitled to terminate the contract immediately after the

expiry of the delivery period initially agreed. This Directive should be without prejudice to national provisions on the way the consumer should notify the trader of his will to terminate the contract.

(53) In addition to the consumer's right to terminate the contract where the trader has failed to fulfil his obligations to deliver the goods in accordance with this Directive, the consumer may, in accordance with the applicable national law, have recourse to other remedies, such as granting the trader an additional period of time for delivery, enforcing the performance of the contract, withholding payment, and seeking damages.

(54) In accordance with Article 52(3) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market (12), Member States should be able to prohibit or limit traders' right to request charges from consumers taking into account the need to encourage competition and promote the use of efficient payment instruments. In any event, traders should be prohibited from charging consumers fees that exceed the cost borne by the trader for the use of a certain means of payment.

(55) Where the goods are dispatched by the trader to the consumer, disputes may arise, in the event of loss or damage, as to the moment at which the transfer of risk takes place. Therefore this Directive should provide that the consumer be protected against any risk of loss of or damage to the goods occurring before he has acquired the physical possession of the goods. The consumer should be protected during a transport arranged or carried out by the trader, even where the consumer has chosen a particular delivery method from a range of options offered by the trader. However, that provision should not apply to contracts where it is up to the consumer to take delivery of the goods himself or to ask a carrier to take delivery. Regarding the moment of the transfer of the risk, a consumer should be considered to have acquired the physical possession of the goods when he has received them.

(56) Persons or organisations regarded under national law as having a legitimate interest in protecting consumer contractual rights should be afforded the right to initiate proceedings, either before a court or before an administrative authority which is competent to decide upon complaints or to initiate appropriate legal proceedings.

(57) It is necessary that Member States lay down penalties for infringements of this Directive and ensure that they are enforced. The penalties should be effective, proportionate and dissuasive.

(58) The consumer should not be deprived of the protection granted by this Directive. Where the law applicable to the contract is that of a third country, Regulation (EC) No 593/2008 should apply, in order to determine whether the consumer retains the protection granted by this Directive.

(59) The Commission, following consultation with the Member States and stakeholders, should look into the most appropriate way to ensure that all consumers are made aware of their rights at the point of sale.

(60) Since inertia selling, which consists of unsolicited supply of goods or provision of services to consumers, is prohibited by Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive') (13) but no contractual remedy is provided therein, it is necessary to introduce in this Directive the contractual remedy of exempting the consumer from the obligation to provide any consideration for such unsolicited supply or provision.

(61) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (14) already regulates unsolicited communications and provides for a high level of consumer

protection. The corresponding provisions on the same issue contained in Directive 97/7/EC are therefore not needed.

(62) It is appropriate for the Commission to review this Directive if some barriers to the internal market are identified. In its review, the Commission should pay particular attention to the possibilities granted to Member States to maintain or introduce specific national provisions including in certain areas of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (15) and Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees (16). That review could lead to a Commission proposal to amend this Directive; that proposal may include amendments to other consumer protection legislation reflecting the Commission's Consumer Policy Strategy commitment to review the Union acquis in order to achieve a high, common level of consumer protection.

(63) Directives 93/13/EEC and 1999/44/EC should be amended to require Member States to inform the Commission about the adoption of specific national provisions in certain areas.

(64) Directives 85/577/EEC and 97/7/EC should be repealed.

(65) Since the objective of this Directive, namely, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market, cannot be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(66) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union.

(67) In accordance with point 34 of the Interinstitutional agreement on better law-making (17), Member States are encouraged to draw up, for themselves and in the interests of the Union, their own tables, which will, as far as possible, illustrate the correlation between this Directive and the transposition measures, and to make them public,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

SUBJECT MATTER, DEFINITIONS AND SCOPE

Article 1

Subject matter

The purpose of this Directive is, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market by approximating certain aspects of the laws, Regulations and administrative provisions of the Member States concerning contracts concluded between consumers and traders.

Article 2

Definitions

For the purpose of this Directive, the following definitions shall apply:

(1) 'consumer' means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession;

(2) 'trader' means any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive;

(3) 'goods' means any tangible movable items, with the exception of items sold by way of execution or otherwise by authority of law; water, gas and electricity shall be considered as goods within the meaning of this Directive where they are put up for sale in a limited volume or a set quantity;

(4) 'goods made to the consumer's specifications' means non-prefabricated goods made on the basis of an individual choice of or decision by the consumer;

(5) 'sales contract' means any contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer and the consumer pays or undertakes to pay the price thereof, including any contract having as its object both goods and services;

(6) 'service contract' means any contract other than a sales contract under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof;

(7) 'distance contract' means any contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded;

(8) 'off-premises contract' means any contract between the trader and the consumer:

(a) concluded in the simultaneous physical presence of the trader and the consumer, in a place which is not the business premises of the trader;

(b) for which an offer was made by the consumer in the same circumstances as referred to in point (a);

(c) concluded on the business premises of the trader or through any means of distance communication immediately after the consumer was personally and individually addressed in a place which is not the business premises of the trader in the simultaneous physical presence of the trader and the consumer; or

(d) concluded during an excursion organised by the trader with the aim or effect of promoting and selling goods or services to the consumer;

(9) 'business premises' means:

(a) any immovable retail premises where the trader carries out his activity on a permanent basis; or

(b) any movable retail premises where the trader carries out his activity on a usual basis;

(10) 'durable medium' means any instrument which enables the consumer or the trader to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;

(11) 'digital content' means data which are produced and supplied in digital form;

(12) 'financial service' means any service of a banking, credit, insurance, personal pension, investment or payment nature;

(13) 'public auction' means a method of sale where goods or services are offered by the trader to consumers, who attend or are given the possibility to attend the auction in person, through a transparent, competitive bidding procedure run by an auctioneer and where the successful bidder is bound to purchase the goods or services;

(14) 'commercial guarantee' means any undertaking by the trader or a producer (the guarantor) to the consumer, in addition to his legal obligation relating to the guarantee of conformity, to reimburse the price paid or to replace, repair or service goods in any way if they do not meet the specifications or any other requirements not related to conformity set out in the guarantee statement or in the relevant advertising available at the time of, or before the conclusion of the contract;

(15) 'ancillary contract' means a contract by which the consumer acquires goods or services related to a distance contract or an off-premises contract and where those goods are supplied or those services are provided by the trader or by a third party on the basis of an arrangement between that third party and the trader.

Article 3 Scope

1. This Directive shall apply, under the conditions and to the extent set out in its provisions, to any contract concluded between a trader and a consumer. It shall also apply to contracts for the supply of water, gas, electricity or district heating, including by public providers, to the extent that these commodities are provided on a contractual basis.

2. If any provision of this Directive conflicts with a provision of another Union act governing specific sectors, the provision of that other Union act shall prevail and shall apply to those specific sectors.

3. This Directive shall not apply to contracts:

(a) for social services, including social housing, childcare and support of families and persons permanently or temporarily in need, including long-term care;

(b) for healthcare as defined in point (a) of Article 3 of Directive 2011/24/EU, whether or not they are provided via healthcare facilities;

(c) for gambling, which involves wagering a stake with pecuniary value in games of chance, including lotteries, casino games and betting transactions;

(d) for financial services;

(e) for the creation, acquisition or transfer of immovable property or of rights in immovable property;

(f) for the construction of new buildings, the substantial conversion of existing buildings and for rental of accommodation for residential purposes;

(g) which fall within the scope of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours (18);

(h) which fall within the scope of Directive 2008/122/EC of the European Parliament and of the Council of 14 January 2009 on the protection of consumers in respect of certain aspects of timeshare, long-term holiday product, resale and exchange contracts (19);

(i) which, in accordance with the laws of Member States, are established by a public office-holder who has a statutory obligation to be independent and impartial and who must ensure, by providing comprehensive legal information, that the consumer only concludes the contract on the basis of careful legal consideration and with knowledge of its legal scope;

(j) for the supply of foodstuffs, beverages or other goods intended for current consumption in the household, and which are physically supplied by a trader on frequent and regular rounds to the consumer's home, residence or workplace;

(k) for passenger transport services, with the exception of Article 8(2) and Articles 19 and 22;

(l) concluded by means of automatic vending machines or automated commercial premises;

(m) concluded with telecommunications operators through public payphones for their use or concluded for the use of one single connection by telephone, Internet or fax established by a consumer.

4. Member States may decide not to apply this Directive or not to maintain or introduce corresponding national provisions to off-premises contracts for which the payment to be made by the consumer does not exceed EUR 50. Member States may define a lower value in their national legislation.

5. This Directive shall not affect national general contract law such as the rules on the validity, formation or effect of a contract, in so far as general contract law aspects are not regulated in this Directive.

6. This Directive shall not prevent traders from offering consumers contractual arrangements which go beyond the protection provided for in this Directive.

Article 4

Level of harmonisation

Member States shall not maintain or introduce, in their national law, provisions diverging from those laid down in this Directive, including more or less stringent provisions to ensure a different level of consumer protection, unless otherwise provided for in this Directive.

CHAPTER II
CONSUMER INFORMATION FOR CONTRACTS OTHER THAN
DISTANCE OR OFF-PREMISES CONTRACTS

Article 5

Information requirements for contracts other than distance or off-premises contracts

1. Before the consumer is bound by a contract other than a distance or an off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner, if that information is not already apparent from the context:

- (a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;
- (b) the identity of the trader, such as his trading name, the geographical address at which he is established and his telephone number;
- (c) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable;
- (d) where applicable, the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the service, and the trader's complaint handling policy;
- (e) in addition to a reminder of the existence of a legal guarantee of conformity for goods, the existence and the conditions of after-sales services and commercial guarantees, where applicable;
- (f) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract;
- (g) where applicable, the functionality, including applicable technical protection measures, of digital content;
- (h) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of.

2. Paragraph 1 shall also apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium.

3. Member States shall not be required to apply paragraph 1 to contracts which involve day-to-day transactions and which are performed immediately at the time of their conclusion.

4. Member States may adopt or maintain additional pre-contractual information requirements for contracts to which this Article applies.

CHAPTER III
CONSUMER INFORMATION AND RIGHT OF WITHDRAWAL
FOR DISTANCE AND OFF-PREMISES CONTRACTS

Article 6

Information requirements for distance and off-premises contracts

1. Before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner:

- (a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;
- (b) the identity of the trader, such as his trading name;
- (c) the geographical address at which the trader is established and the trader's telephone number, fax

number and e-mail address, where available, to enable the consumer to contact the trader quickly and communicate with him efficiently and, where applicable, the geographical address and identity of the trader on whose behalf he is acting;

(d) if different from the address provided in accordance with point (c), the geographical address of the place of business of the trader, and, where applicable, that of the trader on whose behalf he is acting, where the consumer can address any complaints;

(e) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges and any other costs or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable. In the case of a contract of indeterminate duration or a contract containing a subscription, the total price shall include the total costs per billing period. Where such contracts are charged at a fixed rate, the total price shall also mean the total monthly costs. Where the total costs cannot be reasonably calculated in advance, the manner in which the price is to be calculated shall be provided;

(f) the cost of using the means of distance communication for the conclusion of the contract where that cost is calculated other than at the basic rate;

(g) the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the services and, where applicable, the trader's complaint handling policy;

(h) where a right of withdrawal exists, the conditions, time limit and procedures for exercising that right in accordance with Article 11(1), as well as the model withdrawal form set out in Annex I(B);

(i) where applicable, that the consumer will have to bear the cost of returning the goods in case of withdrawal and, for distance contracts, if the goods, by their nature, cannot normally be returned by post, the cost of returning the goods;

(j) that, if the consumer exercises the right of withdrawal after having made a request in accordance with Article 7(3) or Article 8(8), the consumer shall be liable to pay the trader reasonable costs in accordance with Article 14(3);

(k) where a right of withdrawal is not provided for in accordance with Article 16, the information that the consumer will not benefit from a right of withdrawal or, where applicable, the circumstances under which the consumer loses his right of withdrawal;

(l) a reminder of the existence of a legal guarantee of conformity for goods;

(m) where applicable, the existence and the conditions of after sale customer assistance, after-sales services and commercial guarantees;

(n) the existence of relevant codes of conduct, as defined in point (f) of Article 2 of Directive 2005/29/EC, and how copies of them can be obtained, where applicable;

(o) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract;

(p) where applicable, the minimum duration of the consumer's obligations under the contract;

(q) where applicable, the existence and the conditions of deposits or other financial guarantees to be paid or provided by the consumer at the request of the trader;

(r) where applicable, the functionality, including applicable technical protection measures, of digital content;

(s) where applicable, any relevant interoperability of digital content with hardware and software that the

trader is aware of or can reasonably be expected to have been aware of;

(t) where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is subject, and the methods for having access to it.

2. Paragraph 1 shall also apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium.

3. In the case of a public auction, the information referred to in points (b), (c) and (d) of paragraph 1 may be replaced by the equivalent details for the auctioneer.

4. The information referred to in points (h), (i) and (j) of paragraph 1 may be provided by means of the model instructions on withdrawal set out in Annex I(A). The trader shall have fulfilled the information requirements laid down in points (h), (i) and (j) of paragraph 1 if he has supplied these instructions to the consumer, correctly filled in.

5. The information referred to in paragraph 1 shall form an integral part of the distance or off-premises contract and shall not be altered unless the contracting parties expressly agree otherwise.

6. If the trader has not complied with the information requirements on additional charges or other costs as referred to in point (e) of paragraph 1, or on the costs of returning the goods as referred to in point (i) of paragraph 1, the consumer shall not bear those charges or costs.

7. Member States may maintain or introduce in their national law language requirements regarding the contractual information, so as to ensure that such information is easily understood by the consumer.

8. The information requirements laid down in this Directive are in addition to information requirements contained in Directive 2006/123/EC and Directive 2000/31/EC and do not prevent Member States from imposing additional information requirements in accordance with those Directives.

Without prejudice to the first subparagraph, if a provision of Directive 2006/123/EC or Directive 2000/31/EC on the content and the manner in which the information is to be provided conflicts with a provision of this Directive, the provision of this Directive shall prevail.

9. As regards compliance with the information requirements laid down in this Chapter, the burden of proof shall be on the trader.

Article 7

Formal requirements for off-premises contracts

1. With respect to off-premises contracts, the trader shall give the information provided for in Article 6(1) to the consumer on paper or, if the consumer agrees, on another durable medium. That information shall be legible and in plain, intelligible language.

2. The trader shall provide the consumer with a copy of the signed contract or the confirmation of the contract on paper or, if the consumer agrees, on another durable medium, including, where applicable, the confirmation of the consumer's prior express consent and acknowledgement in accordance with point (m) of Article 16.

3. Where a consumer wants the performance of services or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating to begin during the withdrawal period provided for in Article 9(2), the trader shall require that the consumer makes such an express request on a durable medium.

4. With respect to off-premises contracts where the consumer has explicitly requested the services of the trader for the purpose of carrying out repairs or maintenance for which the trader and the consumer immediately perform their contractual obligations and where the payment to be made by the consumer does not exceed EUR 200:

(a) the trader shall provide the consumer with the information referred to in points (b) and (c) of Article 6(1) and information about the price or the manner in

which the price is to be calculated together with an estimate of the total price, on paper or, if the consumer agrees, on another durable medium. The trader shall provide the information referred to in points (a), (h) and (k) of Article 6(1), but may choose not to provide it on paper or another durable medium if the consumer expressly agrees;

(b) the confirmation of the contract provided in accordance with paragraph 2 of this Article shall contain the information provided for in Article 6(1).

Member States may decide not to apply this paragraph.

5. Member States shall not impose any further formal pre-contractual information requirements for the fulfilment of the information obligations laid down in this Directive.

Article 8

Formal requirements for distance contracts

1. With respect to distance contracts, the trader shall give the information provided for in Article 6(1) or make that information available to the consumer in a way appropriate to the means of distance communication used in plain and intelligible language. In so far as that information is provided on a durable medium, it shall be legible.

2. If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the trader shall make the consumer aware in a clear and prominent manner, and directly before the consumer places his order, of the information provided for in points (a), (e), (o) and (p) of Article 6(1).

The trader shall ensure that the consumer, when placing his order, explicitly acknowledges that the order implies an obligation to pay. If placing an order entails activating a button or a similar function, the button or similar function shall be labelled in an easily legible manner only with the words 'order with obligation to pay' or a corresponding unambiguous formulation indicating that placing the order entails an obligation to pay the trader. If the trader has not complied with this subparagraph, the consumer shall not be bound by the contract or order.

3. Trading websites shall indicate clearly and legibly at the latest at the beginning of the ordering process whether any delivery restrictions apply and which means of payment are accepted.

4. If the contract is concluded through a means of distance communication which allows limited space or time to display the information, the trader shall provide, on that particular means prior to the conclusion of such a contract, at least the pre-contractual information regarding the main characteristics of the goods or services, the identity of the trader, the total price, the right of withdrawal, the duration of the contract and, if the contract is of indeterminate duration, the conditions for terminating the contract, as referred to in points (a), (b), (e), (h) and (o) of Article 6(1). The other information referred to in Article 6(1) shall be provided by the trader to the consumer in an appropriate way in accordance with paragraph 1 of this Article.

5. Without prejudice to paragraph 4, if the trader makes a telephone call to the consumer with a view to concluding a distance contract, he shall, at the beginning of the conversation with the consumer, disclose his identity and, where applicable, the identity of the person on whose behalf he makes that call, and the commercial purpose of the call.

6. Where a distance contract is to be concluded by telephone, Member States may provide that the trader has to confirm the offer to the consumer who is bound only once he has signed the offer or has sent his written consent. Member States may also provide that such confirmations have to be made on a durable medium.

7. The trader shall provide the consumer with the confirmation of the contract concluded, on a durable medium within a reasonable time after the conclusion of the distance contract, and at the latest at the time of the delivery of the goods or before the performance of the service begins. That confirmation shall include:

(a) all the information referred to in Article 6(1) unless the trader has already provided that information to the consumer on a durable medium prior to the conclusion of the distance contract; and

(b) where applicable, the confirmation of the consumer's prior express consent and acknowledgment in accordance with point (m) of Article 16.

8. Where a consumer wants the performance of services, or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating, to begin during the withdrawal period provided for in Article 9(2), the trader shall require that the consumer make an express request.

9. This Article shall be without prejudice to the provisions on the conclusion of e-contracts and the placing of e-orders set out in Articles 9 and 11 of Directive 2000/31/EC.

10. Member States shall not impose any further formal pre-contractual information requirements for the fulfilment of the information obligations laid down in this Directive.

Article 9

Right of withdrawal

1. Save where the exceptions provided for in Article 16 apply, the consumer shall have a period of 14 days to withdraw from a distance or off-premises contract, without giving any reason, and without incurring any costs other than those provided for in Article 13(2) and Article 14.

2. Without prejudice to Article 10, the withdrawal period referred to in paragraph 1 of this Article shall expire after 14 days from:

(a) in the case of service contracts, the day of the conclusion of the contract;

(b) in the case of sales contracts, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the goods or:

(i) in the case of multiple goods ordered by the consumer in one order and delivered separately, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the last good;

(ii) in the case of delivery of a good consisting of multiple lots or pieces, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the last lot or piece;

(iii) in the case of contracts for regular delivery of goods during defined period of time, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the first good;

(c) in the case of contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium, the day of the conclusion of the contract.

3. The Member States shall not prohibit the contracting parties from performing their contractual obligations during the withdrawal period. Nevertheless, in the case of off-premises contracts, Member States may maintain existing national legislation prohibiting the trader from collecting the payment from the consumer during the given period after the conclusion of the contract.

Article 10

Omission of information on the right of withdrawal

1. If the trader has not provided the consumer with the information on the right of withdrawal as required by point (h) of Article 6(1), the withdrawal period shall expire 12 months from the end of the initial withdrawal period, as determined in accordance with Article 9(2).

2. If the trader has provided the consumer with the information provided for in paragraph 1 of this Article within

12 months from the day referred to in Article 9(2), the withdrawal period shall expire 14 days after the day upon which the consumer receives that information.

Article 11

Exercise of the right of withdrawal

1. Before the expiry of the withdrawal period, the consumer shall inform the trader of his decision to withdraw from the contract. For this purpose, the consumer may either:

(a) use the model withdrawal form as set out in Annex I(B); or

(b) make any other unequivocal statement setting out his decision to withdraw from the contract.

Member States shall not provide for any formal requirements applicable to the model withdrawal form other than those set out in Annex I(B).

2. The consumer shall have exercised his right of withdrawal within the withdrawal period referred to in Article 9(2) and Article 10 if the communication concerning the exercise of the right of withdrawal is sent by the consumer before that period has expired.

3. The trader may, in addition to the possibilities referred to in paragraph 1, give the option to the consumer to electronically fill in and submit either the model withdrawal form set out in Annex I(B) or any other unequivocal statement on the trader's website. In those cases the trader shall communicate to the consumer an acknowledgement of receipt of such a withdrawal on a durable medium without delay.

4. The burden of proof of exercising the right of withdrawal in accordance with this Article shall be on the consumer.

Article 12

Effects of withdrawal

The exercise of the right of withdrawal shall terminate the obligations of the parties:

(a) to perform the distance or off-premises contract; or

(b) to conclude the distance or off-premises contract, in cases where an offer was made by the consumer.

Article 13

Obligations of the trader in the event of withdrawal

1. The trader shall reimburse all payments received from the consumer, including, if applicable, the costs of delivery without undue delay and in any event not later than 14 days from the day on which he is informed of the consumer's decision to withdraw from the contract in accordance with Article 11.

The trader shall carry out the reimbursement referred to in the first subparagraph using the same means of payment as the consumer used for the initial transaction, unless the consumer has expressly agreed otherwise and provided that the consumer does not incur any fees as a result of such reimbursement.

2. Notwithstanding paragraph 1, the trader shall not be required to reimburse the supplementary costs, if the consumer has expressly opted for a type of delivery other than the least expensive type of standard delivery offered by the trader.

3. Unless the trader has offered to collect the goods himself, with regard to sales contracts, the trader may withhold the reimbursement until he has received the goods back, or until the consumer has supplied evidence of having sent back the goods, whichever is the earliest.

Article 14

Obligations of the consumer in the event of withdrawal

1. Unless the trader has offered to collect the goods himself, the consumer shall send back the goods or hand them over to the trader or to a person authorised by the trader to receive the goods, without undue delay and in any event not later than 14 days from the day on which he has communicated his decision to withdraw from the contract to the trader in

accordance with Article 11. The deadline shall be met if the consumer sends back the goods before the period of 14 days has expired.

The consumer shall only bear the direct cost of returning the goods unless the trader has agreed to bear them or the trader failed to inform the consumer that the consumer has to bear them.

In the case of off-premises contracts where the goods have been delivered to the consumer's home at the time of the conclusion of the contract, the trader shall at his own expense collect the goods if, by their nature, those goods cannot normally be returned by post.

2. The consumer shall only be liable for any diminished value of the goods resulting from the handling of the goods other than what is necessary to establish the nature, characteristics and functioning of the goods. The consumer shall in any event not be liable for diminished value of the goods where the trader has failed to provide notice of the right of withdrawal in accordance with point (h) of Article 6(1).

3. Where a consumer exercises the right of withdrawal after having made a request in accordance with Article 7(3) or Article 8(8), the consumer shall pay to the trader an amount which is in proportion to what has been provided until the time the consumer has informed the trader of the exercise of the right of withdrawal, in comparison with the full coverage of the contract. The proportionate amount to be paid by the consumer to the trader shall be calculated on the basis of the total price agreed in the contract. If the total price is excessive, the proportionate amount shall be calculated on the basis of the market value of what has been provided.

4. The consumer shall bear no cost for:

(a) the performance of services or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating, in full or in part, during the withdrawal period, where:

- (i) the trader has failed to provide information in accordance with points (h) or (j) of Article 6(1); or
- (ii) the consumer has not expressly requested performance to begin during the withdrawal period in accordance with Article 7(3) and Article 8(8); or

(b) the supply, in full or in part, of digital content which is not supplied on a tangible medium where:

- (i) the consumer has not given his prior express consent to the beginning of the performance before the end of the 14-day period referred to in Article 9;
- (ii) the consumer has not acknowledged that he loses his right of withdrawal when giving his consent; or
- (iii) the trader has failed to provide confirmation in accordance with Article 7(2) or Article 8(7).

5. Except as provided for in Article 13(2) and in this Article, the consumer shall not incur any liability as a consequence of the exercise of the right of withdrawal.

Article 15

Effects of the exercise of the right of withdrawal on ancillary contracts

1. Without prejudice to Article 15 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers (20), if the consumer exercises his right of withdrawal from a distance or an off-premises contract in accordance with Articles 9 to 14 of this Directive, any ancillary contracts shall be automatically terminated, without any costs for the consumer, except as provided for in Article 13(2) and in Article 14 of this Directive.

2. The Member States shall lay down detailed rules on the termination of such contracts.

Article 16

Exceptions from the right of withdrawal

Member States shall not provide for the right of withdrawal set out in Articles 9 to 15 in respect of distance and off-premises contracts as regards the following:

(a) service contracts after the service has been fully performed if the performance has begun with the consumer's prior express consent, and with the acknowledgement that he will lose his right of withdrawal once the contract has been fully performed by the trader;

(b) the supply of goods or services for which the price is dependent on fluctuations in the financial market which cannot be controlled by the trader and which may occur within the withdrawal period;

(c) the supply of goods made to the consumer's specifications or clearly personalised;

(d) the supply of goods which are liable to deteriorate or expire rapidly;

(e) the supply of sealed goods which are not suitable for return due to health protection or hygiene reasons and were unsealed after delivery;

(f) the supply of goods which are, after delivery, according to their nature, inseparably mixed with other items;

(g) the supply of alcoholic beverages, the price of which has been agreed upon at the time of the conclusion of the sales contract, the delivery of which can only take place after 30 days and the actual value of which is dependent on fluctuations in the market which cannot be controlled by the trader;

(h) contracts where the consumer has specifically requested a visit from the trader for the purpose of carrying out urgent repairs or maintenance. If, on the occasion of such visit, the trader provides services in addition to those specifically requested by the consumer or goods other than replacement parts necessarily used in carrying out the maintenance or in making the repairs, the right of withdrawal shall apply to those additional services or goods;

(i) the supply of sealed audio or sealed video recordings or sealed computer software which were unsealed after delivery;

(j) the supply of a newspaper, periodical or magazine with the exception of subscription contracts for the supply of such publications;

(k) contracts concluded at a public auction;

(l) the provision of accommodation other than for residential purpose, transport of goods, car rental services, catering or services related to leisure activities if the contract provides for a specific date or period of performance;

(m) the supply of digital content which is not supplied on a tangible medium if the performance has begun with the consumer's prior express consent and his acknowledgment that he thereby loses his right of withdrawal.

CHAPTER IV

OTHER CONSUMER RIGHTS

Article 17

Scope

1. Articles 18 and 20 shall apply to sales contracts. Those Articles shall not apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or the supply of digital content which is not supplied on a tangible medium.

2. Articles 19, 21 and 22 shall apply to sales and service contracts and to contracts for the supply of water, gas, electricity, district heating or digital content.

Article 18

Delivery

1. Unless the parties have agreed otherwise on the time of delivery, the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer without undue delay, but not later than 30 days from the conclusion of the contract.

2. Where the trader has failed to fulfil his obligation to deliver the goods at the time agreed upon with the consumer or within the time limit set out in paragraph 1, the consumer shall call upon him to make the delivery within an additional period of time appropriate to the circumstances. If the trader fails to deliver the goods within that additional period of time, the consumer shall be entitled to terminate the contract.

The first subparagraph shall not be applicable to sales contracts where the trader has refused to deliver the goods or where delivery within the agreed delivery period is essential taking into account all the circumstances attending the conclusion of the contract or where the consumer informs the trader, prior to the conclusion of the contract, that delivery by or on a specified date is essential. In those cases, if the trader fails to deliver the goods at the time agreed upon with the consumer or within the time limit set out in paragraph 1, the consumer shall be entitled to terminate the contract immediately.

3. Upon termination of the contract, the trader shall, without undue delay, reimburse all sums paid under the contract.

4. In addition to the termination of the contract in accordance with paragraph 2, the consumer may have recourse to other remedies provided for by national law.

Article 19

Fees for the use of means of payment

Member States shall prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such means.

Article 20

Passing of risk

In contracts where the trader dispatches the goods to the consumer, the risk of loss of or damage to the goods shall pass to the consumer when he or a third party indicated by the consumer and other than the carrier has acquired the physical possession of the goods. However, the risk shall pass to the consumer upon delivery to the carrier if the carrier was commissioned by the consumer to carry the goods and that choice was not offered by the trader, without prejudice to the rights of the consumer against the carrier.

Article 21

Communication by telephone

Member States shall ensure that where the trader operates a telephone line for the purpose of contacting him by telephone in relation to the contract concluded, the consumer, when contacting the trader is not bound to pay more than the basic rate.

The first subparagraph shall be without prejudice to the right of telecommunication services providers to charge for such calls.

Article 22

Additional payments

Before the consumer is bound by the contract or offer, the trader shall seek the express consent of the consumer to any extra payment in addition to the remuneration agreed upon for the trader's main contractual obligation. If the trader has not obtained the consumer's express consent but has inferred it by using default options which the consumer is required to reject in order to avoid the additional payment, the consumer shall be entitled to reimbursement of this payment.

CHAPTER V

GENERAL PROVISIONS

Article 23

Enforcement

1. Member States shall ensure that adequate and effective means exist to ensure compliance with this Directive.

2. The means referred to in paragraph 1 shall include provisions whereby one or more of the following bodies, as determined by national law, may take action under national law before the courts or before the competent administrative bodies to ensure that the national provisions transposing this Directive are applied:

(a) public bodies or their representatives;

(b) consumer organisations having a legitimate interest in protecting consumers;

(c) professional organisations having a legitimate interest in acting.

Article 24

Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.

2. Member States shall notify those provisions to the Commission by 13 December 2013 and shall notify it without delay of any subsequent amendment affecting them.

Article 25

Imperative nature of the Directive

If the law applicable to the contract is the law of a Member State, consumers may not waive the rights conferred on them by the national measures transposing this Directive.

Any contractual terms which directly or indirectly waive or restrict the rights resulting from this Directive shall not be binding on the consumer.

Article 26

Information

Member States shall take appropriate measures to inform consumers and traders of the national provisions transposing this Directive and shall, where appropriate, encourage traders and code owners as defined in point (g) of Article 2 of Directive 2005/29/EC, to inform consumers of their codes of conduct.

Article 27

Inertia selling

The consumer shall be exempted from the obligation to provide any consideration in cases of unsolicited supply of goods, water, gas, electricity, district heating or digital content or unsolicited provision of services, prohibited by Article 5(5) and point 29 of Annex I to Directive 2005/29/EC. In such cases, the absence of a response from the consumer following such an unsolicited supply or provision shall not constitute consent.

Article 28

Transposition

1. Member States shall adopt and publish, by 13 December 2013, the laws, Regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of these measures in the form of documents. The Commission shall make use of these documents for the purposes of the report referred to in Article 30.

They shall apply those measures from 13 June 2014.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. The provisions of this Directive shall apply to contracts concluded after 13 June 2014.

Article 29

Reporting requirements

1. Where a Member State makes use of any of the regulatory choices referred to in Article 3(4), Article 6(7), Article 6(8), Article 7(4), Article 8(6) and Article 9(3), it shall inform the

Commission thereof by 13 December 2013, as well as of any subsequent changes.

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.

Article 30

Reporting by the Commission and review

By 13 December 2016, the Commission shall submit a report on the application of this Directive to the European Parliament and the Council. That report shall include in particular an evaluation of the provisions of this Directive regarding digital content including the right of withdrawal. The report shall be accompanied, where necessary, by legislative proposals to adapt this Directive to developments in the field of consumer rights.

CHAPTER VI

FINAL PROVISIONS

Article 31

Repeals

Directive 85/577/EEC and Directive 97/7/EC, as amended by Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services (21) and by Directives 2005/29/EC and 2007/64/EC, are repealed as of 13 June 2014.

References to the repealed Directives shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex II.

Article 32

Amendment to Directive 93/13/EEC

In Directive 93/13/EEC, the following Article is inserted:

'Article 8a

1. Where a Member State adopts provisions in accordance with Article 8, it shall inform the Commission thereof, as well as of any subsequent changes, in particular where those provisions:

— extend the unfairness assessment to individually negotiated contractual terms or to the adequacy of the price or remuneration; or,

— contain lists of contractual terms which shall be considered as unfair,

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.'

Article 33

Amendment to Directive 1999/44/EC

In Directive 1999/44/EC, the following Article is inserted:

'Article 8a

Reporting requirements

1. Where, in accordance with Article 8(2), a Member State adopts more stringent consumer protection provisions than those provided for in Article 5(1) to (3) and in Article 7(1), it shall inform the Commission thereof, as well as of any subsequent changes.

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European

Parliament. The Commission shall consult stakeholders on that information.'

Article 34

Entry into force

This Directive shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

Article 35

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 25 October 2011.

For the European Parliament

The President

J. BUZEK

For the Council

The President

M. DOWGIELEWICZ

(1) OJ C 317, 23.12.2009, p. 54.

(2) OJ C 200, 25.8.2009, p. 76.

(3) Position of the European Parliament of 23 June 2011 (not yet published in the Official Journal) and decision of the Council of 10 October 2011.

(4) OJ L 372, 31.12.1985, p. 31.

(5) OJ L 144, 4.6.1997, p. 19.

(6) OJ L 177, 4.7.2008, p. 6.

(7) OJ L 376, 27.12.2006, p. 36.

(8) OJ L 178, 17.7.2000, p. 1.

(9) OJ L 88, 4.4.2011, p. 45.

(10) OJ L 255, 30.9.2005, p. 22.

(11) OJ L 124, 8.6.1971, p. 1.

(12) OJ L 319, 5.12.2007, p. 1.

(13) OJ L 149, 11.6.2005, p. 22.

(14) OJ L 201, 31.7.2002, p. 37.

(15) OJ L 95, 21.4.1993, p. 29.

(16) OJ L 171, 7.7.1999, p. 12.

(17) OJ C 321, 31.12.2003, p. 1.

(18) OJ L 158, 23.6.1990, p. 59.

(19) OJ L 33, 3.2.2009, p. 10.

(20) OJ L 133, 22.5.2008, p. 66.

(21) OJ L 271, 9.10.2002, p. 16.

ANNEX I

Information concerning the exercise of the right of withdrawal

A. Model instructions on withdrawal

Right of withdrawal

You have the right to withdraw from this contract within 14 days without giving any reason.

The withdrawal period will expire after 14 days from the day

To exercise the right of withdrawal, you must inform us () of your decision to withdraw from this contract by an unequivocal statement (e.g. a letter sent by post, fax or e-mail). You may use the attached model withdrawal form, but it is not obligatory.

To meet the withdrawal deadline, it is sufficient for you to send your communication concerning your exercise of the right of withdrawal before the withdrawal period has expired.

Effects of withdrawal

If you withdraw from this contract, we shall reimburse to you all payments received from you, including the costs of delivery (with the exception of the supplementary costs resulting from your choice of a type of delivery other than the least expensive type of standard delivery offered by us), without undue delay and in any event not later than 14 days from the day on which we are informed about your decision to withdraw from this contract. We will carry out such reimbursement using the same means of payment as you used for the initial transaction, unless you have expressly agreed otherwise; in any event, you will not incur any fees as a result of such reimbursement.

Instructions for completion:

Insert one of the following texts between inverted commas:

(a)
in the case of a service contract or a contract for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium: 'of the conclusion of the contract.';

(b)
in the case of a sales contract: 'on which you acquire, or a third party other than the carrier and indicated by you acquires, physical possession of the goods.';

(c)
in the case of a contract relating to multiple goods ordered by the consumer in one order and delivered separately: 'on which you acquire, or a third party other than the carrier and indicated by you acquires, physical possession of the last good.';

(d)
in the case of a contract relating to delivery of a good consisting of multiple lots or pieces: 'on which you acquire, or a third party other than the carrier and indicated by you acquires, physical possession of the last lot or piece.';

(e)
in the case of a contract for regular delivery of goods during a defined period of time: 'on which you acquire, or a third party other than the carrier and indicated by you acquires, physical possession of the first good.'.

Insert your name, geographical address and, where available, your telephone number, fax number and e-mail address.

If you give the option to the consumer to electronically fill in and submit information about his withdrawal from the contract on your website, insert the following: 'You can also electronically fill in and submit the model withdrawal form or any other unequivocal statement on our website [insert Internet address]. If you use this option, we will communicate to you an acknowledgement of receipt of such a withdrawal on a durable medium (e.g. by e-mail) without delay.'

In the case of sales contracts in which you have not offered to collect the goods in the event of withdrawal insert the following: 'We may withhold reimbursement until we have received the goods back or you have supplied evidence of having sent back the goods, whichever is the earliest.'

If the consumer has received goods in connection with the contract:

(a)
insert:

—
'We will collect the goods.'; or,

—
'You shall send back the goods or hand them over to us or ... [insert the name and geographical address, where applicable, of the person authorised by you to receive the goods], without undue delay and in any event not later than 14 days from the day on which you communicate your withdrawal from this contract to us. The deadline is met if you send back the goods before the period of 14 days has expired.'

ANNEX II

(b)
insert:

—
'We will bear the cost of returning the goods.';

—
'You will have to bear the direct cost of returning the goods.';

—
If, in a distance contract, you do not offer to bear the cost of returning the goods and the goods, by their nature, cannot normally be returned by post: 'You will have to bear the direct cost of returning the goods, ... EUR [insert the amount].'; or if the cost of returning the goods cannot reasonably be calculated in advance: 'You will have to bear the direct cost of returning the goods. The cost is estimated at a maximum of approximately ... EUR [insert the amount].'; or

—
If, in an off-premises contract, the goods, by their nature, cannot normally be returned by post and have been delivered to the consumer's home at the time of the conclusion of the contract: 'We will collect the goods at our own expense.'; and,

(c)
insert 'You are only liable for any diminished value of the goods resulting from the handling other than what is necessary to establish the nature, characteristics and functioning of the goods.'

In the case of a contract for the provision of services or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating, insert the following: 'If you requested to begin the performance of services or the supply of water/gas/electricity/district heating [delete where inapplicable] during the withdrawal period, you shall pay us an amount which is in proportion to what has been provided until you have communicated us your withdrawal from this contract, in comparison with the full coverage of the contract.'

B. Model withdrawal form

—
To [here the trader's name, geographical address and, where available, his fax number and e-mail address are to be inserted by the trader]:

—
I/We (1) hereby give notice that I/We (1) withdraw from my/our (1) contract of sale of the following goods (1)/for the provision of the following service (1),

—
Ordered on (1)/received on (1),

—
Name of consumer(s),

—
Address of consumer(s),

—
Signature of consumer(s) (only if this form is notified on paper),

—
Date

(1) Delete as appropriate.

ANNEX II

Correlation table

Directive 85/577/EEC	Directive 97/7/EC	This Directive
Article 1		Article 3 read in conjunction with Article 2, points 8 and 9, and Article 16, point (h)
	Article 1	Article 1 read in conjunction with Article 2, point 7
Article 2		Article 2, points 1 and 2
	Article 2, point 1	Article 2, point 7

	Article 2, point 2	Article 2, point 1
	Article 2, point 3	Article 2, point 2
	Article 2, point 4, first sentence	Article 2, point 7
	Article 2, point 4, second sentence	—
	Article 2, point 5	—
Article 3(1)		Article 3(4)
Article 3(2), point (a)		Article 3(3), points (e) and (f)
Article 3(2), point (b)		Article 3(3), point (j)
Article 3(2), point (c)		—
Article 3(2), point (d)		Article 3(3), point (d)
Article 3(2), point (e)		Article 3(3), point (d)
Article 3(3)		—
	Article 3(1), first indent	Article 3(3), point (d)
	Article 3(1), second indent	Article 3(3), point (l)
	Article 3(1), third indent	Article 3(3), point (m)
	Article 3(1), fourth indent	Article 3(3), points (e) and (f)
	Article 3(1), fifth indent	Article 6(3) and Article 16, point (k) read in conjunction with Article 2, point 13
	Article 3(2), first indent	Article 3(3), point (j)
	Article 3(2), second indent	Article 3(3), point (f) (for rental of accommodation for residential purposes), point (g) (for package travel), point (h) (for timeshare), point (k) (for passenger transport with some exceptions) and Article 16, point (l) (exemption from the right of withdrawal)
Article 4, first sentence		Article 6(1), points (b), (c) and (h), and Article 7(1) and (2)
Article 4, second sentence		Article 6(1), point a and Article 7(1)
Article 4, third sentence		Article 6(1)
Article 4, fourth sentence		Article 10
	Article 4(1), point (a)	Article 6(1), points (b) and (c)
	Article 4(1), point (b)	Article 6(1), point (a)
	Article 4(1), point (c)	Article 6(1), point (e)
	Article 4(1), point (d)	Article 6(1), point (e)
	Article 4(1), point (e)	Article 6(1), point (g)
	Article 4(1), point (f)	Article 6(1), point (h)
	Article 4(1), point (g)	Article 6(1), point (f)
	Article 4(1), point (h)	—
	Article 4(1), point (i)	Article 6(1), points (o) and (p)
	Article 4(2)	Article 6(1) read in conjunction with Article 8(1), (2) and (4)

	Article 4(3)	Article 8(5)
	Article 5(1)	Article 8(7)
	Article 5(2)	Article 3(3), point m
	Article 6(1)	Article 9(1) and (2), Article 10, Article 13(2), Article 14
	Article 6(2)	Article 13 and Article 14(1), second and third subparagraphs
	Article 6(3), first indent	Article 16, point (a)
	Article 6(3), second indent	Article 16, point (b)
	Article 6(3), third indent	Article 16, point (c) and (d)
	Article 6(3), fourth indent	Article 16, point (i)
	Article 6(3), fifth indent	Article 16, point (j)
	Article 6(3), sixth indent	Article 3(3), point (c)
	Article 6(4)	Article 15
	Article 7(1)	Article 18(1) (for sales contracts)
	Article 7(2)	Article 18(2), (3) and (4)
	Article 7(3)	—
	Article 8	—
	Article 9	Article 27
	Article 10	— (but see Article 13 of Directive 2002/58/EC)
	Article 11(1)	Article 23(1)
	Article 11(2)	Article 23(2)
	Article 11(3), point (a)	Article 6(9) for the burden of proof concerning pre-contractual information; for the rest: —
	Article 11(3), point (b)	Article 24(1)
	Article 11(4)	—
	Article 12(1)	Article 25
	Article 12(2)	—
	Article 13	Article 3(2)
	Article 14	Article 4
	Article 15(1)	Article 28(1)
	Article 15(2)	Article 28(1)
	Article 15(3)	Article 28(1)
	Article 15(4)	Article 30
	Article 16	Article 26
	Article 17	—
	Article 18	Article 34
	Article 19	Article 35
Article 5(1)		Articles 9 and 11
Article 5(2)		Article 12
Article 6		Article 25
Article 7		Articles 13, 14 and 15
Article 8		Article 4

Annex to Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation) ⁽¹⁾	To be construed as a reference to
Paragraphs 2 and 11	This Directive

Directive 2013/11/EU of the European parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission, After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Article 169(1) and point (a) of Article 169(2) of the Treaty on the Functioning of the European Union (TFEU) provide that the Union is to contribute to the attainment of a high level of consumer protection through measures adopted pursuant to Article 114 TFEU. Article 38 of the Charter of Fundamental Rights of the European Union provides that Union policies are to ensure a high level of consumer protection.

(2) In accordance with Article 26(2) TFEU, the internal market is to comprise an area without internal frontiers in which the free movement of goods and services is ensured. The internal market should provide consumers with added value in the form of better quality, greater variety, reasonable prices and high safety standards for goods and services, which should promote a high level of consumer protection.

(3) Fragmentation of the internal market is detrimental to competitiveness, growth and job creation within the Union. Eliminating direct and indirect obstacles to the proper functioning of the internal market and improving citizens' trust is essential for the completion of the internal market.

(4) Ensuring access to simple, efficient, fast and low-cost ways of resolving domestic and cross-border disputes which arise from sales or service contracts should benefit consumers and therefore boost their confidence in the market. That access should apply to online as well as to offline transactions, and is particularly important when consumers shop across borders.

(5) Alternative dispute resolution (ADR) offers a simple, fast and low-cost out-of-court solution to disputes between consumers and traders. However, ADR is not yet sufficiently and consistently developed across the Union. It is regrettable that, despite Commission Recommendations 98/257/EC of 30 March 1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes (3) and 2001/310/EC of 4 April 2001 on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes (4), ADR has not been correctly established and is not running satisfactorily in all geographical areas or business sectors in the Union. Consumers and traders are still not aware of the existing out-of-court redress mechanisms, with only a small percentage of citizens knowing how to file a complaint with an ADR entity. Where ADR procedures are available, their quality levels vary considerably in the Member States and cross-border disputes are often not handled effectively by ADR entities.

(6) The disparities in ADR coverage, quality and awareness in Member States constitute a barrier to the internal market and are among the reasons why many consumers abstain from shopping across borders and why they lack confidence that potential disputes with traders can be resolved in an easy, fast and inexpensive way. For the same reasons, traders might abstain from selling to consumers in other Member States

where there is no sufficient access to high-quality ADR procedures. Furthermore, traders established in a Member State where high-quality ADR procedures are not sufficiently available are put at a competitive disadvantage with regard to traders that have access to such procedures and can thus resolve consumer disputes faster and more cheaply.

(7) In order for consumers to exploit fully the potential of the internal market, ADR should be available for all types of domestic and cross-border disputes covered by this Directive, ADR procedures should comply with consistent quality requirements that apply throughout the Union, and consumers and traders should be aware of the existence of such procedures. Due to increased cross-border trade and movement of persons, it is also important that ADR entities handle cross-border disputes effectively.

(8) As advocated by the European Parliament in its resolutions of 25 October 2011 on alternative dispute resolution in civil, commercial and family matters and of 20 May 2010 on delivering a single market to consumers and citizens, any holistic approach to the single market which delivers results for its citizens should as a priority develop simple, affordable, expedient and accessible system of redress.

(9) In its Communication of 13 April 2011 entitled 'Single Market Act — Twelve levers to boost growth and strengthen confidence — "Working together to create new growth"', the Commission identified legislation on ADR which includes an electronic commerce (e-commerce) dimension, as one of the twelve levers to boost growth, strengthen confidence and make progress towards completing the Single Market.

(10) In its conclusions of 24-25 March and 23 October 2011, the European Council invited the European Parliament and the Council to adopt, by the end of 2012, a first set of priority measures to bring a new impetus to the Single Market. Moreover, in its Conclusions of 30 May 2011 on the Priorities for relaunching the Single Market, the Council of the European Union highlighted the importance of e-commerce and agreed that consumer ADR schemes can offer low-cost, simple and quick redress for both consumers and traders. The successful implementation of those schemes requires sustained political commitment and support from all actors, without compromising the affordability, transparency, flexibility, speed and quality of decision-making by the ADR entities falling within the scope of this Directive.

(11) Given the increasing importance of online commerce and in particular cross-border trade as a pillar of Union economic activity, a properly functioning ADR infrastructure for consumer disputes and a properly integrated online dispute resolution (ODR) framework for consumer disputes arising from online transactions are necessary in order to achieve the Single Market Act's aim of boosting citizens' confidence in the internal market.

(12) This Directive and Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes (5) are two interlinked and complementary legislative instruments. Regulation (EU) No 524/2013 provides for the establishment of an ODR platform which offers consumers and traders a single point of entry for the out-of-court resolution of online disputes, through ADR entities which are linked to the platform and offer ADR through quality ADR procedures. The availability of quality ADR entities across the Union is thus a precondition for the proper functioning of the ODR platform.

(13) This Directive should not apply to non-economic services of general interest. Non-economic services are services which are not performed for economic consideration. As a result, non-economic services of general interest performed by the State or on behalf of the State, without remuneration, should not be covered by this Directive irrespective of the legal form through which those services are provided.

(14) This Directive should not apply to health care services as defined in point (a) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (6).

(15) The development within the Union of properly functioning ADR is necessary to strengthen consumers' confidence in the internal market, including in the area of online commerce, and to fulfil the potential for and opportunities of cross-border and online trade. Such development should build on existing ADR procedures in the Member States and respect their legal traditions. Both existing and newly established properly functioning dispute resolution entities that comply with the quality requirements set out in this Directive should be considered as 'ADR entities' within the meaning of this Directive. The dissemination of ADR can also prove to be important in those Member States in which there is a substantial backlog of cases pending before the courts, preventing Union citizens from exercising their right to a fair trial within a reasonable time.

(16) This Directive should apply to disputes between consumers and traders concerning contractual obligations stemming from sales or services contracts, both online and offline, in all economic sectors, other than the exempted sectors. This should include disputes arising from the sale or provision of digital content for remuneration. This Directive should apply to complaints submitted by consumers against traders. It should not apply to complaints submitted by traders against consumers or to disputes between traders. However, it should not prevent Member States from adopting or maintaining in force provisions on procedures for the out-of-court resolution of such disputes.

(17) Member States should be permitted to maintain or introduce national provisions with regard to procedures not covered by this Directive, such as internal complaint handling procedures operated by the trader. Such internal complaint handling procedures can constitute an effective means for resolving consumer disputes at an early stage.

(18) The definition of 'consumer' should cover natural persons who are acting outside their trade, business, craft or profession. However, if the contract is concluded for purposes partly within and partly outside the person's trade (dual purpose contracts) and the trade purpose is so limited as not to be predominant in the overall context of the supply, that person should also be considered as a consumer.

(19) Some existing Union legal acts already contain provisions concerning ADR. In order to ensure legal certainty, it should be provided that, in the event of conflict, this Directive is to prevail, except where it explicitly provides otherwise. In particular, this Directive should be without prejudice to Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters (7), which already sets out a framework for systems of mediation at Union level for cross-border disputes, without preventing the application of that Directive to internal mediation systems. This Directive is intended to apply horizontally to all types of ADR procedures, including to ADR procedures covered by Directive 2008/52/EC.

(20) ADR entities are highly diverse across the Union but also within the Member States. This Directive should cover any entity that is established on a durable basis, offers the resolution of a dispute between a consumer and a trader through an ADR procedure and is listed in accordance with this Directive. This Directive may also cover, if Member States so decide, dispute resolution entities which impose solutions which are binding on the parties. However, an out-of-court procedure which is created on an ad hoc basis for a single

dispute between a consumer and a trader should not be considered as an ADR procedure.

(21) Also ADR procedures are highly diverse across the Union and within Member States. They can take the form of procedures where the ADR entity brings the parties together with the aim of facilitating an amicable solution, or procedures where the ADR entity proposes a solution or procedures where the ADR entity imposes a solution. They can also take the form of a combination of two or more such procedures. This Directive should be without prejudice to the form which ADR procedures take in the Member States.

(22) Procedures before dispute resolution entities where the natural persons in charge of dispute resolution are employed or receive any form of remuneration exclusively from the trader are likely to be exposed to a conflict of interest. Therefore, those procedures should, in principle, be excluded from the scope of this Directive, unless a Member State decides that such procedures can be recognised as ADR procedures under this Directive and provided that those entities are in complete conformity with the specific requirements on independence and impartiality laid down in this Directive. ADR entities offering dispute resolution through such procedures should be subject to regular evaluation of their compliance with the quality requirements set out in this Directive, including the specific additional requirements ensuring their independence.

(23) This Directive should not apply to procedures before consumer-complaint handling systems operated by the trader, nor to direct negotiations between the parties. Furthermore, it should not apply to attempts made by a judge to settle a dispute in the course of a judicial proceeding concerning that dispute.

(24) Member States should ensure that disputes covered by this Directive can be submitted to an ADR entity which complies with the requirements set out in this Directive and is listed in accordance with it. Member States should have the possibility of fulfilling this obligation by building on existing properly functioning ADR entities and adjusting their scope of application, if needed, or by providing for the creation of new ADR entities. This Directive should not preclude the functioning of existing dispute resolution entities operating within the framework of national consumer protection authorities of Member States where State officials are in charge of dispute resolution. State officials should be regarded as representatives of both consumers' and traders' interests. This Directive should not oblige Member States to create a specific ADR entity in each retail sector. When necessary, in order to ensure full sectoral and geographical coverage by and access to ADR, Member States should have the possibility to provide for the creation of a residual ADR entity that deals with disputes for the resolution of which no specific ADR entity is competent. Residual ADR entities are intended to be a safeguard for consumers and traders by ensuring that there are no gaps in access to an ADR entity.

(25) This Directive should not prevent Member States from maintaining or introducing legislation on procedures for out-of-court resolution of consumer contractual disputes which is in compliance with the requirements set out in this Directive. Furthermore, in order to ensure that ADR entities can operate effectively, those entities should have the possibility of maintaining or introducing, in accordance with the laws of the Member State in which they are established, procedural rules that allow them to refuse to deal with disputes in specific circumstances, for example where a dispute is too complex and would therefore be better resolved in court. However, procedural rules allowing ADR entities to refuse to deal with a dispute should not impair significantly consumers' access to ADR procedures, including in the case of cross-border disputes. Thus, when providing for a monetary threshold, Member States should always take into account that the real value of a dispute may vary among Member States and, consequently, setting a disproportionately high threshold in one Member State could impair access to ADR procedures for consumers from other Member States. Member States should not be required to ensure that the consumer can submit his complaint to another ADR entity, where an ADR entity to which the complaint was

first submitted has refused to deal with it because of its procedural rules. In such cases Member States should be deemed to have fulfilled their obligation to ensure full coverage of ADR entities.

(26) This Directive should allow traders established in a Member State to be covered by an ADR entity which is established in another Member State. In order to improve the coverage of and consumer access to ADR across the Union, Member States should have the possibility of deciding to rely on ADR entities established in another Member State or regional, transnational or pan-European ADR entities, where traders from different Member States are covered by the same ADR entity. Recourse to ADR entities established in another Member State or to transnational or pan-European ADR entities should, however, be without prejudice to Member States' responsibility to ensure full coverage by and access to ADR entities.

(27) This Directive should be without prejudice to Member States maintaining or introducing ADR procedures dealing jointly with identical or similar disputes between a trader and several consumers. Comprehensive impact assessments should be carried out on collective out-of-court settlements before such settlements are proposed at Union level. The existence of an effective system for collective claims and easy recourse to ADR should be complementary and they should not be mutually exclusive procedures.

(28) The processing of information relating to disputes covered by this Directive should comply with the rules on the protection of personal data laid down in the laws, Regulations and administrative provisions of the Member States adopted pursuant to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (8).

(29) Confidentiality and privacy should be respected at all times during the ADR procedure. Member States should be encouraged to protect the confidentiality of ADR procedures in any subsequent civil or commercial judicial proceedings or arbitration.

(30) Member States should nevertheless ensure that ADR entities make publicly available any systematic or significant problems that occur frequently and lead to disputes between consumers and traders. The information communicated in this regard could be accompanied by recommendations as to how such problems can be avoided or resolved in future, in order to raise traders' standards and to facilitate the exchange of information and best practices.

(31) Member States should ensure that ADR entities resolve disputes in a manner that is fair, practical and proportionate to both the consumer and the trader, on the basis of an objective assessment of the circumstances in which the complaint is made and with due regard to the rights of the parties.

(32) The independence and integrity of ADR entities is crucial in order to gain Union citizens' trust that ADR mechanisms will offer them a fair and independent outcome. The natural person or collegial body in charge of ADR should be independent of all those who might have an interest in the outcome and should have no conflict of interest which could impede him or it from reaching a decision in a fair, impartial and independent manner.

(33) The natural persons in charge of ADR should only be considered impartial if they cannot be subject to pressure that potentially influences their attitude towards the dispute. In order to ensure the independence of their actions, those persons should also be appointed for a sufficient duration, and should not be subject to any instructions from either party or their representative.

(34) In order to ensure the absence of any conflict of interest, natural persons in charge of ADR should disclose any circumstances that might affect their independence and impartiality or give rise to a conflict of interest with either party to the dispute they are asked to resolve. This could be any financial interest, direct or indirect, in the outcome of the ADR procedure or any personal or business relationship with one or more of the parties during the three years prior to assuming the

post, including any capacity other than for the purposes of ADR in which the person concerned has acted for one or more of the parties, for a professional organisation or a business association of which one of the parties is a member or for any other member thereof.

(35) There is a particular need to ensure the absence of such pressure where the natural persons in charge of ADR are employed or receive any form of remuneration from the trader. Therefore, specific requirements should be provided for in the event that Member States decide to allow dispute resolution procedures in such cases to qualify as ADR procedures under this Directive. Where natural persons in charge of ADR are employed or receive any form of remuneration exclusively from a professional organisation or a business association of which the trader is a member, they should have at their disposal a separate and dedicated budget sufficient to fulfil their tasks.

(36) It is essential for the success of ADR, in particular in order to ensure the necessary trust in ADR procedures, that the natural persons in charge of ADR possess the necessary expertise, including a general understanding of law. In particular, those persons should have sufficient general knowledge of legal matters in order to understand the legal implications of the dispute, without being obliged to be a qualified legal professional.

(37) The applicability of certain quality principles to ADR procedures strengthens both consumers' and traders' confidence in such procedures. Such quality principles were first developed at Union level in Recommendations 98/257/EC and 2001/310/EC. By making some of the principles established in those Commission Recommendations binding, this Directive establishes a set of quality requirements which apply to all ADR procedures carried out by an ADR entity which has been notified to the Commission.

(38) This Directive should establish quality requirements of ADR entities, which should ensure the same level of protection and rights for consumers in both domestic and cross-border disputes. This Directive should not prevent Member States from adopting or maintaining rules that go beyond what is provided for in this Directive.

(39) ADR entities should be accessible and transparent. In order to ensure the transparency of ADR entities and of ADR procedures it is necessary that the parties receive the clear and accessible information they need in order to take an informed decision before engaging in an ADR procedure. The provision of such information to traders should not be required where their participation in ADR procedures is mandatory under national law.

(40) A properly functioning ADR entity should conclude online and offline dispute resolution proceedings expeditiously within a timeframe of 90 calendar days starting on the date on which the ADR entity has received the complete complaint file including all relevant documentation pertaining to that complaint, and ending on the date on which the outcome of the ADR procedure is made available. The ADR entity which has received a complaint should notify the parties after receiving all the documents necessary to carry out the ADR procedure. In certain exceptional cases of a highly complex nature, including where one of the parties is unable, on justified grounds, to take part in the ADR procedure, ADR entities should be able to extend the timeframe for the purpose of undertaking an examination of the case in question. The parties should be informed of any such extension, and of the expected approximate length of time that will be needed for the conclusion of the dispute.

(41) ADR procedures should preferably be free of charge for the consumer. In the event that costs are applied, the ADR procedure should be accessible, attractive and inexpensive for consumers. To that end, costs should not exceed a nominal fee.

(42) ADR procedures should be fair so that the parties to a dispute are fully informed about their rights and the consequences of the choices they make in the context of an ADR procedure. ADR entities should inform consumers of their rights before they agree to or follow a proposed solution. Both

parties should also be able to submit their information and evidence without being physically present.

(43) An agreement between a consumer and a trader to submit complaints to an ADR entity should not be binding on the consumer if it was concluded before the dispute has materialised and if it has the effect of depriving the consumer of his right to bring an action before the courts for the settlement of the dispute. Furthermore, in ADR procedures which aim at resolving the dispute by imposing a solution, the solution imposed should be binding on the parties only if they were informed of its binding nature in advance and specifically accepted this. Specific acceptance by the trader should not be required if national rules provide that such solutions are binding on traders.

(44) In ADR procedures which aim at resolving the dispute by imposing a solution on the consumer, in a situation where there is no conflict of laws, the solution imposed should not result in the consumer being deprived of the protection afforded to him by the provisions that cannot be derogated from by agreement by virtue of the law of the Member State where the consumer and the trader are habitually resident. In a situation involving a conflict of laws, where the law applicable to the sales or service contract is determined in accordance with Article 6(1) and (2) of Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (9), the solution imposed by the ADR entity should not result in the consumer being deprived of the protection afforded to him by the provisions that cannot be derogated from by agreement by virtue of the law of the Member State in which the consumer is habitually resident. In a situation involving a conflict of laws, where the law applicable to the sales or service contract is determined in accordance with Article 5(1) to (3) of the Rome Convention of 19 June 1980 on the law applicable to contractual obligations (10), the solution imposed by the ADR entity should not result in the consumer being deprived of the protection afforded to the consumer by the mandatory rules of the law of the Member State in which the consumer is habitually resident.

(45) The right to an effective remedy and the right to a fair trial are fundamental rights laid down in Article 47 of the Charter of Fundamental Rights of the European Union. Therefore, ADR procedures should not be designed to replace court procedures and should not deprive consumers or traders of their rights to seek redress before the courts. This Directive should not prevent parties from exercising their right of access to the judicial system. In cases where a dispute could not be resolved through a given ADR procedure whose outcome is not binding, the parties should subsequently not be prevented from initiating judicial proceedings in relation to that dispute. Member States should be free to choose the appropriate means to achieve this objective. They should have the possibility to provide, inter alia, that limitation or prescription periods do not expire during an ADR procedure.

(46) In order to function efficiently, ADR entities should have sufficient human, material and financial resources at their disposal. Member States should decide on an appropriate form of funding for ADR entities on their territories, without restricting the funding of entities that are already operational. This Directive should be without prejudice to the question of whether ADR entities are publicly or privately funded or funded through a combination of public and private funding. However, ADR entities should be encouraged to specifically consider private forms of funding and to utilise public funds only at Member States' discretion. This Directive should not affect the possibility for businesses or for professional organisations or business associations to fund ADR entities.

(47) When a dispute arises it is necessary that consumers are able to identify quickly which ADR entities are competent to deal with their complaint and to know whether or not the trader concerned will participate in proceedings submitted to an ADR entity. Traders who commit to use ADR entities to resolve disputes with consumers should inform consumers of the address and website of the ADR entity or entities by which they are covered. That information should be provided in a

clear, comprehensible and easily accessible way on the trader's website, where one exists, and if applicable in the general terms and conditions of sales or service contracts between the trader and the consumer. Traders should have the possibility of including on their websites, and in the terms and conditions of the relevant contracts, any additional information on their internal complaint handling procedures or on any other ways of directly contacting them with a view to settling disputes with consumers without referring them to an ADR entity. Where a dispute cannot be settled directly, the trader should provide the consumer, on paper or another durable medium, with the information on relevant ADR entities and specify if he will make use of them.

(48) The obligation on traders to inform consumers about the ADR entities by which those traders are covered should be without prejudice to provisions on consumer information on out-of-court redress procedures contained in other Union legal acts, which should apply in addition to the relevant information obligation provided for in this Directive.

(49) This Directive should not require the participation of traders in ADR procedures to be mandatory or the outcome of such procedures to be binding on traders, when a consumer has lodged a complaint against them. However, in order to ensure that consumers have access to redress and that they are not obliged to forego their claims, traders should be encouraged as far as possible to participate in ADR procedures. Therefore, this Directive should be without prejudice to any national rules making the participation of traders in such procedures mandatory or subject to incentives or sanctions or making their outcome binding on traders, provided that such legislation does not prevent the parties from exercising their right of access to the judicial system as provided for in Article 47 of the Charter of Fundamental Rights of the European Union.

(50) In order to avoid an unnecessary burden being placed on ADR entities, Member States should encourage consumers to contact the trader in an effort to solve the problem bilaterally before submitting a complaint to an ADR entity. In many cases, doing so would allow consumers to settle their disputes swiftly and at an early stage.

(51) Member States should involve the representatives of professional organisations, business associations and consumer organisations when developing ADR, in particular in relation to the principles of impartiality and independence.

(52) Member States should ensure that ADR entities cooperate on the resolution of cross-border disputes.

(53) Networks of ADR entities, such as the financial dispute resolution network 'FIN-NET' in the area of financial services, should be strengthened within the Union. Member States should encourage ADR entities to become part of such networks.

(54) Close cooperation between ADR entities and national authorities should strengthen the effective application of Union legal acts on consumer protection. The Commission and the Member States should facilitate cooperation between the ADR entities, in order to encourage the exchange of best practice and technical expertise and to discuss any problems arising from the operation of ADR procedures. Such cooperation should be supported, inter alia, through the Union's forthcoming Consumer Programme.

(55) In order to ensure that ADR entities function properly and effectively, they should be closely monitored. For that purpose, each Member States should designate a competent authority or competent authorities which should perform that function. The Commission and competent authorities under this Directive should publish and update a list of ADR entities that comply with this Directive. Member States should ensure that ADR entities, the European Consumer Centre Network, and, where appropriate, the bodies designated in accordance with this Directive publish that list on their website by providing a link to the Commission's website, and whenever possible on a durable medium at their premises. Furthermore, Member States should also encourage relevant consumer organisations and business associations to publish the list. Member States

should also ensure the appropriate dissemination of information on what consumers should do if they have a dispute with a trader. In addition, competent authorities should publish regular reports on the development and functioning of ADR entities in their Member States. ADR entities should notify to competent authorities specific information on which those reports should be based. Member States should encourage ADR entities to provide such information using Commission Recommendation 2010/304/EU of 12 May 2010 on the use of a harmonised methodology for classifying and reporting consumer complaints and enquiries (11).

(56) It is necessary for Member States to lay down rules on penalties for infringements of the national provisions adopted to comply with this Directive and to ensure that those rules are implemented. The penalties should be effective, proportionate and dissuasive.

(57) Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation) (12) should be amended to include a reference to this Directive in its Annex so as to reinforce cross-border cooperation on enforcement of this Directive.

(58) Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (13) (Injunctions Directive) should be amended to include a reference to this Directive in its Annex so as to ensure that the consumers' collective interests laid down in this Directive are protected.

(59) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents (14), Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a Directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(60) Since the objective of this Directive, namely to contribute, through the achievement of a high level of consumer protection and without restricting consumers' access to the courts, to the proper functioning of the internal market, cannot be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(61) This Directive respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and specifically Articles 7, 8, 38 and 47 thereof.

(62) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (15) and delivered an opinion on 12 January 2012 (16),

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Subject matter

The purpose of this Directive is, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market by ensuring that consumers can, on a voluntary basis, submit complaints against traders to entities offering independent, impartial, transparent, effective,

fast and fair alternative dispute resolution procedures. This Directive is without prejudice to national legislation making participation in such procedures mandatory, provided that such legislation does not prevent the parties from exercising their right of access to the judicial system.

Article 2

Scope

1. This Directive shall apply to procedures for the out-of-court resolution of domestic and cross-border disputes concerning contractual obligations stemming from sales contracts or service contracts between a trader established in the Union and a consumer resident in the Union through the intervention of an ADR entity which proposes or imposes a solution or brings the parties together with the aim of facilitating an amicable solution.

2. This Directive shall not apply to:

- (a) procedures before dispute resolution entities where the natural persons in charge of dispute resolution are employed or remunerated exclusively by the individual trader, unless Member States decide to allow such procedures as ADR procedures under this Directive and the requirements set out in Chapter II, including the specific requirements of independence and transparency set out in Article 6(3), are met;
- (b) procedures before consumer complaint-handling systems operated by the trader;
- (c) non-economic services of general interest;
- (d) disputes between traders;
- (e) direct negotiation between the consumer and the trader;
- (f) attempts made by a judge to settle a dispute in the course of a judicial proceeding concerning that dispute;
- (g) procedures initiated by a trader against a consumer;
- (h) health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices;
- (i) public providers of further or higher education.

3. This Directive establishes harmonised quality requirements for ADR entities and ADR procedures in order to ensure that, after its implementation, consumers have access to high-quality, transparent, effective and fair out-of-court redress mechanisms no matter where they reside in the Union. Member States may maintain or introduce rules that go beyond those laid down by this Directive, in order to ensure a higher level of consumer protection.

4. This Directive acknowledges the competence of Member States to determine whether ADR entities established on their territories are to have the power to impose a solution.

Article 3

Relationship with other Union legal acts

1. Save as otherwise set out in this Directive, if any provision of this Directive conflicts with a provision laid down in another Union legal act and relating to out-of-court redress procedures initiated by a consumer against a trader, the provision of this Directive shall prevail.

2. This Directive shall be without prejudice to Directive 2008/52/EC.

3. Article 13 of this Directive shall be without prejudice to provisions on consumer information on out-of-court redress procedures contained in other Union legal acts which shall apply in addition to that Article.

Article 4

Definitions

1. For the purposes of this Directive:

- (a) 'consumer' means any natural person who is acting for purposes which are outside his trade, business, craft or profession;
- (b) 'trader' means any natural persons, or any legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession;

(c) 'sales contract' means any contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer and the consumer pays or undertakes to pay the price thereof, including any contract having as its object both goods and services;

(d) 'service contract' means any contract other than a sales contract under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof;

(e) 'domestic dispute' means a contractual dispute arising from a sales or service contract where, at the time the consumer orders the goods or services, the consumer is resident in the same Member State as that in which the trader is established;

(f) 'cross-border dispute' means a contractual dispute arising from a sales or service contract where, at the time the consumer orders the goods or services, the consumer is resident in a Member State other than the Member State in which the trader is established;

(g) 'ADR procedure' means a procedure, as referred to in Article 2, which complies with the requirements set out in this Directive and is carried out by an ADR entity;

(h) 'ADR entity' means any entity, however named or referred to, which is established on a durable basis and offers the resolution of a dispute through an ADR procedure and that is listed in accordance with Article 20(2);

(i) 'competent authority' means any public authority designated by a Member State for the purposes of this Directive and established at national, regional or local level.

2. A trader is established:

— if the trader is a natural person, where he has his place of business,

- if the trader is a company or other legal person or association of natural or legal persons, where it has its statutory seat, central administration or place of business, including a branch, agency or any other establishment.

3. An ADR entity is established:

— if it is operated by a natural person, at the place where it carries out ADR activities,

— if the entity is operated by a legal person or association of natural or legal persons, at the place where that legal person or association of natural or legal persons carries out ADR activities or has its statutory seat,

— if it is operated by an authority or other public body, at the place where that authority or other public body has its seat.

CHAPTER II

ACCESS TO AND REQUIREMENTS APPLICABLE TO ADR ENTITIES AND ADR PROCEDURES

Article 5 Access to ADR entities and ADR procedures

1. Member States shall facilitate access by consumers to ADR procedures and shall ensure that disputes covered by this Directive and which involve a trader established on their respective territories can be submitted to an ADR entity which complies with the requirements set out in this Directive.

2. Member States shall ensure that ADR entities:

(a) maintain an up-to-date website which provides the parties with easy access to information concerning the ADR procedure, and which enables consumers to submit a complaint and the requisite supporting documents online;

(b) provide the parties, at their request, with the information referred to in point (a) on a durable medium;

(c) where applicable, enable the consumer to submit a complaint offline;

(d) enable the exchange of information between the parties via electronic means or, if applicable, by post;

(e) accept both domestic and cross-border disputes, including disputes covered by Regulation (EU) No 524/2013; and

(f) when dealing with disputes covered by this Directive, take the necessary measures to ensure that the processing of personal data complies with the rules on the protection of personal data laid down in the national legislation

implementing Directive 95/46/EC in the Member State in which the ADR entity is established.

3. Member States may fulfil their obligation under paragraph 1 by ensuring the existence of a residual ADR entity which is competent to deal with disputes as referred to in that paragraph for the resolution of which no existing ADR entity is competent. Member States may also fulfil that obligation by relying on ADR entities established in another Member State or regional, transnational or pan-European dispute resolution entities, where traders from different Member States are covered by the same ADR entity, without prejudice to their responsibility to ensure full coverage and access to ADR entities.

4. Member States may, at their discretion, permit ADR entities to maintain and introduce procedural rules that allow them to refuse to deal with a given dispute on the grounds that:

(a) the consumer did not attempt to contact the trader concerned in order to discuss his complaint and seek, as a first step, to resolve the matter directly with the trader;

(b) the dispute is frivolous or vexatious;

(c) the dispute is being or has previously been considered by another ADR entity or by a court;

(d) the value of the claim falls below or above a pre-specified monetary threshold;

(e) the consumer has not submitted the complaint to the ADR entity within a pre-specified time limit, which shall not be set at less than one year from the date upon which the consumer submitted the complaint to the trader;

(f) dealing with such a type of dispute would otherwise seriously impair the effective operation of the ADR entity.

Where, in accordance with its procedural rules, an ADR entity is unable to consider a dispute that has been submitted to it, that ADR entity shall provide both parties with a reasoned explanation of the grounds for not considering the dispute within three weeks of receiving the complaint file.

Such procedural rules shall not significantly impair consumers' access to ADR procedures, including in the case of cross-border disputes.

5. Member States shall ensure that, when ADR entities are permitted to establish pre-specified monetary thresholds in order to limit access to ADR procedures, those thresholds are not set at a level at which they significantly impair the consumers' access to complaint handling by ADR entities.

6. Where, in accordance with the procedural rules referred to in paragraph 4, an ADR entity is unable to consider a complaint that has been submitted to it, a Member State shall not be required to ensure that the consumer can submit his complaint to another ADR entity.

7. Where an ADR entity dealing with disputes in a specific economic sector is competent to consider disputes relating to a trader operating in that sector but which is not a member of the organisation or association forming or funding the ADR entity, the Member State shall be deemed to have fulfilled its obligation under paragraph 1 also with respect to disputes concerning that trader.

Article 6

Expertise, independence and impartiality

1. Member States shall ensure that the natural persons in charge of ADR possess the necessary expertise and are independent and impartial. This shall be guaranteed by ensuring that such persons:

(a) possess the necessary knowledge and skills in the field of alternative or judicial resolution of consumer disputes, as well as a general understanding of law;

(b) are appointed for a term of office of sufficient duration to ensure the independence of their actions, and are not liable to be relieved from their duties without just cause;

(c) are not subject to any instructions from either party or their representatives;

(d) are remunerated in a way that is not linked to the outcome of the procedure;

(e) without undue delay disclose to the ADR entity any circumstances that may, or may be seen to, affect their independence and impartiality or give rise to a conflict of interest with either party to the dispute they are asked to resolve. The obligation to disclose such circumstances shall be a continuing obligation throughout the ADR procedure. It shall not apply where the ADR entity comprises only one natural person.

2. Member States shall ensure that ADR entities have in place procedures to ensure that in the case of circumstances referred to in point (e) of paragraph 1:

(a) the natural person concerned is replaced by another natural person that shall be entrusted with conducting the ADR procedure; or failing that

(b) the natural person concerned refrains from conducting the ADR procedure and, where possible, the ADR entity proposes to the parties to submit the dispute to another ADR entity which is competent to deal with the dispute; or failing that

(c) the circumstances are disclosed to the parties and the natural person concerned is allowed to continue to conduct the ADR procedure only if the parties have not objected after they have been informed of the circumstances and their right to object.

This paragraph shall be without prejudice to point (a) of Article 9(2).

Where the ADR entity comprises only one natural person, only points (b) and (c) of the first subparagraph of this paragraph shall apply.

3. Where Member States decide to allow procedures referred to in point (a) of Article 2(2) as ADR procedures under this Directive, they shall ensure that, in addition to the general requirements set out in paragraphs 1 and 5, those procedures comply with the following specific requirements:

(a) the natural persons in charge of dispute resolution are nominated by, or form part of, a collegial body composed of an equal number of representatives of consumer organisations and of representatives of the trader and are appointed as result of a transparent procedure;

(b) the natural persons in charge of dispute resolution are granted a period of office of a minimum of three years to ensure the independence of their actions;

(c) the natural persons in charge of dispute resolution commit not to work for the trader or a professional organisation or business association of which the trader is a member for a period of three years after their position in the dispute resolution entity has ended;

(d) the dispute resolution entity does not have any hierarchical or functional link with the trader and is clearly separated from the trader's operational entities and has a sufficient budget at its disposal, which is separate from the trader's general budget, to fulfil its tasks.

4. Where the natural persons in charge of ADR are employed or remunerated exclusively by a professional organisation or a business association of which the trader is a member, Member States shall ensure that, in addition to the general requirements set out in paragraphs 1 and 5, they have a separate and dedicated budget at their disposal which is sufficient to fulfil their tasks.

This paragraph shall not apply where the natural persons concerned form part of a collegial body composed of an equal number of representatives of the professional organisation or business association by which they are employed or remunerated and of consumer organisations.

5. Member States shall ensure that ADR entities where the natural persons in charge of dispute resolution form part of a collegial body provide for an equal number of representatives of consumers' interests and of representatives of traders' interests in that body.

6. For the purposes of point (a) of paragraph 1, Member States shall encourage ADR entities to provide training for natural persons in charge of ADR. If such training is provided, competent authorities shall monitor the training schemes established by ADR entities, on the basis of information

communicated to them in accordance with point (g) of Article 19(3).

Article 7

Transparency

1. Member States shall ensure that ADR entities make publicly available on their websites, on a durable medium upon request, and by any other means they consider appropriate, clear and easily understandable information on:

(a) their contact details, including postal address and e-mail address;

(b) the fact that ADR entities are listed in accordance with Article 20(2);

(c) the natural persons in charge of ADR, the method of their appointment and the length of their mandate;

(d) the expertise, impartiality and independence of the natural persons in charge of ADR, if they are employed or remunerated exclusively by the trader;

(e) their membership in networks of ADR entities facilitating cross-border dispute resolution, if applicable;

(f) the types of disputes they are competent to deal with, including any threshold if applicable;

(g) the procedural rules governing the resolution of a dispute and the grounds on which the ADR entity may refuse to deal with a given dispute in accordance with Article 5(4);

(h) the languages in which complaints can be submitted to the ADR entity and in which the ADR procedure is conducted;

(i) the types of rules the ADR entity may use as a basis for the dispute resolution (for example legal provisions, considerations of equity, codes of conduct);

(j) any preliminary requirements the parties may have to meet before an ADR procedure can be instituted, including the requirement that an attempt be made by the consumer to resolve the matter directly with the trader;

(k) whether or not the parties can withdraw from the procedure;

(l) the costs, if any, to be borne by the parties, including any rules on awarding costs at the end of the procedure;

(m) the average length of the ADR procedure;

(n) the legal effect of the outcome of the ADR procedure, including the penalties for non-compliance in the case of a decision having binding effect on the parties, if applicable;

(o) the enforceability of the ADR decision, if relevant.

2. Member States shall ensure that ADR entities make publicly available on their websites, on a durable medium upon request, and by any other means they consider appropriate, annual activity reports. Those reports shall include the following information relating to both domestic and cross-border disputes:

(a) the number of disputes received and the types of complaints to which they related;

(b) any systematic or significant problems that occur frequently and lead to disputes between consumers and traders; such information may be accompanied by recommendations as to how such problems can be avoided or resolved in future, in order to raise traders' standards and to facilitate the exchange of information and best practices;

(c) the rate of disputes the ADR entity has refused to deal with and the percentage share of the types of grounds for such refusal as referred to in Article 5(4);

(d) in the case of procedures referred to in point (a) of Article 2(2), the percentage shares of solutions proposed or imposed in favour of the consumer and in favour of the trader, and of disputes resolved by an amicable solution;

(e) the percentage share of ADR procedures which were discontinued and, if known, the reasons for their discontinuation;

(f) the average time taken to resolve disputes;

(g) the rate of compliance, if known, with the outcomes of the ADR procedures;

(h) cooperation of ADR entities within networks of ADR entities which facilitate the resolution of cross-border disputes, if applicable.

Article 8

Effectiveness

Member States shall ensure that ADR procedures are effective and fulfil the following requirements:

- (a) the ADR procedure is available and easily accessible online and offline to both parties irrespective of where they are;
- (b) the parties have access to the procedure without being obliged to retain a lawyer or a legal advisor, but the procedure shall not deprive the parties of their right to independent advice or to be represented or assisted by a third party at any stage of the procedure;
- (c) the ADR procedure is free of charge or available at a nominal fee for consumers;
- (d) the ADR entity which has received a complaint notifies the parties to the dispute as soon as it has received all the documents containing the relevant information relating to the complaint;
- (e) the outcome of the ADR procedure is made available within a period of 90 calendar days from the date on which the ADR entity has received the complete complaint file. In the case of highly complex disputes, the ADR entity in charge may, at its own discretion, extend the 90 calendar days' time period. The parties shall be informed of any extension of that period and of the expected length of time that will be needed for the conclusion of the dispute.

Article 9

Fairness

1. Member States shall ensure that in ADR procedures:

- (a) the parties have the possibility, within a reasonable period of time, of expressing their point of view, of being provided by the ADR entity with the arguments, evidence, documents and facts put forward by the other party, any statements made and opinions given by experts, and of being able to comment on them;
 - (b) the parties are informed that they are not obliged to retain a lawyer or a legal advisor, but they may seek independent advice or be represented or assisted by a third party at any stage of the procedure;
 - (c) the parties are notified of the outcome of the ADR procedure in writing or on a durable medium, and are given a statement of the grounds on which the outcome is based.
2. In ADR procedures which aim at resolving the dispute by proposing a solution, Member States shall ensure that:
- (a) The parties have the possibility of withdrawing from the procedure at any stage if they are dissatisfied with the performance or the operation of the procedure. They shall be informed of that right before the procedure commences. Where national rules provide for mandatory participation by the trader in ADR procedures, this point shall apply only to the consumer.

(b) The parties, before agreeing or following a proposed solution, are informed that:

- (i) they have the choice as to whether or not to agree to or follow the proposed solution;
- (ii) participation in the procedure does not preclude the possibility of seeking redress through court proceedings;
- (iii) the proposed solution may be different from an outcome determined by a court applying legal rules.

(c) The parties, before agreeing to or following a proposed solution, are informed of the legal effect of agreeing to or following such a proposed solution.

(d) The parties, before expressing their consent to a proposed solution or amicable agreement, are allowed a reasonable period of time to reflect.

3. Where, in accordance with national law, ADR procedures provide that their outcome becomes binding on the trader once the consumer has accepted the proposed solution, Article 9(2) shall be read as applicable only to the consumer.

Article 10

Liberty

1. Member States shall ensure that an agreement between a consumer and a trader to submit complaints to an ADR entity is not binding on the consumer if it was concluded before the dispute has materialised and if it has the effect of depriving the consumer of his right to bring an action before the courts for the settlement of the dispute.

2. Member States shall ensure that in ADR procedures which aim at resolving the dispute by imposing a solution the solution imposed may be binding on the parties only if they were informed of its binding nature in advance and specifically accepted this. Specific acceptance by the trader is not required if national rules provide that solutions are binding on traders.

Article 11

Legality

1. Member States shall ensure that in ADR procedures which aim at resolving the dispute by imposing a solution on the consumer:

(a) in a situation where there is no conflict of laws, the solution imposed shall not result in the consumer being deprived of the protection afforded to him by the provisions that cannot be derogated from by agreement by virtue of the law of the Member State where the consumer and the trader are habitually resident;

(b) in a situation involving a conflict of laws, where the law applicable to the sales or service contract is determined in accordance with Article 6(1) and (2) of Regulation (EC) No 593/2008, the solution imposed by the ADR entity shall not result in the consumer being deprived of the protection afforded to him by the provisions that cannot be derogated from by agreement by virtue of the law of the Member State in which he is habitually resident;

(c) in a situation involving a conflict of laws, where the law applicable to the sales or service contract is determined in accordance with Article 5(1) to (3) of the Rome Convention of 19 June 1980 on the law applicable to contractual obligations, the solution imposed by the ADR entity shall not result in the consumer being deprived of the protection afforded to him by the mandatory rules of the law of the Member State in which he is habitually resident.

2. For the purposes of this Article, 'habitual residence' shall be determined in accordance with Regulation (EC) No 593/2008.

Article 12

Effect of ADR procedures on limitation and prescription periods

1. Member States shall ensure that parties who, in an attempt to settle a dispute, have recourse to ADR procedures the outcome of which is not binding, are not subsequently prevented from initiating judicial proceedings in relation to that dispute as a result of the expiry of limitation or prescription periods during the ADR procedure.

2. Paragraph 1 shall be without prejudice to provisions on limitation or prescription contained in international agreements to which Member States are party.

CHAPTER III

INFORMATION AND COOPERATION

Article 13

Consumer information by traders

1. Member States shall ensure that traders established on their territories inform consumers about the ADR entity or ADR entities by which those traders are covered, when those traders commit to or are obliged to use those entities to resolve disputes with consumers. That information shall include the website address of the relevant ADR entity or ADR entities.

2. The information referred to in paragraph 1 shall be provided in a clear, comprehensible and easily accessible way on the traders' website, where one exists, and, if applicable, in the

general terms and conditions of sales or service contracts between the trader and a consumer.

3. Member States shall ensure that, in cases where a dispute between a consumer and a trader established in their territory could not be settled further to a complaint submitted directly by the consumer to the trader, the trader provides the consumer with the information referred to in paragraph 1, specifying whether he will make use of the relevant ADR entities to settle the dispute. That information shall be provided on paper or on another durable medium.

Article 14

Assistance for consumers

1. Member States shall ensure that, with regard to disputes arising from cross-border sales or service contracts, consumers can obtain assistance to access the ADR entity operating in another Member State which is competent to deal with their cross-border dispute.

2. Member States shall confer responsibility for the task referred to in paragraph 1 on their centres of the European Consumer Centre Network, on consumer organisations or on any other body.

Article 15

General information

1. Member States shall ensure that ADR entities, the centres of the European Consumer Centre Network and, where appropriate, the bodies designated in accordance with Article 14(2) make publicly available on their websites, by providing a link to the Commission's website, and whenever possible on a durable medium at their premises, the list of ADR entities referred to in Article 20(4).

2. Member States shall encourage relevant consumer organisations and business associations to make publicly available on their websites, and by any other means they consider appropriate, the list of ADR entities referred to in Article 20(4).

3. The Commission and Member States shall ensure appropriate dissemination of information on how consumers can access ADR procedures for resolving disputes covered by this Directive.

4. The Commission and the Member States shall take accompanying measures to encourage consumer organisations and professional organisations, at Union and at national level, to raise awareness of ADR entities and their procedures and to promote ADR take-up by traders and consumers. Those bodies shall also be encouraged to provide consumers with information about competent ADR entities when they receive complaints from consumers.

Article 16

Cooperation and exchanges of experience between ADR entities

1. Member States shall ensure that ADR entities cooperate in the resolution of cross-border disputes and conduct regular exchanges of best practices as regards the settlement of both cross-border and domestic disputes.

2. The Commission shall support and facilitate the networking of national ADR entities and the exchange and dissemination of their best practices and experiences.

3. Where a network of ADR entities facilitating the resolution of cross-border disputes exists in a sector-specific area within the Union, Member States shall encourage ADR entities that deal with disputes in that area to become a member of that network.

4. The Commission shall publish a list containing the names and contact details of the networks referred to in paragraph 3. The Commission shall, when necessary, update this list.

Article 17

Cooperation between ADR entities and national authorities enforcing Union legal acts on consumer protection

1. Member States shall ensure cooperation between ADR entities and national authorities entrusted with the enforcement of Union legal acts on consumer protection.

2. This cooperation shall in particular include mutual exchange of information on practices in specific business sectors about which consumers have repeatedly lodged complaints. It shall also include the provision of technical assessment and information by such national authorities to ADR entities where such assessment or information is necessary for the handling of individual disputes and is already available.

3. Member States shall ensure that cooperation and mutual information exchanges referred to in paragraphs 1 and 2 comply with the rules on the protection of personal data laid down in Directive 95/46/EC.

4. This Article shall be without prejudice to provisions on professional and commercial secrecy which apply to the national authorities enforcing Union legal acts on consumer protection. ADR entities shall be subject to rules of professional secrecy or other equivalent duties of confidentiality laid down in the legislation of the Member States where they are established.

CHAPTER IV

THE ROLE OF COMPETENT AUTHORITIES AND THE COMMISSION

Article 18

Designation of competent authorities

1. Each Member State shall designate a competent authority which shall carry out the functions set out in Articles 19 and 20. Each Member State may designate more than one competent authority. If a Member State does so, it shall determine which of the competent authorities designated is the single point of contact for the Commission. Each Member State shall communicate the competent authority or, where appropriate, the competent authorities, including the single point of contact it has designated, to the Commission.

2. The Commission shall establish a list of the competent authorities including, where appropriate, the single point of contact communicated to it in accordance with paragraph 1, and publish that list in the Official Journal of the European Union.

Article 19

Information to be notified to competent authorities by dispute resolution entities

1. Member States shall ensure that dispute resolution entities established on their territories, which intend to qualify as ADR entities under this Directive and be listed in accordance with Article 20(2), notify to the competent authority the following:

- (a) their name, contact details and website address;
 - (b) information on their structure and funding, including information on the natural persons in charge of dispute resolution, their remuneration, term of office and by whom they are employed;
 - (c) their procedural rules;
 - (d) their fees, if applicable;
 - (e) the average length of the dispute resolution procedures;
 - (f) the language or languages in which complaints can be submitted and the dispute resolution procedure conducted;
 - (g) a statement on the types of disputes covered by the dispute resolution procedure;
 - (h) the grounds on which the dispute resolution entity may refuse to deal with a given dispute in accordance with Article 5(4);
 - (i) a reasoned statement on whether the entity qualifies as an ADR entity falling within the scope of this Directive and complies with the quality requirements set out in Chapter II.
- In the event of changes to the information referred to in points (a) to (h), ADR entities shall without undue delay notify those changes to the competent authority.

2. Where Member States decide to allow procedures as referred to in point (a) of Article 2(2), they shall ensure that ADR entities applying such procedures notify to the competent authority, in addition to the information and statements referred to in paragraph 1, the information necessary to assess their compliance with the specific additional requirements of independence and transparency set out in Article 6(3).

3. Member States shall ensure that ADR entities communicate to the competent authorities every two years information on:

- (a) the number of disputes received and the types of complaints to which they related;
- (b) the percentage share of ADR procedures which were discontinued before an outcome was reached;
- (c) the average time taken to resolve the disputes received;
- (d) the rate of compliance, if known, with the outcomes of the ADR procedures;
- (e) any systematic or significant problems that occur frequently and lead to disputes between consumers and traders. The information communicated in this regard may be accompanied by recommendations as to how such problems can be avoided or resolved in future;
- (f) where applicable, an assessment of the effectiveness of their cooperation within networks of ADR entities facilitating the resolution of cross-border disputes;
- (g) where applicable, the training provided to natural persons in charge of ADR in accordance with Article 6(6);
- (h) an assessment of the effectiveness of the ADR procedure offered by the entity and of possible ways of improving its performance.

Article 20

Role of the competent authorities and of the Commission

1. Each competent authority shall assess, in particular on the basis of the information it has received in accordance with Article 19(1), whether the dispute resolution entities notified to it qualify as ADR entities falling within the scope of this Directive and comply with the quality requirements set out in Chapter II and in national provisions implementing it, including national provisions going beyond the requirements of this Directive, in conformity with Union law.

2. Each competent authority shall, on the basis of the assessment referred to in paragraph 1, list all the ADR entities that have been notified to it and fulfil the conditions set out in paragraph 1.

That list shall include the following:

- (a) the name, the contact details and the website addresses of the ADR entities referred to in the first subparagraph;
- (b) their fees, if applicable;
- (c) the language or languages in which complaints can be submitted and the ADR procedure conducted;
- (d) the types of disputes covered by the ADR procedure;
- (e) the sectors and categories of disputes covered by each ADR entity;
- (f) the need for the physical presence of the parties or of their representatives, if applicable, including a statement by the ADR entity on whether the ADR procedure is or can be conducted as an oral or a written procedure;
- (g) the binding or non-binding nature of the outcome of the procedure; and
- (h) the grounds on which the ADR entity may refuse to deal with a given dispute in accordance with Article 5(4).

Each competent authority shall notify the list referred to in the first subparagraph of this paragraph to the Commission. If any changes are notified to the competent authority in accordance with the second subparagraph of Article 19(1), that list shall be updated without undue delay and the relevant information notified to the Commission.

If a dispute resolution entity listed as ADR entity under this Directive no longer complies with the requirements referred to in paragraph 1, the competent authority concerned shall contact that dispute resolution entity, stating the requirements the dispute resolution entity fails to comply with and requesting it to ensure compliance immediately. If the dispute

resolution entity after a period of three months still does not fulfil the requirements referred to in paragraph 1, the competent authority shall remove the dispute resolution entity from the list referred to in the first subparagraph of this paragraph. That list shall be updated without undue delay and the relevant information notified to the Commission.

3. If a Member State has designated more than one competent authority, the list and its updates referred to in paragraph 2 shall be notified to the Commission by the single point of contact referred to in Article 18(1). That list and those updates shall relate to all ADR entities established in that Member State.

4. The Commission shall establish a list of the ADR entities notified to it in accordance with paragraph 2 and update that list whenever changes are notified to the Commission. The Commission shall make publicly available that list and its updates on its website and on a durable medium. The Commission shall transmit that list and its updates to the competent authorities. Where a Member State has designated a single point of contact in accordance with Article 18(1), the Commission shall transmit that list and its updates to the single point of contact.

5. Each competent authority shall make publicly available the consolidated list of ADR entities referred to in paragraph 4 on its website by providing a link to the relevant Commission website. In addition, each competent authority shall make publicly available that consolidated list on a durable medium.

6. By 9 July 2018, and every four years thereafter, each competent authority shall publish and send to the Commission a report on the development and functioning of ADR entities. That report shall in particular:

- (a) identify best practices of ADR entities;
- (b) point out the shortcomings, supported by statistics, that hinder the functioning of ADR entities for both domestic and cross-border disputes, where appropriate;
- (c) make recommendations on how to improve the effective and efficient functioning of ADR entities, where appropriate.

7. If a Member State has designated more than one competent authority in accordance with Article 18(1), the report referred to in paragraph 6 of this Article shall be published by the single point of contact referred to in Article 18(1). That report shall relate to all ADR entities established in that Member State.

CHAPTER V

FINAL PROVISIONS

Article 21

Penalties

Member States shall lay down the rules on penalties applicable to infringements of the national provisions adopted in particular pursuant to Article 13 and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

Article 22

Amendment to Regulation (EC) No 2006/2004

In the Annex to Regulation (EC) No 2006/2004, the following point is added:

'20.

Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes (OJ L 165, 18.6.2013, p. 63): Article 13.'

Article 23

Amendment to Directive 2009/22/EC

In Annex I to Directive 2009/22/EC the following point is added:

'14.

Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes (OJ L 165, 18.6.2013, p. 63): Article 13.'

Article 24

Communication

1. By 9 July 2015, Member States shall communicate to the Commission:

(a) where appropriate, the names and contact details of the bodies designated in accordance with Article 14(2); and
(b) the competent authorities including, where appropriate, the single point of contact, designated in accordance with Article 18(1).

Member States shall inform the Commission of any subsequent changes to this information.

2. By 9 January 2016, Member States shall communicate to the Commission the first list referred to in Article 20(2).

3. The Commission shall transmit to the Member States the information referred to in point (a) of paragraph 1.

Article 25

Transposition

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive by 9 July 2015. They shall forthwith communicate to the Commission the text of those provisions.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 26

Report

By 9 July 2019, and every four years thereafter, the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee a report on the application of this Directive. That report shall consider the development and the use of ADR entities and the impact of this Directive on consumers and traders, in particular on the awareness of consumers and the level of adoption by traders.

That report shall be accompanied, where appropriate, by proposals for amendment of this Directive.

Article 27

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 28

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 21 May 2013.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

L. CREIGHTON

(1) OJ C 181, 21.6.2012, p. 93.

(2) Position of the European Parliament of 12 March 2013 (not yet published in the Official Journal) and decision of the Council of 22 April 2013.

(3) OJ L 115, 17.4.1998, p. 31.

(4) OJ L 109, 19.4.2001, p. 56.

(5) See page 1 of this Official Journal.

(6) OJ L 88, 4.4.2011, p. 45.

(7) OJ L 136, 24.5.2008, p. 3.

(8) OJ L 281, 23.11.1995, p. 31.

(9) OJ L 177, 4.7.2008, p. 6.

(10) OJ L 266, 9.10.1980, p. 1.

(11) OJ L 136, 2.6.2010, p. 1.

(12) OJ L 364, 9.12.2004, p. 1.

(13) OJ L 110, 1.5.2009, p. 30.

(14) OJ C 369, 17.12.2011, p. 14.

(15) OJ L 8, 12.1.2001, p. 1.

(16) OJ C 136, 11.5.2012, p. 1.

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

THE COUNCIL OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Economic Community, and in particular Article 100 A thereof,

Having regard to the proposal from the Commission (1),

In cooperation with the European Parliament (2),

Having regard to the opinion of the Economic and Social Committee (3),

Whereas it is necessary to adopt measures with the aim of progressively establishing the internal market before 31 December 1992; whereas the internal market comprises an area without internal frontiers in which goods, persons, services and capital move freely;

Whereas the laws of Member States relating to the terms of contract between the seller of goods or supplier of services, on the one hand, and the consumer of them, on the other hand, show many disparities, with the result that the national markets for the sale of goods and services to consumers differ from each other and that distortions of competition may arise amongst the sellers and suppliers, notably when they sell and supply in other Member States;

Whereas, in particular, the laws of Member States relating to unfair terms in consumer contracts show marked divergences;

Whereas it is the responsibility of the Member States to ensure that contracts concluded with consumers do not contain unfair terms;

Whereas, generally speaking, consumers do not know the rules of law which, in Member States other than their own, govern contracts for the sale of goods or services; whereas this lack of awareness may deter them from direct transactions for the purchase of goods or services in another Member State;

Whereas, in order to facilitate the establishment of the internal market and to safeguard the citizen in his role as consumer when acquiring goods and services under contracts which are governed by the laws of Member States other than his own, it is essential to remove unfair terms from those contracts;

Whereas sellers of goods and suppliers of services will thereby be helped in their task of selling goods and supplying services, both at home and throughout the internal market; whereas competition will thus be stimulated, so contributing to increased choice for Community citizens as consumers;

Whereas the two Community programmes for a consumer protection and information policy (4) underlined the importance of safeguarding consumers in the matter of unfair terms of contract; whereas this protection ought to be provided by laws and Regulations which are either harmonized at Community level or adopted directly at that level;

Whereas in accordance with the principle laid down under the heading 'Protection of the economic interests of the consumers', as stated in those programmes: 'acquirers of goods and services should be protected against the abuse of power by the seller or supplier, in particular against one-sided standard contracts and the unfair exclusion of essential rights in contracts';

Whereas more effective protection of the consumer can be achieved by adopting uniform rules of law in the matter of unfair terms; whereas those rules should apply to all contracts concluded between sellers or suppliers and consumers; whereas as a result inter alia contracts relating to employment, contracts relating to succession rights, contracts relating to rights under family law and contracts relating to the incorporation and organization of companies or partnership agreements must be excluded from this Directive;

Whereas the consumer must receive equal protection under contracts concluded by word of mouth and written contracts regardless, in the latter case, of whether the terms of the contract are contained in one or more documents;

Whereas, however, as they now stand, national laws allow only partial harmonization to be envisaged; whereas, in particular, only contractual terms which have not been individually negotiated are covered by this Directive; whereas Member States should have the option, with due regard for the Treaty, to afford consumers a higher level of protection through national provisions that are more stringent than those of this Directive;

Whereas the statutory or regulatory provisions of the Member States which directly or indirectly determine the terms of consumer contracts are presumed not to contain unfair terms; whereas, therefore, it does not appear to be necessary to subject the terms which reflect mandatory statutory or regulatory provisions and the principles or provisions of international conventions to which the Member States or the Community are party; whereas in that respect the wording 'mandatory statutory or regulatory provisions' in Article 1 (2) also covers rules which, according to the law, shall apply between the contracting parties provided that no other arrangements have been established;

Whereas Member States must however ensure that unfair terms are not included, particularly because this Directive also applies to trades, business or professions of a public nature;

Whereas it is necessary to fix in a general way the criteria for assessing the unfair character of contract terms;

Whereas the assessment, according to the general criteria chosen, of the unfair character of terms, in particular in sale or supply activities of a public nature providing collective services which take account of solidarity among users, must be supplemented by a means of making an overall evaluation of the different interests involved; whereas this constitutes the requirement of good faith; whereas, in making an assessment of good faith, particular regard shall be had to the strength of the bargaining positions of the parties, whether the consumer had an inducement to agree to the term and whether the goods or services were sold or supplied to the special order of the consumer; whereas the requirement of good faith may be satisfied by the seller or supplier where he deals fairly and equitably with the other party whose legitimate interests he has to take into account;

Whereas, for the purposes of this Directive, the annexed list of terms can be of indicative value only and, because of the cause of the minimal character of the Directive, the scope of these terms may be the subject of amplification or more restrictive editing by the Member States in their national laws;

Whereas the nature of goods or services should have an influence on assessing the unfairness of contractual terms;

Whereas, for the purposes of this Directive, assessment of unfair character shall not be made of terms which describe the main subject matter of the contract nor the quality/price ratio of the goods or services supplied; whereas the main subject matter of the contract and the price/quality ratio may nevertheless be taken into account in assessing the fairness of other terms; whereas it follows, inter alia, that in insurance

contracts, the terms which clearly define or circumscribe the insured risk and the insurer's liability shall not be subject to such assessment since these restrictions are taken into account in calculating the premium paid by the consumer;

Whereas contracts should be drafted in plain, intelligible language, the consumer should actually be given an opportunity to examine all the terms and, if in doubt, the interpretation most favourable to the consumer should prevail; Whereas Member States should ensure that unfair terms are not used in contracts concluded with consumers by a seller or supplier and that if, nevertheless, such terms are so used, they will not bind the consumer, and the contract will continue to bind the parties upon those terms if it is capable of continuing in existence without the unfair provisions;

Whereas there is a risk that, in certain cases, the consumer may be deprived of protection under this Directive by designating the law of a non-Member country as the law applicable to the contract; whereas provisions should therefore be included in this Directive designed to avert this risk;

Whereas persons or organizations, if regarded under the law of a Member State as having a legitimate interest in the matter, must have facilities for initiating proceedings concerning terms of contract drawn up for general use in contracts concluded with consumers, and in particular unfair terms, either before a court or before an administrative authority competent to decide upon complaints or to initiate appropriate legal proceedings; whereas this possibility does not, however, entail prior verification of the general conditions obtaining in individual economic sectors;

Whereas the courts or administrative authorities of the Member States must have at their disposal adequate and effective means of preventing the continued application of unfair terms in consumer contracts,

HAS ADOPTED THIS DIRECTIVE:

Article 1

1. The purpose of this Directive is to approximate the laws, Regulations and administrative provisions of the Member States relating to unfair terms in contracts concluded between a seller or supplier and a consumer.

2. The contractual terms which reflect mandatory statutory or regulatory provisions and the provisions or principles of international conventions to which the Member States or the Community are party, particularly in the transport area, shall not be subject to the provisions of this Directive.

Article 2

For the purposes of this Directive:

(a) 'unfair terms' means the contractual terms defined in Article 3;

(b) 'consumer' means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession;

(c) 'seller or supplier' means any natural or legal person who, in contracts covered by this Directive, is acting for purposes relating to his trade, business or profession, whether publicly owned or privately owned.

Article 3

1. A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.

2. A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract.

The fact that certain aspects of a term or one specific term have been individually negotiated shall not exclude the application of this Article to the rest of a contract if an overall assessment

of the contract indicates that it is nevertheless a pre-formulated standard contract.

Where any seller or supplier claims that a standard term has been individually negotiated, the burden of proof in this respect shall be incumbent on him.

3. The Annex shall contain an indicative and non-exhaustive list of the terms which may be regarded as unfair.

Article 4

1. Without prejudice to Article 7, the unfairness of a contractual term shall be assessed, taking into account the nature of the goods or services for which the contract was concluded and by referring, at the time of conclusion of the contract, to all the circumstances attending the conclusion of the contract and to all the other terms of the contract or of another contract on which it is dependent.

2. Assessment of the unfair nature of the terms shall relate neither to the definition of the main subject matter of the contract nor to the adequacy of the price and remuneration, on the one hand, as against the services or goods supplied in exchange, on the other, in so far as these terms are in plain intelligible language.

Article 5

In the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language. Where there is doubt about the meaning of a term, the interpretation most favourable to the consumer shall prevail. This rule on interpretation shall not apply in the context of the procedures laid down in Article 7 (2).

Article 6

1. Member States shall lay down that unfair terms used in a contract concluded with a consumer by a seller or supplier shall, as provided for under their national law, not be binding on the consumer and that the contract shall continue to bind the parties upon those terms if it is capable of continuing in existence without the unfair terms.

2. Member States shall take the necessary measures to ensure that the consumer does not lose the protection granted by this Directive by virtue of the choice of the law of a non-Member country as the law applicable to the contract if the latter has a close connection with the territory of the Member States.

Article 7

1. Member States shall ensure that, in the interests of consumers and of competitors, adequate and effective means exist to prevent the continued use of unfair terms in contracts concluded with consumers by sellers or suppliers.

2. The means referred to in paragraph 1 shall include provisions whereby persons or organizations, having a legitimate interest under national law in protecting consumers, may take action according to the national law concerned before the courts or before competent administrative bodies for a decision as to whether contractual terms drawn up for general use are unfair, so that they can apply appropriate and effective means to prevent the continued use of such terms.

3. With due regard for national laws, the legal remedies referred to in paragraph 2 may be directed separately or jointly against a number of sellers or suppliers from the same economic sector or their associations which use or recommend the use of the same general contractual terms or similar terms.

Article 8

Member States may adopt or retain the most stringent provisions compatible with the Treaty in the area covered by this Directive, to ensure a maximum degree of protection for the consumer.

Article 8a

1. Where a Member State adopts provisions in accordance with Article 8, it shall inform the Commission thereof, as well as of any subsequent changes, in particular where those provisions:

— extend the unfairness assessment to individually negotiated contractual terms or to the adequacy of the price or remuneration; or,

— contain lists of contractual terms which shall be considered as unfair,

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.

Article 9

The Commission shall present a report to the European Parliament and to the Council concerning the application of this Directive five years at the latest after the date in Article 10 (1).

Article 10

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive no later than 31 December 1994. They shall forthwith inform the Commission thereof.

These provisions shall be applicable to all contracts concluded after 31 December 1994.

2. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such a reference shall be laid down by the Member States.

3. Member States shall communicate the main provisions of national law which they adopt in the field covered by this Directive to the Commission.

Article 11

This Directive is addressed to the Member States.

Done at Luxembourg, 5 April 1993.

For the Council

The President

N. HELVEG PETERSEN

(1) OJ No C 73, 24. 3. 1992, p. 7.

(2) OJ No C 326, 16. 12. 1991, p. 108 and OJ No C 21, 25. 1. 1993.

(3) OJ No C 159, 17. 6. 1991, p. 34.

(4) OJ No C 92, 25. 4. 1975, p. 1 and OJ No C 133, 3. 6. 1981, p. 1.

ANNEX

TERMS REFERRED TO IN ARTICLE 3 (3) 1. Terms which have the object or effect of:

(a) excluding or limiting the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier;

(b) inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations, including the option of offsetting a debt owed to the seller or supplier against any claim which the consumer may have against him;

(c) making an agreement binding on the consumer whereas provision of services by the seller or supplier is subject to a condition whose realization depends on his own will alone;

(d) permitting the seller or supplier to retain sums paid by the consumer where the latter decides not to conclude or perform the contract, without providing for the consumer to receive compensation of an equivalent amount from the seller or supplier where the latter is the party cancelling the contract;

(e) requiring any consumer who fails to fulfil his obligation to pay a disproportionately high sum in compensation;

(f) authorizing the seller or supplier to dissolve the contract on a discretionary basis where the same facility is not granted to the consumer, or permitting the seller or supplier to retain the sums paid for services not yet supplied by him where it is the seller or supplier himself who dissolves the contract;

(g) enabling the seller or supplier to terminate a contract of indeterminate duration without reasonable notice except where there are serious grounds for doing so;

(h) automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early;

(i) irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract;

(j) enabling the seller or supplier to alter the terms of the contract unilaterally without a valid reason which is specified in the contract;

(k) enabling the seller or supplier to alter unilaterally without a valid reason any characteristics of the product or service to be provided;

(l) providing for the price of goods to be determined at the time of delivery or allowing a seller of goods or supplier of services to increase their price without in both cases giving the consumer the corresponding right to cancel the contract if the final price is too high in relation to the price agreed when the contract was concluded;

(m) giving the seller or supplier the right to determine whether the goods or services supplied are in conformity with the contract, or giving him the exclusive right to interpret any term of the contract;

(n) limiting the seller's or supplier's obligation to respect commitments undertaken by his agents or making his commitments subject to compliance with a particular formality;

(o) obliging the consumer to fulfil all his obligations where the seller or supplier does not perform his;

(p) giving the seller or supplier the possibility of transferring his rights and obligations under the contract, where this may serve to reduce the guarantees for the consumer, without the latter's agreement;

(q) excluding or hindering the consumer's right to take legal action or exercise any other legal remedy, particularly by requiring the consumer to take disputes exclusively to

arbitration not covered by legal provisions, unduly restricting the evidence available to him or imposing on him a burden of proof which, according to the applicable law, should lie with another party to the contract.

2. Scope of subparagraphs (g), (j) and (l)

(a) Subparagraph (g) is without hindrance to terms by which a supplier of financial services reserves the right to terminate unilaterally a contract of indeterminate duration without notice where there is a valid reason, provided that the supplier is required to inform the other contracting party or parties thereof immediately.

(b) Subparagraph (j) is without hindrance to terms under which a supplier of financial services reserves the right to alter the rate of interest payable by the consumer or due to the latter, or the amount of other charges for financial services without notice where there is a valid reason, provided that the supplier is required to inform the other contracting party or parties thereof at the earliest opportunity and that the latter are free to dissolve the contract immediately.

Subparagraph (j) is also without hindrance to terms under which a seller or supplier reserves the right to alter unilaterally the conditions of a contract of indeterminate duration, provided that he is required to inform the consumer with reasonable notice and that the consumer is free to dissolve the contract.

(c) Subparagraphs (g), (j) and (l) do not apply to:

- transactions in transferable securities, financial instruments and other products or services where the price is linked to fluctuations in a stock exchange quotation or index or a financial market rate that the seller or supplier does not control;

- contracts for the purchase or sale of foreign currency, traveller's cheques or international money orders denominated in foreign currency;

(d) Subparagraph (l) is without hindrance to price-indexation clauses, where lawful, provided that the method by which prices vary is explicitly described.

Relevant case law on unfair terms in consumer contracts

C-243/08, Pannon GSM Zrt. v Erzsébet Sustikné Gyórfi,

Summary of the Judgment

1. Approximation of laws – Unfair terms in consumer contracts – Directive 93/13
(Council Directive 93/13, Art. 6)

2. Approximation of laws – Unfair terms in consumer contracts – Directive 93/13
(Council Directive 93/13)

3. Approximation of laws – Unfair terms in consumer contracts – Directive 93/13
(Council Directive 93/13, Art. 3)

1. Article 6(1) of Council Directive 93/13 on unfair terms in consumer contracts must be interpreted as meaning that an unfair contract term is not binding on the consumer, and it is not necessary, in that regard, for that consumer to have successfully contested the validity of such a term beforehand.

The aim of Article 6 of that Directive, which is to strengthen consumer protection, would not be achieved if the consumer were himself obliged to raise the unfairness of contractual terms. In addition, effective protection of the consumer may be

attained only if the national court acknowledges that it has power to evaluate terms of this kind of its own motion.
(see paras 23, 28, operative part 1)

2. The national court is required to examine, of its own motion, the unfairness of a contractual term where it has available to it the legal and factual elements necessary for that task. Where it considers such a term to be unfair, it must not apply it, except if the consumer opposes that non-application. That duty is also incumbent on the national court when it is ascertaining its own territorial jurisdiction.

The court seized of the action is required to ensure the effectiveness of the protection intended to be given by the provisions of Directive 93/13 on unfair terms in consumer contracts. Consequently, the role thus attributed to the national court by Community law in this area is not limited to a mere power to rule on the possible unfairness of a contractual term, but also consists of the obligation to examine that issue of its own motion, where it has available to it the legal and factual elements necessary for that task, including when it is assessing whether it has territorial jurisdiction. In carrying out that obligation, the national court is not, however, required under that Directive to exclude the possibility that the term in question may be applicable, if the consumer, after having been informed of it by that court, does not intend to assert its unfair or non-binding status.

(see paras 32-33, 35, operative part 2)

3. It is for the national court to determine whether a contractual term, such as a term conferring jurisdiction, satisfies the criteria to be categorised as unfair within the meaning of Article 3(1) of Directive 93/13 on unfair terms in consumer contracts. In so doing, the national court must take account of the fact that a term, contained in a contract concluded between a consumer and a seller or supplier, which

has been included without being individually negotiated and which confers exclusive jurisdiction on the court in the territorial jurisdiction of which the seller or supplier has his principal place of business, may be considered to be unfair. (see para. 44, operative part 3)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof, Having regard to the proposal from the Commission(1), Having regard to the opinion of the Economic and Social Committee(2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(1) The European Union is seeking to forge ever closer links between the States and peoples of Europe, to ensure economic and social progress; in accordance with Article 14(2) of the Treaty, the internal market comprises an area without internal frontiers in which the free movements of goods, services and the freedom of establishment are ensured; the development of information society services within the area without internal frontiers is vital to eliminating the barriers which divide the European peoples.

(2) The development of electronic commerce within the information society offers significant employment opportunities in the Community, particularly in small and medium-sized enterprises, and will stimulate economic growth and investment in innovation by European companies, and can also enhance the competitiveness of European industry, provided that everyone has access to the Internet.

(3) Community law and the characteristics of the Community legal order are a vital asset to enable European citizens and operators to take full advantage, without consideration of borders, of the opportunities afforded by electronic commerce; this Directive therefore has the purpose of ensuring a high level of Community legal integration in order to establish a real area without internal borders for information society services.

(4) It is important to ensure that electronic commerce could fully benefit from the internal market and therefore that, as with Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, Regulation or administrative action in Member States concerning the pursuit of television broadcasting activities(4), a high level of Community integration is achieved.

(5) The development of information society services within the Community is hampered by a number of legal obstacles to the proper functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services; these obstacles arise from

divergences in legislation and from the legal uncertainty as to which national rules apply to such services; in the absence of coordination and adjustment of legislation in the relevant areas, obstacles might be justified in the light of the case-law of the Court of Justice of the European Communities; legal uncertainty exists with regard to the extent to which Member States may control services originating from another Member State.

(6) In the light of Community objectives, of Articles 43 and 49 of the Treaty and of secondary Community law, these obstacles should be eliminated by coordinating certain national laws and by clarifying certain legal concepts at Community level to the extent necessary for the proper functioning of the internal market; by dealing only with certain specific matters which give rise to problems for the internal market, this Directive is fully consistent with the need to respect the principle of subsidiarity as set out in Article 5 of the Treaty.

(7) In order to ensure legal certainty and consumer confidence, this Directive must lay down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market.

(8) The objective of this Directive is to create a legal framework to ensure the free movement of information society services between Member States and not to harmonise the field of criminal law as such.

(9) The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, Directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.

(10) In accordance with the principle of proportionality, the measures provided for in this Directive are strictly limited to the minimum needed to achieve the objective of the proper functioning of the internal market; where action at Community level is necessary, and in order to guarantee an area which is truly without internal frontiers as far as electronic commerce is concerned, the Directive must ensure a high level of protection of objectives of general interest, in particular the protection of minors and human dignity, consumer protection and the

protection of public health; according to Article 152 of the Treaty, the protection of public health is an essential component of other Community policies.

(11) This Directive is without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts; amongst others, Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts(5) and Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts(6) form a vital element for protecting consumers in contractual matters; those Directives also apply in their entirety to information society services; that same Community acquis, which is fully applicable to information society services, also embraces in particular Council Directive 84/450/EEC of 10 September 1984 concerning misleading and comparative advertising(7), Council Directive 87/102/EEC of 22 December 1986 for the approximation of the laws, Regulations and administrative provisions of the Member States concerning consumer credit(8), Council Directive 93/22/EEC of 10 May 1993 on investment services in the securities field(9), Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours(10), Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer production in the indication of prices of products offered to consumers(11), Council Directive 92/59/EEC of 29 June 1992 on general product safety(12), Directive 94/47/EC of the European Parliament and of the Council of 26 October 1994 on the protection of purchasers in respect of certain aspects on contracts relating to the purchase of the right to use immovable properties on a timeshare basis(13), Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests(14), Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, Regulations and administrative provisions concerning liability for defective products(15), Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees(16), the future Directive of the European Parliament and of the Council concerning the distance marketing of consumer financial services and Council Directive 92/28/EEC of 31 March 1992 on the advertising of medicinal products(17); this Directive should be without prejudice to Directive 98/43/EC of the European Parliament and of the Council of 6 July 1998 on the approximation of the laws, Regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products(18) adopted within the framework of the internal market, or to Directives on the protection of public health; this Directive complements information requirements established by the abovementioned Directives and in particular Directive 97/7/EC.

(12) It is necessary to exclude certain activities from the scope of this Directive, on the grounds that the freedom to provide services in these fields cannot, at this stage, be guaranteed under the Treaty or existing secondary legislation; excluding these activities does not preclude any instruments which might prove necessary for the proper functioning of the internal market; taxation, particularly value added tax imposed on a large number of the services covered by this Directive, must be excluded from the scope of this Directive.

(13) This Directive does not aim to establish rules on fiscal obligations nor does it pre-empt the drawing up of Community instruments concerning fiscal aspects of electronic commerce.

(14) The protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(19) and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(20) which are fully applicable to information society services; these Directives already establish

a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet.

(15) The confidentiality of communications is guaranteed by Article 5 Directive 97/66/EC; in accordance with that Directive, Member States must prohibit any kind of interception or surveillance of such communications by others than the senders and receivers, except when legally authorised.

(16) The exclusion of gambling activities from the scope of application of this Directive covers only games of chance, lotteries and betting transactions, which involve wagering a stake with monetary value; this does not cover promotional competitions or games where the purpose is to encourage the sale of goods or services and where payments, if they arise, serve only to acquire the promoted goods or services.

(17) The definition of information society services already exists in Community law in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and Regulations and of rules on information society services(21) and in Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access(22); this definition covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service; those services referred to in the indicative list in Annex V to Directive 98/34/EC which do not imply data processing and storage are not covered by this definition.

(18) Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line; activities such as the delivery of goods as such or the provision of services off-line are not covered; information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service; television broadcasting within the meaning of Directive EEC/89/552 and radio broadcasting are not information society services because they are not provided at individual request; by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services; the use of electronic mail or equivalent individual communications for instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service; activities which by their very nature cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient are not information society services.

(19) The place at which a service provider is established should be determined in conformity with the case-law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period; this requirement

is also fulfilled where a company is constituted for a given period; the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.

(20) The definition of "recipient of a service" covers all types of usage of information society services, both by persons who provide information on open networks such as the Internet and by persons who seek information on the Internet for private or professional reasons.

(21) The scope of the coordinated field is without prejudice to future Community harmonisation relating to information society services and to future legislation adopted at national level in accordance with Community law; the coordinated field covers only requirements relating to on-line activities such as on-line information, on-line advertising, on-line shopping, on-line contracting and does not concern Member States' legal requirements relating to goods such as safety standards, labelling obligations, or liability for goods, or Member States' requirements relating to the delivery or the transport of goods, including the distribution of medicinal products; the coordinated field does not cover the exercise of rights of pre-emption by public authorities concerning certain goods such as works of art.

(22) Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens; in order to improve mutual trust between Member States, it is essential to state clearly this responsibility on the part of the Member State where the services originate; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, such information society services should in principle be subject to the law of the Member State in which the service provider is established.

(23) This Directive neither aims to establish additional rules on private international law relating to conflicts of law nor does it deal with the jurisdiction of Courts; provisions of the applicable law designated by rules of private international law must not restrict the freedom to provide information society services as established in this Directive.

(24) In the context of this Directive, notwithstanding the rule on the control at source of information society services, it is legitimate under the conditions established in this Directive for Member States to take measures to restrict the free movement of information society services.

(25) National courts, including civil courts, dealing with private law disputes can take measures to derogate from the freedom to provide information society services in conformity with conditions established in this Directive.

(26) Member States, in conformity with conditions established in this Directive, may apply their national rules on criminal law and criminal proceedings with a view to taking all investigative and other measures necessary for the detection and prosecution of criminal offences, without there being a need to notify such measures to the Commission.

(27) This Directive, together with the future Directive of the European Parliament and of the Council concerning the distance marketing of consumer financial services, contributes to the creating of a legal framework for the on-line provision of financial services; this Directive does not pre-empt future initiatives in the area of financial services in particular with regard to the harmonisation of rules of conduct in this field; the possibility for Member States, established in this Directive, under certain circumstances of restricting the freedom to

provide information society services in order to protect consumers also covers measures in the area of financial services in particular measures aiming at protecting investors. (28) The Member States' obligation not to subject access to the activity of an information society service provider to prior authorisation does not concern postal services covered by Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service⁽²³⁾ consisting of the physical delivery of a printed electronic mail message and does not affect voluntary accreditation systems, in particular for providers of electronic signature certification service.

(29) Commercial communications are essential for the financing of information society services and for developing a wide variety of new, charge-free services; in the interests of consumer protection and fair trading, commercial communications, including discounts, promotional offers and promotional competitions or games, must meet a number of transparency requirements; these requirements are without prejudice to Directive 97/7/EC; this Directive should not affect existing Directives on commercial communications, in particular Directive 98/43/EC.

(30) The sending of unsolicited commercial communications by electronic mail may be undesirable for consumers and information society service providers and may disrupt the smooth functioning of interactive networks; the question of consent by recipient of certain forms of unsolicited commercial communications is not addressed by this Directive, but has already been addressed, in particular, by Directive 97/7/EC and by Directive 97/66/EC; in Member States which authorise unsolicited commercial communications by electronic mail, the setting up of appropriate industry filtering initiatives should be encouraged and facilitated; in addition it is necessary that in any event unsolicited commercial communities are clearly identifiable as such in order to improve transparency and to facilitate the functioning of such industry initiatives; unsolicited commercial communications by electronic mail should not result in additional communication costs for the recipient.

(31) Member States which allow the sending of unsolicited commercial communications by electronic mail without prior consent of the recipient by service providers established in their territory have to ensure that the service providers consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

(32) In order to remove barriers to the development of cross-border services within the Community which members of the regulated professions might offer on the Internet, it is necessary that compliance be guaranteed at Community level with professional rules aiming, in particular, to protect consumers or public health; codes of conduct at Community level would be the best means of determining the rules on professional ethics applicable to commercial communication; the drawing-up or, where appropriate, the adaptation of such rules should be encouraged without prejudice to the autonomy of professional bodies and associations.

(33) This Directive complements Community law and national law relating to regulated professions maintaining a coherent set of applicable rules in this field.

(34) Each Member State is to amend its legislation containing requirements, and in particular requirements as to form, which are likely to curb the use of contracts by electronic means; the examination of the legislation requiring such adjustment should be systematic and should cover all the necessary stages and acts of the contractual process, including the filing of the contract; the result of this amendment should be to make contracts concluded electronically workable; the legal effect of electronic signatures is dealt with by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures⁽²⁴⁾; the acknowledgement of receipt by a service

provider may take the form of the on-line provision of the service paid for.

(35) This Directive does not affect Member States' possibility of maintaining or establishing general or specific legal requirements for contracts which can be fulfilled by electronic means, in particular requirements concerning secure electronic signatures.

(36) Member States may maintain restrictions for the use of electronic contracts with regard to contracts requiring by law the involvement of courts, public authorities, or professions exercising public authority; this possibility also covers contracts which require the involvement of courts, public authorities, or professions exercising public authority in order to have an effect with regard to third parties as well as contracts requiring by law certification or attestation by a notary.

(37) Member States' obligation to remove obstacles to the use of electronic contracts concerns only obstacles resulting from legal requirements and not practical obstacles resulting from the impossibility of using electronic means in certain cases.

(38) Member States' obligation to remove obstacles to the use of electronic contracts is to be implemented in conformity with legal requirements for contracts enshrined in Community law.

(39) The exceptions to the provisions concerning the contracts concluded exclusively by electronic mail or by equivalent individual communications provided for by this Directive, in relation to information to be provided and the placing of orders, should not enable, as a result, the by-passing of those provisions by providers of information society services.

(40) Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.

(41) This Directive strikes a balance between the different interests at stake and establishes principles upon which industry agreements and standards can be based.

(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

(43) A service provider can benefit from the exemptions for "mere conduit" and for "caching" when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.

(44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as

a result cannot benefit from the liability exemptions established for these activities.

(45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.

(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.

(47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.

(48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

(49) Member States and the Commission are to encourage the drawing-up of codes of conduct; this is not to impair the voluntary nature of such codes and the possibility for interested parties of deciding freely whether to adhere to such codes.

(50) It is important that the proposed Directive on the harmonisation of certain aspects of copyright and related rights in the information society and this Directive come into force within a similar time scale with a view to establishing a clear framework of rules relevant to the issue of liability of intermediaries for copyright and relating rights infringements at Community level.

(51) Each Member State should be required, where necessary, to amend any legislation which is liable to hamper the use of schemes for the out-of-court settlement of disputes through electronic channels; the result of this amendment must be to make the functioning of such schemes genuinely and effectively possible in law and in practice, even across borders.

(52) The effective exercise of the freedoms of the internal market makes it necessary to guarantee victims effective access to means of settling disputes; damage which may arise in connection with information society services is characterised both by its rapidity and by its geographical extent; in view of this specific character and the need to ensure that national authorities do not endanger the mutual confidence which they should have in one another, this Directive requests Member States to ensure that appropriate court actions are available; Member States should examine the need to provide access to judicial procedures by appropriate electronic means.

(53) Directive 98/27/EC, which is applicable to information society services, provides a mechanism relating to actions for an injunction aimed at the protection of the collective interests of consumers; this mechanism will contribute to the free movement of information society services by ensuring a high level of consumer protection.

(54) The sanctions provided for under this Directive are without prejudice to any other sanction or remedy provided under national law; Member States are not obliged to provide criminal sanctions for infringement of national provisions adopted pursuant to this Directive.

(55) This Directive does not affect the law applicable to contractual obligations relating to consumer contracts;

accordingly, this Directive cannot have the result of depriving the consumer of the protection afforded to him by the mandatory rules relating to contractual obligations of the law of the Member State in which he has his habitual residence.

(56) As regards the derogation contained in this Directive regarding contractual obligations concerning contracts concluded by consumers, those obligations should be interpreted as including information on the essential elements of the content of the contract, including consumer rights, which have a determining influence on the decision to contract.

(57) The Court of Justice has consistently held that a Member State retains the right to take measures against a service provider that is established in another Member State but directs all or most of his activity to the territory of the first Member State if the choice of establishment was made with a view to evading the legislation that would have applied to the provider had he been established on the territory of the first Member State.

(58) This Directive should not apply to services supplied by service providers established in a third country; in view of the global dimension of electronic commerce, it is, however, appropriate to ensure that the Community rules are consistent with international rules; this Directive is without prejudice to the results of discussions within international organisations (amongst others WTO, OECD, Uncitral) on legal issues.

(59) Despite the global nature of electronic communications, coordination of national regulatory measures at European Union level is necessary in order to avoid fragmentation of the internal market, and for the establishment of an appropriate European regulatory framework; such coordination should also contribute to the establishment of a common and strong negotiating position in international forums.

(60) In order to allow the unhampered development of electronic commerce, the legal framework must be clear and simple, predictable and consistent with the rules applicable at international level so that it does not adversely affect the competitiveness of European industry or impede innovation in that sector.

(61) If the market is actually to operate by electronic means in the context of globalisation, the European Union and the major non-European areas need to consult each other with a view to making laws and procedures compatible.

(62) Cooperation with third countries should be strengthened in the area of electronic commerce, in particular with applicant countries, the developing countries and the European Union's other trading partners.

(63) The adoption of this Directive will not prevent the Member States from taking into account the various social, societal and cultural implications which are inherent in the advent of the information society; in particular it should not hinder measures which Member States might adopt in conformity with Community law to achieve social, cultural and democratic goals taking into account their linguistic diversity, national and regional specificities as well as their cultural heritage, and to ensure and maintain public access to the widest possible range of information society services; in any case, the development of the information society is to ensure that Community citizens can have access to the cultural European heritage provided in the digital environment.

(64) Electronic communication offers the Member States an excellent means of providing public services in the cultural, educational and linguistic fields.

(65) The Council, in its resolution of 19 January 1999 on the consumer dimension of the information society⁽²⁵⁾, stressed that the protection of consumers deserved special attention in this field; the Commission will examine the degree to which existing consumer protection rules provide insufficient protection in the context of the information society and will identify, where necessary, the deficiencies of this legislation and those issues which could require additional measures; if need be, the Commission should make specific additional proposals to resolve such deficiencies that will thereby have been identified,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Objective and scope

1. This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.

2. This Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.

3. This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.

4. This Directive does not establish additional rules on private international law nor does it deal with the jurisdiction of Courts.

5. This Directive shall not apply to:

- (a) the field of taxation;
- (b) questions relating to information society services covered by Directives 95/46/EC and 97/66/EC;
- (c) questions relating to agreements or practices governed by cartel law;
- (d) the following activities of information society services:
 - the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority,
 - the representation of a client and defence of his interests before the courts,
 - gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

6. This Directive does not affect measures taken at Community or national level, in the respect of Community law, in order to promote cultural and linguistic diversity and to ensure the defence of pluralism.

Article 2

Definitions

For the purpose of this Directive, the following terms shall bear the following meanings:

- (a) "information society services": services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC;
- (b) "service provider": any natural or legal person providing an information society service;
- (c) "established service provider": a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider;
- (d) "recipient of the service": any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible;
- (e) "consumer": any natural person who is acting for purposes which are outside his or her trade, business or profession;
- (f) "commercial communication": any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession. The following do not in themselves constitute commercial communications:
 - information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address,

- communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration;

(g) "regulated profession": any profession within the meaning of either Article 1(d) of Council Directive 89/48/EEC of 21 December 1988 on a general system for the recognition of higher-education diplomas awarded on completion of professional education and training of at least three-years' duration(26) or of Article 1(f) of Council Directive 92/51/EEC of 18 June 1992 on a second general system for the recognition of professional education and training to supplement Directive 89/48/EEC(27);

(h) "coordinated field": requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.

(i) The coordinated field concerns requirements with which the service provider has to comply in respect of:

- the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification,

- the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider;

(ii) The coordinated field does not cover requirements such as:

- requirements applicable to goods as such,
- requirements applicable to the delivery of goods,
- requirements applicable to services not provided by electronic means.

Article 3

Internal market

1. Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.

2. Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.

3. Paragraphs 1 and 2 shall not apply to the fields referred to in the Annex.

4. Member States may take measures to derogate from paragraph 2 in respect of a given information society service if the following conditions are fulfilled:

(a) the measures shall be:

(i) necessary for one of the following reasons:

- public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons,

- the protection of public health,

- public security, including the safeguarding of national security and defence,

- the protection of consumers, including investors;

(ii) taken against a given information society service which prejudices the objectives referred to in point (i) or which presents a serious and grave risk of prejudice to those objectives;

(iii) proportionate to those objectives;

(b) before taking the measures in question and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the Member State has:

- asked the Member State referred to in paragraph 1 to take measures and the latter did not take such measures, or they were inadequate,

- notified the Commission and the Member State referred to in paragraph 1 of its intention to take such measures.

5. Member States may, in the case of urgency, derogate from the conditions stipulated in paragraph 4(b). Where this is the case, the measures shall be notified in the shortest possible time to the Commission and to the Member State referred to in paragraph 1, indicating the reasons for which the Member State considers that there is urgency.

6. Without prejudice to the Member State's possibility of proceeding with the measures in question, the Commission shall examine the compatibility of the notified measures with Community law in the shortest possible time; where it comes to the conclusion that the measure is incompatible with Community law, the Commission shall ask the Member State in question to refrain from taking any proposed measures or urgently to put an end to the measures in question.

CHAPTER II

PRINCIPLES

Section 1: Establishment and information requirements

Article 4

Principle excluding prior authorisation

1. Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect.

2. Paragraph 1 shall be without prejudice to authorisation schemes which are not specifically and exclusively targeted at information society services, or which are covered by Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorisations and individual licences in the field of telecommunications services(28).

Article 5

General information to be provided

1. In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information:

(a) the name of the service provider;

(b) the geographic address at which the service provider is established;

(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

(e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

(f) as concerns the regulated professions:

- any professional body or similar institution with which the service provider is registered,

- the professional title and the Member State where it has been granted,

- a reference to the applicable professional rules in the Member State of establishment and the means to access them;

(g) where the service provider undertakes an activity that is subject to VAT, the identification number referred to in Article 22(1) of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment(29).

2. In addition to other information requirements established by Community law, Member States shall at least ensure that, where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs.

Section 2: Commercial communications

Article 6

Information to be provided

In addition to other information requirements established by Community law, Member States shall ensure that commercial communications which are part of, or constitute, an

information society service comply at least with the following conditions:

- (a) the commercial communication shall be clearly identifiable as such;
- (b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
- (c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;
- (d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

Article 7

Unsolicited commercial communication

1. In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.
2. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

Article 8

Regulated professions

1. Member States shall ensure that the use of commercial communications which are part of, or constitute, an information society service provided by a member of a regulated profession is permitted subject to compliance with the professional rules regarding, in particular, the independence, dignity and honour of the profession, professional secrecy and fairness towards clients and other members of the profession.
2. Without prejudice to the autonomy of professional bodies and associations, Member States and the Commission shall encourage professional associations and bodies to establish codes of conduct at Community level in order to determine the types of information that can be given for the purposes of commercial communication in conformity with the rules referred to in paragraph 1.
3. When drawing up proposals for Community initiatives which may become necessary to ensure the proper functioning of the Internal Market with regard to the information referred to in paragraph 2, the Commission shall take due account of codes of conduct applicable at Community level and shall act in close cooperation with the relevant professional associations and bodies.
4. This Directive shall apply in addition to Community Directives concerning access to, and the exercise of, activities of the regulated professions.

Section 3: Contracts concluded by electronic means

Article 9

Treatment of contracts

1. Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.
2. Member States may lay down that paragraph 1 shall not apply to all or certain contracts falling into one of the following categories:
 - (a) contracts that create or transfer rights in real estate, except for rental rights;

- (b) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;
- (c) contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession;
- (d) contracts governed by family law or by the law of succession.

3. Member States shall indicate to the Commission the categories referred to in paragraph 2 to which they do not apply paragraph 1. Member States shall submit to the Commission every five years a report on the application of paragraph 2 explaining the reasons why they consider it necessary to maintain the category referred to in paragraph 2(b) to which they do not apply paragraph 1.

Article 10

Information to be provided

1. In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:
 - (a) the different technical steps to follow to conclude the contract;
 - (b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible;
 - (c) the technical means for identifying and correcting input errors prior to the placing of the order;
 - (d) the languages offered for the conclusion of the contract.

2. Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically.

3. Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

4. Paragraphs 1 and 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

Article 11

Placing of the order

1. Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means, the following principles apply:

- the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means,
- the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.

2. Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.

3. Paragraph 1, first indent, and paragraph 2 shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

Section 4: Liability of intermediary service providers

Article 12

"Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

- (a) does not initiate the transmission;
- (b) does not select the receiver of the transmission; and
- (c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13 "Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

- (a) the provider does not modify the information;
- (b) the provider complies with conditions on access to the information;
- (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
- (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14 Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

- (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15

No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or

obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

CHAPTER III IMPLEMENTATION

Article 16

Codes of conduct

1. Member States and the Commission shall encourage:

- (a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15;
- (b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;
- (c) the accessibility of these codes of conduct in the Community languages by electronic means;
- (d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce;
- (e) the drawing up of codes of conduct regarding the protection of minors and human dignity.

2. Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests and drawn up in accordance with paragraph 1(a). Where appropriate, to take account of their specific needs, associations representing the visually impaired and disabled should be consulted.

Article 17

Out-of-court dispute settlement

1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means.

2. Member States shall encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned.

3. Member States shall encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decisions they take regarding information society services and to transmit any other information on the practices, usages or customs relating to electronic commerce.

Article 18

Court actions

1. Member States shall ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

2. The Annex to Directive 98/27/EC shall be supplemented as follows:

"11. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects on information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1)."

Article 19

Cooperation

1. Member States shall have adequate means of supervision and investigation necessary to implement this Directive effectively and shall ensure that service providers supply them with the requisite information.

2. Member States shall cooperate with other Member States; they shall, to that end, appoint one or several contact points, whose details they shall communicate to the other Member States and to the Commission.

3. Member States shall, as quickly as possible, and in conformity with national law, provide the assistance and information

requested by other Member States or by the Commission, including by appropriate electronic means.

4. Member States shall establish contact points which shall be accessible at least by electronic means and from which recipients and service providers may:

(a) obtain general information on contractual rights and obligations as well as on the complaint and redress mechanisms available in the event of disputes, including practical aspects involved in the use of such mechanisms;

(b) obtain the details of authorities, associations or organisations from which they may obtain further information or practical assistance.

5. Member States shall encourage the communication to the Commission of any significant administrative or judicial decisions taken in their territory regarding disputes relating to information society services and practices, usages and customs relating to electronic commerce. The Commission shall communicate these decisions to the other Member States.

Article 20

Sanctions

Member States shall determine the sanctions applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are enforced. The sanctions they provide for shall be effective, proportionate and dissuasive.

CHAPTER IV

FINAL PROVISIONS

Article 21

Re-examination

1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.

2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, "notice and take down" procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.

Article 22

Transposition

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive before 17 January 2002. They shall forthwith inform the Commission thereof.

2. When Member States adopt the measures referred to in paragraph 1, these shall contain a reference to this Directive or shall be accompanied by such reference at the time of their official publication. The methods of making such reference shall be laid down by Member States.

Article 23

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 24

Addressees

This Directive is addressed to the Member States.

Done at Luxembourg, 8 June 2000.

For the European Parliament

The President

N. Fontaine

For the Council

The President

G. d'Oliveira Martins

(1) OJ C 30, 5.2.1999, p. 4.

(2) OJ C 169, 16.6.1999, p. 36.

(3) Opinion of the European Parliament of 6 May 1999 (OJ C 279, 1.10.1999, p. 389), Council common position of 28 February 2000 (OJ C 128, 8.5.2000, p. 32) and Decision of the European Parliament of 4 May 2000 (not yet published in the Official Journal).

(4) OJ L 298, 17.10.1989, p. 23. Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30.7.1997, p. 60).

(5) OJ L 95, 21.4.1993, p. 29.

(6) OJ L 144, 4.6.1999, p. 19.

(7) OJ L 250, 19.9.1984, p. 17. Directive as amended by Directive 97/55/EC of the European Parliament and of the Council (OJ L 290, 23.10.1997, p. 18).

(8) OJ L 42, 12.2.1987, p. 48. Directive as last amended by Directive 98/7/EC of the European Parliament and of the Council (OJ L 101, 1.4.1998, p. 17).

(9) OJ L 141, 11.6.1993, p. 27. Directive as last amended by Directive 97/9/EC of the European Parliament and of the Council (OJ L 84, 26.3.1997, p. 22).

(10) OJ L 158, 23.6.1990, p. 59.

(11) OJ L 80, 18.3.1998, p. 27.

(12) OJ L 228, 11.8.1992, p. 24.

(13) OJ L 280, 29.10.1994, p. 83.

(14) OJ L 166, 11.6.1998, p. 51. Directive as amended by Directive 1999/44/EC (OJ L 171, 7.7.1999, p. 12).

(15) OJ L 210, 7.8.1985, p. 29. Directive as amended by Directive 1999/34/EC (OJ L 141, 4.6.1999, p. 20).

(16) OJ L 171, 7.7.1999, p. 12.

(17) OJ L 113, 30.4.1992, p. 13.

(18) OJ L 213, 30.7.1998, p. 9.

(19) OJ L 281, 23.11.1995, p. 31.

(20) OJ L 24, 30.1.1998, p. 1.

(21) OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

(22) OJ L 320, 28.11.1998, p. 54.

(23) OJ L 15, 21.1.1998, p. 14.

(24) OJ L 13, 19.1.2000, p. 12.

(25) OJ C 23, 28.1.1999, p. 1.

(26) OJ L 19, 24.1.1989, p. 16.

(27) OJ L 209, 24.7.1992, p. 25. Directive as last amended by Commission Directive 97/38/EC (OJ L 184, 12.7.1997, p. 31).

(28) OJ L 117, 7.5.1997, p. 15.

(29) OJ L 145, 13.6.1977, p. 1. Directive as last amended by Directive 1999/85/EC (OJ L 277, 28.10.1999, p. 34).

ANNEX

DEROGATIONS FROM ARTICLE 3

As provided for in Article 3(3), Article 3(1) and (2) do not apply to:

- copyright, neighbouring rights, rights referred to in Directive 87/54/EEC(1) and Directive 96/9/EC(2) as well as industrial property rights,

- the emission of electronic money by institutions in respect of which Member States have applied one of the derogations provided for in Article 8(1) of Directive 2000/46/EC(3),

- Article 44(2) of Directive 85/611/EEC(4),

- Article 30 and Title IV of Directive 92/49/EEC(5), Title IV of Directive 92/96/EEC(6), Articles 7 and 8 of Directive 88/357/EEC(7) and Article 4 of Directive 90/619/EEC(8),

- the freedom of the parties to choose the law applicable to their contract,

- contractual obligations concerning consumer contacts,

- formal validity of contracts creating or transferring rights in real estate where such contracts are subject to mandatory formal requirements of the law of the Member State where the real estate is situated,

- the permissibility of unsolicited commercial communications by electronic mail.

(1) OJ L 24, 27.1.1987, p. 36.

(2) OJ L 77, 27.3.1996, p. 20.

(3) Not yet published in the Official Journal.

(4) OJ L 375, 31.12.1985, p. 3. Directive as last amended by Directive 95/26/EC (OJ L 168, 18.7.1995, p. 7).

(5) OJ L 228, 11.8.1992, p. 1. Directive as last amended by Directive 95/26/EC.

(6) OJ L 360, 9.12.1992, p. 2. Directive as last amended by Directive 95/26/EC.

(7) OJ L 172, 4.7.1988, p. 1. Directive as last amended by Directive 92/49/EC.

Relevant Case Law on Directive 2000/31/EC on electronic commerce

C-244/06, Dynamic Medien Vertriebs GmbH v Avides Media AG, THE COURT (Third Chamber),

Summary of the Judgment

Free movement of goods – Quantitative restrictions – Measures having equivalent effect

(Art. 28 EC)

National rules which prohibit the sale and transfer by mail order of image storage media which have not been examined and classified by a competent national authority or by a national voluntary self-regulatory body for the purposes of protecting young persons and which do not bear a label from that authority or body indicating the age from which they may be viewed, does not constitute a selling arrangement which is capable of hindering, directly or indirectly, actually or potentially intra-Community trade, but a measure having equivalent effect to quantitative restrictions within the meaning of Article 28 EC and is, in principle, incompatible with the obligations arising from that provision.

However, those rules may be compatible with that provision provided that they do not go beyond what is necessary to attain the objective of protecting children pursued by the Member State concerned, as will be the case where the rules do not preclude all forms of marketing of unchecked image storage media and where it is permissible to import and sell such image storage media to adults, while ensuring that children do not have access to them. It could be otherwise only if it appears that the procedure for examining, classifying and labelling image storage media established by those rules is not easily accessible or cannot be completed within a reasonable period or that the decision of refusal cannot be open to challenge before the courts.

(see paras 29, 32, 35, 42, 47-48, operative part)

C298/07, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v deutsche internet versicherung AG,

Summary of the Judgment

Approximation of laws – Electronic commerce – Directive 2000/31 – Supply of services via the internet

(European Parliament and Council Directive 2000/31, Art. 5(1)(c))

Article 5(1)(c) of Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the internal market must be interpreted as meaning that a service provider is required to supply to recipients of the service, before the conclusion of a contract with them, in addition to its electronic mail address, other information which allows the service provider to be contacted rapidly and communicated with in a direct and effective

manner. That information does not necessarily have to be a telephone number. That information may be in the form of an electronic enquiry template through which the recipients of the service can contact the service provider via the internet, to whom the service provider replies by electronic mail except in situations where a recipient of the service, who, after contacting the service provider electronically, finds himself without access to the electronic network, requests the latter to provide access to another, non-electronic, means of communication.

(see para. 40, operative part)

C-509/09 and C-161/10 (Joined Cases) eDate Advertising GmbH v X, Olivier Martinez, Robert Martinez v MGN Limited

Operative part of the judgment

1. Article 5(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that, in the event of an alleged infringement of personality rights by means of content placed online on an internet website, the person who considers that his rights have been infringed has the option of bringing an action for liability, in respect of all the damage caused, either before the courts of the Member State in which the publisher of that content is established or before the courts of the Member State in which the centre of his interests is based. That person may also, instead of an action for liability in respect of all the damage caused, bring his action before the courts of each Member State in the territory of which content placed online is or has been accessible. Those courts have jurisdiction only in respect of the damage caused in the territory of the Member State of the court seised.

2. Article 3 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), must be interpreted as not requiring transposition in the form of a specific conflict-of-laws rule. Nevertheless, in relation to the coordinated field, Member States must ensure that, subject to the derogations authorised in accordance with the conditions set out in Article 3(4) of Directive 2000/31, the provider of an electronic commerce service is not made subject to stricter requirements than those provided for by the substantive law applicable in the Member State in which that service provider is established.

C 292/10, G v Cornelius de Visser,

Ruling:

1. In circumstances such as those in the main proceedings, Article 4(1) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and

enforcement of judgments in civil and commercial matters must be interpreted as meaning that it does not preclude the application of Article 5(3) of that Regulation to an action for liability arising from the operation of an Internet site against a defendant who is probably a European Union citizen but whose whereabouts are unknown if the court seised of the case does not hold firm evidence to support the conclusion that the defendant is in fact domiciled outside the European Union.

2. European Union law must be interpreted as meaning that it does not preclude the issue of judgment by default against a defendant on whom, given that it is impossible to locate him, the document instituting proceedings has been served by public notice under national law, provided that the court seised of the matter has first satisfied itself that all investigations required by the principles of diligence and good faith have been undertaken to trace the defendant.

3. European Union law must be interpreted as precluding certification as a European Enforcement Order, within the meaning of Regulation (EC) No 805/2004 of the European Parliament and of the Council of 21 April 2004 creating a European Enforcement Order for uncontested claims, of a judgment by default issued against a defendant whose address is unknown.

4. Article 3(1) and (2) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market does not apply to a situation where the place of establishment of the information society services provider is unknown, since application of that provision is subject to identification of the Member State in whose territory the service provider in question is actually established.

C-291/13 *Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis*

Ruling:

1. Article 2(a) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') must be interpreted as meaning that the concept of 'information society services', within the meaning of that provision, covers the provision of online information services

for which the service provider is remunerated, not by the recipient, but by income generated by advertisements posted on a website.

2. In a case such as that at issue in the main proceedings, Directive 2000/31 does not preclude the application of rules of civil liability for defamation.

3. The limitations of civil liability specified in Articles 12 to 14 of Directive 2000/31 do not apply to the case of a newspaper publishing company which operates a website on which the online version of a newspaper is posted, that company being, moreover, remunerated by income generated by commercial advertisements posted on that website, since it has knowledge of the information posted and exercises control over that information, whether or not access to that website is free of charge.

4. The limitations of civil liability specified in Articles 12 to 14 of Directive 2000/31 are capable of applying in the context of proceedings between individuals relating to civil liability for defamation, where the conditions referred to in those articles are satisfied.

5. Articles 12 to 14 of Directive 2000/31 do not allow information society service providers to oppose the bringing of legal proceedings for civil liability against them and, consequently, the adoption of a prohibitory injunction by a national court. The limitations of liability provided for in those articles may be invoked by the provider in accordance with the provisions of national law transposing them or, failing that, for the purpose of an interpretation of that law in conformity with the Directive. By contrast, in a case such as that in the main proceedings, Directive 2000/31 cannot, in itself, create obligations on the part of individuals and therefore cannot be relied on against those individuals.

Cases of partial relevance published in other parts of the reader:

C-322/01 - Deutscher Apothekerverband

C-244/06 - Dynamic Medien

C-275/06 - Promusicae

C-298/07 - Deutsche internet versicherung

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market ("Unfair Commercial Practices Directive")

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,
Having regard to the proposal from the Commission,
Having regard to the opinion of the European Economic and Social Committee [1],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [2],

Whereas:

(1) Article 153(1) and (3)(a) of the Treaty provides that the Community is to contribute to the attainment of a high level of consumer protection by the measures it adopts pursuant to Article 95 thereof.

(2) In accordance with Article 14(2) of the Treaty, the internal market comprises an area without internal frontiers in which

the free movement of goods and services and freedom of establishment are ensured. The development of fair commercial practices within the area without internal frontiers is vital for the promotion of the development of cross-border activities.

(3) The laws of the Member States relating to unfair commercial practices show marked differences which can generate appreciable distortions of competition and obstacles to the smooth functioning of the internal market. In the field of advertising, Council Directive 84/450/EEC of 10 September 1984 concerning misleading and comparative advertising [3] establishes minimum criteria for harmonising legislation on misleading advertising, but does not prevent the Member States from retaining or adopting measures which provide more extensive protection for consumers. As a result, Member States' provisions on misleading advertising diverge significantly.

(4) These disparities cause uncertainty as to which national rules apply to unfair commercial practices harming consumers' economic interests and create many barriers affecting business and consumers. These barriers increase the cost to business of exercising internal market freedoms, in particular when businesses wish to engage in cross border marketing, advertising campaigns and sales promotions. Such barriers also make consumers uncertain of their rights and undermine their confidence in the internal market.

(5) In the absence of uniform rules at Community level, obstacles to the free movement of services and goods across borders or the freedom of establishment could be justified in the light of the case-law of the Court of Justice of the European Communities as long as they seek to protect recognised public interest objectives and are proportionate to those objectives. In view of the Community's objectives, as set out in the provisions of the Treaty and in secondary Community law relating to freedom of movement, and in accordance with the Commission's policy on commercial communications as indicated in the Communication from the Commission entitled "The follow-up to the Green Paper on Commercial Communications in the Internal Market", such obstacles should be eliminated. These obstacles can only be eliminated by establishing uniform rules at Community level which establish a high level of consumer protection and by clarifying certain legal concepts at Community level to the extent necessary for the proper functioning of the internal market and to meet the requirement of legal certainty.

(6) This Directive therefore approximates the laws of the Member States on unfair commercial practices, including unfair advertising, which directly harm consumers' economic interests and thereby indirectly harm the economic interests of legitimate competitors. In line with the principle of proportionality, this Directive protects consumers from the consequences of such unfair commercial practices where they are material but recognises that in some cases the impact on consumers may be negligible. It neither covers nor affects the national laws on unfair commercial practices which harm only competitors' economic interests or which relate to a transaction between traders; taking full account of the principle of subsidiarity, Member States will continue to be able to regulate such practices, in conformity with Community law, if they choose to do so. Nor does this Directive cover or affect the provisions of Directive 84/450/EEC on advertising which misleads business but which is not misleading for consumers and on comparative advertising. Further, this Directive does not affect accepted advertising and marketing practices, such as legitimate product placement, brand differentiation or the offering of incentives which may legitimately affect consumers' perceptions of products and influence their behaviour without impairing the consumer's ability to make an informed decision.

(7) This Directive addresses commercial practices directly related to influencing consumers' transactional decisions in relation to products. It does not address commercial practices carried out primarily for other purposes, including for example commercial communication aimed at investors, such as annual reports and corporate promotional literature. It does not

address legal requirements related to taste and decency which vary widely among the Member States. Commercial practices such as, for example, commercial solicitation in the streets, may be undesirable in Member States for cultural reasons. Member States should accordingly be able to continue to ban commercial practices in their territory, in conformity with Community law, for reasons of taste and decency even where such practices do not limit consumers' freedom of choice. Full account should be taken of the context of the individual case concerned in applying this Directive, in particular the general clauses thereof.

(8) This Directive directly protects consumer economic interests from unfair business-to-consumer commercial practices. Thereby, it also indirectly protects legitimate businesses from their competitors who do not play by the rules in this Directive and thus guarantees fair competition in fields coordinated by it. It is understood that there are other commercial practices which, although not harming consumers, may hurt competitors and business customers. The Commission should carefully examine the need for Community action in the field of unfair competition beyond the remit of this Directive and, if necessary, make a legislative proposal to cover these other aspects of unfair competition.

(9) This Directive is without prejudice to individual actions brought by those who have been harmed by an unfair commercial practice. It is also without prejudice to Community and national rules on contract law, on intellectual property rights, on the health and safety aspects of products, on conditions of establishment and authorisation regimes, including those rules which, in conformity with Community law, relate to gambling activities, and to Community competition rules and the national provisions implementing them. The Member States will thus be able to retain or introduce restrictions and prohibitions of commercial practices on grounds of the protection of the health and safety of consumers in their territory wherever the trader is based, for example in relation to alcohol, tobacco or pharmaceuticals. Financial services and immovable property, by reason of their complexity and inherent serious risks, necessitate detailed requirements, including positive obligations on traders. For this reason, in the field of financial services and immovable property, this Directive is without prejudice to the right of Member States to go beyond its provisions to protect the economic interests of consumers. It is not appropriate to regulate here the certification and indication of the standard of fineness of articles of precious metal.

(10) It is necessary to ensure that the relationship between this Directive and existing Community law is coherent, particularly where detailed provisions on unfair commercial practices apply to specific sectors. This Directive therefore amends Directive 84/450/EEC, Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts [4], Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests [5] and Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services [6]. This Directive accordingly applies only in so far as there are no specific Community law provisions regulating specific aspects of unfair commercial practices, such as information requirements and rules on the way the information is presented to the consumer. It provides protection for consumers where there is no specific sectoral legislation at Community level and prohibits traders from creating a false impression of the nature of products. This is particularly important for complex products with high levels of risk to consumers, such as certain financial services products. This Directive consequently complements the Community acquis, which is applicable to commercial practices harming consumers' economic interests.

(11) The high level of convergence achieved by the approximation of national provisions through this Directive creates a high common level of consumer protection. This

Directive establishes a single general prohibition of those unfair commercial practices distorting consumers' economic behaviour. It also sets rules on aggressive commercial practices, which are currently not regulated at Community level.

(12) Harmonisation will considerably increase legal certainty for both consumers and business. Both consumers and business will be able to rely on a single regulatory framework based on clearly defined legal concepts regulating all aspects of unfair commercial practices across the EU. The effect will be to eliminate the barriers stemming from the fragmentation of the rules on unfair commercial practices harming consumer economic interests and to enable the internal market to be achieved in this area.

(13) In order to achieve the Community's objectives through the removal of internal market barriers, it is necessary to replace Member States' existing, divergent general clauses and legal principles. The single, common general prohibition established by this Directive therefore covers unfair commercial practices distorting consumers' economic behaviour. In order to support consumer confidence the general prohibition should apply equally to unfair commercial practices which occur outside any contractual relationship between a trader and a consumer or following the conclusion of a contract and during its execution. The general prohibition is elaborated by rules on the two types of commercial practices which are by far the most common, namely misleading commercial practices and aggressive commercial practices.

(14) It is desirable that misleading commercial practices cover those practices, including misleading advertising, which by deceiving the consumer prevent him from making an informed and thus efficient choice. In conformity with the laws and practices of Member States on misleading advertising, this Directive classifies misleading practices into misleading actions and misleading omissions. In respect of omissions, this Directive sets out a limited number of key items of information which the consumer needs to make an informed transactional decision. Such information will not have to be disclosed in all advertisements, but only where the trader makes an invitation to purchase, which is a concept clearly defined in this Directive. The full harmonisation approach adopted in this Directive does not preclude the Member States from specifying in national law the main characteristics of particular products such as, for example, collectors' items or electrical goods, the omission of which would be material when an invitation to purchase is made. It is not the intention of this Directive to reduce consumer choice by prohibiting the promotion of products which look similar to other products unless this similarity confuses consumers as to the commercial origin of the product and is therefore misleading. This Directive should be without prejudice to existing Community law which expressly affords Member States the choice between several regulatory options for the protection of consumers in the field of commercial practices. In particular, this Directive should be without prejudice to Article 13(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [7].

(15) Where Community law sets out information requirements in relation to commercial communication, advertising and marketing that information is considered as material under this Directive. Member States will be able to retain or add information requirements relating to contract law and having contract law consequences where this is allowed by the minimum clauses in the existing Community law instruments. A non-exhaustive list of such information requirements in the *acquis* is contained in Annex II. Given the full harmonisation introduced by this Directive only the information required in Community law is considered as material for the purpose of Article 7(5) thereof. Where Member States have introduced information requirements over and above what is specified in Community law, on the basis of minimum clauses, the omission of that extra information will not constitute a misleading omission under this Directive. By contrast Member States will

be able, when allowed by the minimum clauses in Community law, to maintain or introduce more stringent provisions in conformity with Community law so as to ensure a higher level of protection of consumers' individual contractual rights.

(16) The provisions on aggressive commercial practices should cover those practices which significantly impair the consumer's freedom of choice. Those are practices using harassment, coercion, including the use of physical force, and undue influence.

(17) It is desirable that those commercial practices which are in all circumstances unfair be identified to provide greater legal certainty. Annex I therefore contains the full list of all such practices. These are the only commercial practices which can be deemed to be unfair without a case-by-case assessment against the provisions of Articles 5 to 9. The list may only be modified by revision of the Directive.

(18) It is appropriate to protect all consumers from unfair commercial practices; however the Court of Justice has found it necessary in adjudicating on advertising cases since the enactment of Directive 84/450/EEC to examine the effect on a notional, typical consumer. In line with the principle of proportionality, and to permit the effective application of the protections contained in it, this Directive takes as a benchmark the average consumer, who is reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors, as interpreted by the Court of Justice, but also contains provisions aimed at preventing the exploitation of consumers whose characteristics make them particularly vulnerable to unfair commercial practices. Where a commercial practice is specifically aimed at a particular group of consumers, such as children, it is desirable that the impact of the commercial practice be assessed from the perspective of the average member of that group. It is therefore appropriate to include in the list of practices which are in all circumstances unfair a provision which, without imposing an outright ban on advertising directed at children, protects them from direct exhortations to purchase. The average consumer test is not a statistical test. National courts and authorities will have to exercise their own faculty of judgement, having regard to the case-law of the Court of Justice, to determine the typical reaction of the average consumer in a given case.

(19) Where certain characteristics such as age, physical or mental infirmity or credulity make consumers particularly susceptible to a commercial practice or to the underlying product and the economic behaviour only of such consumers is likely to be distorted by the practice in a way that the trader can reasonably foresee, it is appropriate to ensure that they are adequately protected by assessing the practice from the perspective of the average member of that group.

(20) It is appropriate to provide a role for codes of conduct, which enable traders to apply the principles of this Directive effectively in specific economic fields. In sectors where there are specific mandatory requirements regulating the behaviour of traders, it is appropriate that these will also provide evidence as to the requirements of professional diligence in that sector. The control exercised by code owners at national or Community level to eliminate unfair commercial practices may avoid the need for recourse to administrative or judicial action and should therefore be encouraged. With the aim of pursuing a high level of consumer protection, consumers' organisations could be informed and involved in the drafting of codes of conduct.

(21) Persons or organisations regarded under national law as having a legitimate interest in the matter must have legal remedies for initiating proceedings against unfair commercial practices, either before a court or before an administrative authority which is competent to decide upon complaints or to initiate appropriate legal proceedings. While it is for national law to determine the burden of proof, it is appropriate to enable courts and administrative authorities to require traders to produce evidence as to the accuracy of factual claims they have made.

(22) It is necessary that Member States lay down penalties for infringements of the provisions of this Directive and they must

ensure that these are enforced. The penalties must be effective, proportionate and dissuasive.

(23) Since the objectives of this Directive, namely to eliminate the barriers to the functioning of the internal market represented by national laws on unfair commercial practices and to provide a high common level of consumer protection, by approximating the laws, Regulations and administrative provisions of the Member States on unfair commercial practices, cannot be sufficiently achieved by the Member States and can therefore be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to eliminate the internal market barriers and achieve a high common level of consumer protection.

(24) It is appropriate to review this Directive to ensure that barriers to the internal market have been addressed and a high level of consumer protection achieved. The review could lead to a Commission proposal to amend this Directive, which may include a limited extension to the derogation in Article 3(5), and/or amendments to other consumer protection legislation reflecting the Commission's Consumer Policy Strategy commitment to review the existing acquis in order to achieve a high, common level of consumer protection.

(25) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Purpose

The purpose of this Directive is to contribute to the proper functioning of the internal market and achieve a high level of consumer protection by approximating the laws, Regulations and administrative provisions of the Member States on unfair commercial practices harming consumers' economic interests.

Article 2

Definitions

For the purposes of this Directive:

(a) "consumer" means any natural person who, in commercial practices covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession;

(b) "trader" means any natural or legal person who, in commercial practices covered by this Directive, is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader;

(c) "product" means any goods or service including immovable property, rights and obligations;

(d) "business-to-consumer commercial practices" (hereinafter also referred to as commercial practices) means any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers;

(e) "to materially distort the economic behaviour of consumers" means using a commercial practice to appreciably impair the consumer's ability to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken otherwise;

(f) "code of conduct" means an agreement or set of rules not imposed by law, Regulation or administrative provision of a Member State which defines the behaviour of traders who undertake to be bound by the code in relation to one or more particular commercial practices or business sectors;

(g) "code owner" means any entity, including a trader or group of traders, which is responsible for the formulation and revision of a code of conduct and/or for monitoring compliance with the code by those who have undertaken to be bound by it;

(h) "professional diligence" means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity;

(i) "invitation to purchase" means a commercial communication which indicates characteristics of the product and the price in a way appropriate to the means of the commercial communication used and thereby enables the consumer to make a purchase;

(j) "undue influence" means exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision;

(k) "transactional decision" means any decision taken by a consumer concerning whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting;

(l) "regulated profession" means a professional activity or a group of professional activities, access to which or the pursuit of which, or one of the modes of pursuing which, is conditional, directly or indirectly, upon possession of specific professional qualifications, pursuant to laws, Regulations or administrative provisions.

Article 3

Scope

1. This Directive shall apply to unfair business-to-consumer commercial practices, as laid down in Article 5, before, during and after a commercial transaction in relation to a product.

2. This Directive is without prejudice to contract law and, in particular, to the rules on the validity, formation or effect of a contract.

3. This Directive is without prejudice to Community or national rules relating to the health and safety aspects of products.

4. In the case of conflict between the provisions of this Directive and other Community rules regulating specific aspects of unfair commercial practices, the latter shall prevail and apply to those specific aspects.

5. For a period of six years from 12 June 2007, Member States shall be able to continue to apply national provisions within the field approximated by this Directive which are more restrictive or prescriptive than this Directive and which implement Directives containing minimum harmonisation clauses. These measures must be essential to ensure that consumers are adequately protected against unfair commercial practices and must be proportionate to the attainment of this objective. The review referred to in Article 18 may, if considered appropriate, include a proposal to prolong this derogation for a further limited period.

6. Member States shall notify the Commission without delay of any national provisions applied on the basis of paragraph 5.

7. This Directive is without prejudice to the rules determining the jurisdiction of the courts.

8. This Directive is without prejudice to any conditions of establishment or of authorisation regimes, or to the deontological codes of conduct or other specific rules governing regulated professions in order to uphold high standards of integrity on the part of the professional, which Member States may, in conformity with Community law, impose on professionals.

9. In relation to "financial services", as defined in Directive 2002/65/EC, and immovable property, Member States may impose requirements which are more restrictive or prescriptive than this Directive in the field which it approximates.

10. This Directive shall not apply to the application of the laws, Regulations and administrative provisions of Member States relating to the certification and indication of the standard of fineness of articles of precious metal.

Article 4

Internal market

Member States shall neither restrict the freedom to provide services nor restrict the free movement of goods for reasons falling within the field approximated by this Directive.

CHAPTER 2

UNFAIR COMMERCIAL PRACTICES

Article 5

Prohibition of unfair commercial practices

1. Unfair commercial practices shall be prohibited.

2. A commercial practice shall be unfair if:

(a) it is contrary to the requirements of professional diligence, and

(b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.

3. Commercial practices which are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group. This is without prejudice to the common and legitimate advertising practice of making exaggerated statements or statements which are not meant to be taken literally.

4. In particular, commercial practices shall be unfair which:

(a) are misleading as set out in Articles 6 and 7,

or

(b) are aggressive as set out in Articles 8 and 9.

5. Annex I contains the list of those commercial practices which shall in all circumstances be regarded as unfair. The same single list shall apply in all Member States and may only be modified by revision of this Directive.

Section 1

Misleading commercial practices

Article 6

Misleading actions

1. A commercial practice shall be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise:

(a) the existence or nature of the product;

(b) the main characteristics of the product, such as its availability, benefits, risks, execution, composition, accessories, after-sale customer assistance and complaint handling, method and date of manufacture or provision, delivery, fitness for purpose, usage, quantity, specification, geographical or commercial origin or the results to be expected from its use, or the results and material features of tests or checks carried out on the product;

(c) the extent of the trader's commitments, the motives for the commercial practice and the nature of the sales process, any statement or symbol in relation to direct or indirect sponsorship or approval of the trader or the product;

(d) the price or the manner in which the price is calculated, or the existence of a specific price advantage;

(e) the need for a service, part, replacement or repair;

(f) the nature, attributes and rights of the trader or his agent, such as his identity and assets, his qualifications, status, approval, affiliation or connection and ownership of industrial, commercial or intellectual property rights or his awards and distinctions;

(g) the consumer's rights, including the right to replacement or reimbursement under Directive 1999/44/EC of the European

Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees [8], or the risks he may face.

2. A commercial practice shall also be regarded as misleading if, in its factual context, taking account of all its features and circumstances, it causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise, and it involves:

(a) any marketing of a product, including comparative advertising, which creates confusion with any products, trademarks, trade names or other distinguishing marks of a competitor;

(b) non-compliance by the trader with commitments contained in codes of conduct by which the trader has undertaken to be bound, where:

(i) the commitment is not aspirational but is firm and is capable of being verified, and

(ii) the trader indicates in a commercial practice that he is bound by the code.

Article 7

Misleading omissions

1. A commercial practice shall be regarded as misleading if, in its factual context, taking account of all its features and circumstances and the limitations of the communication medium, it omits material information that the average consumer needs, according to the context, to take an informed transactional decision and thereby causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.

2. It shall also be regarded as a misleading omission when, taking account of the matters described in paragraph 1, a trader hides or provides in an unclear, unintelligible, ambiguous or untimely manner such material information as referred to in that paragraph or fails to identify the commercial intent of the commercial practice if not already apparent from the context, and where, in either case, this causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.

3. Where the medium used to communicate the commercial practice imposes limitations of space or time, these limitations and any measures taken by the trader to make the information available to consumers by other means shall be taken into account in deciding whether information has been omitted.

4. In the case of an invitation to purchase, the following information shall be regarded as material, if not already apparent from the context:

(a) the main characteristics of the product, to an extent appropriate to the medium and the product;

(b) the geographical address and the identity of the trader, such as his trading name and, where applicable, the geographical address and the identity of the trader on whose behalf he is acting;

(c) the price inclusive of taxes, or where the nature of the product means that the price cannot reasonably be calculated in advance, the manner in which the price is calculated, as well as, where appropriate, all additional freight, delivery or postal charges or, where these charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable;

(d) the arrangements for payment, delivery, performance and the complaint handling policy, if they depart from the requirements of professional diligence;

(e) for products and transactions involving a right of withdrawal or cancellation, the existence of such a right.

5. Information requirements established by Community law in relation to commercial communication including advertising or marketing, a non-exhaustive list of which is contained in Annex II, shall be regarded as material.

Section 2

Aggressive commercial practices

Article 8

Aggressive commercial practices

A commercial practice shall be regarded as aggressive if, in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise.

Article 9

Use of harassment, coercion and undue influence

In determining whether a commercial practice uses harassment, coercion, including the use of physical force, or undue influence, account shall be taken of:

- (a) its timing, location, nature or persistence;
- (b) the use of threatening or abusive language or behaviour;
- (c) the exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision with regard to the product;
- (d) any onerous or disproportionate non-contractual barriers imposed by the trader where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader;
- (e) any threat to take any action that cannot legally be taken.

CHAPTER 3

CODES OF CONDUCT

Article 10

Codes of conduct

This Directive does not exclude the control, which Member States may encourage, of unfair commercial practices by code owners and recourse to such bodies by the persons or organisations referred to in Article 11 if proceedings before such bodies are in addition to the court or administrative proceedings referred to in that Article.

Recourse to such control bodies shall never be deemed the equivalent of foregoing a means of judicial or administrative recourse as provided for in Article 11.

CHAPTER 4

FINAL PROVISIONS

Article 11

Enforcement

1. Member States shall ensure that adequate and effective means exist to combat unfair commercial practices in order to enforce compliance with the provisions of this Directive in the interest of consumers.

Such means shall include legal provisions under which persons or organisations regarded under national law as having a legitimate interest in combating unfair commercial practices, including competitors, may:

- (a) take legal action against such unfair commercial practices; and/or
- (b) bring such unfair commercial practices before an administrative authority competent either to decide on complaints or to initiate appropriate legal proceedings.

It shall be for each Member State to decide which of these facilities shall be available and whether to enable the courts or administrative authorities to require prior recourse to other established means of dealing with complaints, including those referred to in Article 10. These facilities shall be available regardless of whether the consumers affected are in the territory of the Member State where the trader is located or in another Member State.

It shall be for each Member State to decide:

- (a) whether these legal facilities may be directed separately or jointly against a number of traders from the same economic sector; and
- (b) whether these legal facilities may be directed against a code owner where the relevant code promotes non-compliance with legal requirements.

2. Under the legal provisions referred to in paragraph 1, Member States shall confer upon the courts or administrative authorities powers enabling them, in cases where they deem

such measures to be necessary taking into account all the interests involved and in particular the public interest:

- (a) to order the cessation of, or to institute appropriate legal proceedings for an order for the cessation of, unfair commercial practices;

or

- (b) if the unfair commercial practice has not yet been carried out but is imminent, to order the prohibition of the practice, or to institute appropriate legal proceedings for an order for the prohibition of the practice, even without proof of actual loss or damage or of intention or negligence on the part of the trader.

Member States shall also make provision for the measures referred to in the first subparagraph to be taken under an accelerated procedure:

- either with interim effect,

or

- with definitive effect,

on the understanding that it is for each Member State to decide which of the two options to select.

Furthermore, Member States may confer upon the courts or administrative authorities powers enabling them, with a view to eliminating the continuing effects of unfair commercial practices the cessation of which has been ordered by a final decision:

- (a) to require publication of that decision in full or in part and in such form as they deem adequate;

- (b) to require in addition the publication of a corrective statement.

3. The administrative authorities referred to in paragraph 1 must:

- (a) be composed so as not to cast doubt on their impartiality;
- (b) have adequate powers, where they decide on complaints, to monitor and enforce the observance of their decisions effectively;
- (c) normally give reasons for their decisions.

Where the powers referred to in paragraph 2 are exercised exclusively by an administrative authority, reasons for its decisions shall always be given. Furthermore, in this case, provision must be made for procedures whereby improper or unreasonable exercise of its powers by the administrative authority or improper or unreasonable failure to exercise the said powers can be the subject of judicial review.

Article 12

Courts and administrative authorities: substantiation of claims
Member States shall confer upon the courts or administrative authorities powers enabling them in the civil or administrative proceedings provided for in Article 11:

- (a) to require the trader to furnish evidence as to the accuracy of factual claims in relation to a commercial practice if, taking into account the legitimate interest of the trader and any other party to the proceedings, such a requirement appears appropriate on the basis of the circumstances of the particular case;

and

- (b) to consider factual claims as inaccurate if the evidence demanded in accordance with (a) is not furnished or is deemed insufficient by the court or administrative authority.

Article 13

Penalties

Member States shall lay down penalties for infringements of national provisions adopted in application of this Directive and shall take all necessary measures to ensure that these are enforced. These penalties must be effective, proportionate and dissuasive.

Article 14

Amendments to Directive 84/450/EEC

Directive 84/450/EEC is hereby amended as follows:

1. Article 1 shall be replaced by the following:

"Article 1

The purpose of this Directive is to protect traders against misleading advertising and the unfair consequences thereof and to lay down the conditions under which comparative advertising is permitted."

;

2. in Article 2:

- point 3 shall be replaced by the following:

"3. "trader" means any natural or legal person who is acting for purposes relating to his trade, craft, business or profession and any one acting in the name of or on behalf of a trader."

,

- the following point shall be added:

"4. "code owner" means any entity, including a trader or group of traders, which is responsible for the formulation and revision of a code of conduct and/or for monitoring compliance with the code by those who have undertaken to be bound by it."

;

3. Article 3a shall be replaced by the following:

"Article 3a

1. Comparative advertising shall, as far as the comparison is concerned, be permitted when the following conditions are met:

(a) it is not misleading within the meaning of Articles 2(2), 3 and 7(1) of this Directive or Articles 6 and 7 of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market [];

(b) it compares goods or services meeting the same needs or intended for the same purpose;

(c) it objectively compares one or more material, relevant, verifiable and representative features of those goods and services, which may include price;

(d) it does not discredit or denigrate the trade marks, trade names, other distinguishing marks, goods, services, activities, or circumstances of a competitor;

(e) for products with designation of origin, it relates in each case to products with the same designation;

(f) it does not take unfair advantage of the reputation of a trade mark, trade name or other distinguishing marks of a competitor or of the designation of origin of competing products;

(g) it does not present goods or services as imitations or replicas of goods or services bearing a protected trade mark or trade name;

(h) it does not create confusion among traders, between the advertiser and a competitor or between the advertiser's trade marks, trade names, other distinguishing marks, goods or services and those of a competitor.

4. Article 4(1) shall be replaced by the following:

"1. Member States shall ensure that adequate and effective means exist to combat misleading advertising in order to enforce compliance with the provisions on comparative advertising in the interest of traders and competitors. Such means shall include legal provisions under which persons or organisations regarded under national law as having a legitimate interest in combating misleading advertising or regulating comparative advertising may:

(a) take legal action against such advertising;

or

(b) bring such advertising before an administrative authority competent either to decide on complaints or to initiate appropriate legal proceedings.

It shall be for each Member State to decide which of these facilities shall be available and whether to enable the courts or administrative authorities to require prior recourse to other established means of dealing with complaints, including those referred to in Article 5.

It shall be for each Member State to decide:

(a) whether these legal facilities may be directed separately or jointly against a number of traders from the same economic sector;

and

(b) whether these legal facilities may be directed against a code owner where the relevant code promotes non-compliance with legal requirements."

;

5. Article 7(1) shall be replaced by the following:

"1. This Directive shall not preclude Member States from retaining or adopting provisions with a view to ensuring more

extensive protection, with regard to misleading advertising, for traders and competitors."

Article 15

Amendments to Directives 97/7/EC and 2002/65/EC

1. Article 9 of Directive 97/7/EC shall be replaced by the following:

"Article 9

Inertia selling

Given the prohibition of inertia selling practices laid down in Directive 2005/29/EC of 11 May 2005 of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [], Member States shall take the measures necessary to exempt the consumer from the provision of any consideration in cases of unsolicited supply, the absence of a response not constituting consent.

2. Article 9 of Directive 2002/65/EC shall be replaced by the following:

"Article 9

Given the prohibition of inertia selling practices laid down in Directive 2005/29/EC of 11 May 2005 of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [] and without prejudice to the provisions of Member States' legislation on the tacit renewal of distance contracts, when such rules permit tacit renewal, Member States shall take measures to exempt the consumer from any obligation in the event of unsolicited supplies, the absence of a reply not constituting consent.

Article 16

Amendments to Directive 98/27/EC and Regulation (EC) No 2006/2004

1. In the Annex to Directive 98/27/EC, point 1 shall be replaced by the following:

"1. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (OJ L 149, 11.6.2005, p. 22)."

2. In the Annex to Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of the consumer protection law (the Regulation on consumer protection cooperation) [12] the following point shall be added:

"16. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (OJ L 149, 11.6.2005, p. 22)."

Article 17

Information

Member States shall take appropriate measures to inform consumers of the national law transposing this Directive and shall, where appropriate, encourage traders and code owners to inform consumers of their codes of conduct.

Article 18

Review

1. By 12 June 2011 the Commission shall submit to the European Parliament and the Council a comprehensive report on the application of this Directive, in particular of Articles 3(9) and 4 and Annex I, on the scope for further harmonisation and simplification of Community law relating to consumer protection, and, having regard to Article 3(5), on any measures that need to be taken at Community level to ensure that appropriate levels of consumer protection are maintained. The report shall be accompanied, if necessary, by a proposal to revise this Directive or other relevant parts of Community law.

2. The European Parliament and the Council shall endeavour to act, in accordance with the Treaty, within two years of the presentation by the Commission of any proposal submitted under paragraph 1.

Article 19

Transposition

Member States shall adopt and publish the laws, Regulations and administrative provisions necessary to comply with this

Directive by 12 June 2007. They shall forthwith inform the Commission thereof and inform the Commission of any subsequent amendments without delay.

They shall apply those measures by 12 December 2007. When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

Article 20

Entry into force

This Directive shall enter into force on the day following its publication in the Official Journal of the European Union.

Article 21

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 11 May 2005.

For the European Parliament

The President

J. P. Borrell Fontelles

For the Council

The President

N. Schmit

[1] OJ C 108, 30.4.2004, p. 81.

[2] Opinion of the European Parliament of 20 April 2004 (OJ C 104 E, 30.4.2004, p. 260), Council Common Position of 15 November 2004 (OJ C 38 E, 15.2.2005, p. 1), Position of the European Parliament of 24 February 2005 (not yet published in the Official Journal) and Council Decision of 12 April 2005.

[3] OJ L 250, 19.9.1984, p. 17. Directive as amended by Directive 97/55/EC of the European Parliament and of the Council (OJ L 290, 23.10.1997, p. 18).

[4] OJ L 144, 4.6.1997, p. 19. Directive as amended by Directive 2002/65/EC (OJ L 271, 9.10.2002, p. 16).

[5] OJ L 166, 11.6.1998, p. 51. Directive as last amended by Directive 2002/65/EC.

[6] OJ L 271, 9.10.2002, p. 16.

[7] OJ L 201, 31.7.2002, p. 37.

[8] OJ L 171, 7.7.1999, p. 12.

[] OJ L 149, 11.6.2005, p. 22.;

[] OJ L 149, 11.6.2005, p. 22.;

[] OJ L 149, 11.6.2005, p. 22."

[12] OJ L 364, 9.12.2004, p. 1.

20050511

ANNEX I

COMMERCIAL PRACTICES WHICH ARE IN ALL CIRCUMSTANCES CONSIDERED UNFAIR

Misleading commercial practices

1. Claiming to be a signatory to a code of conduct when the trader is not.

2. Displaying a trust mark, quality mark or equivalent without having obtained the necessary authorisation.

3. Claiming that a code of conduct has an endorsement from a public or other body which it does not have.

4. Claiming that a trader (including his commercial practices) or a product has been approved, endorsed or authorised by a public or private body when he/it has not or making such a claim without complying with the terms of the approval, endorsement or authorisation.

5. Making an invitation to purchase products at a specified price without disclosing the existence of any reasonable grounds the trader may have for believing that he will not be able to offer for supply or to procure another trader to supply, those products or equivalent products at that price for a period that is, and in quantities that are, reasonable having regard to the product, the scale of advertising of the product and the price offered (bait advertising).

6. Making an invitation to purchase products at a specified price and then:

(a) refusing to show the advertised item to consumers;

or

(b) refusing to take orders for it or deliver it within a reasonable time;

or

(c) demonstrating a defective sample of it, with the intention of promoting a different product (bait and switch)

7. Falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice.

8. Undertaking to provide after-sales service to consumers with whom the trader has communicated prior to a transaction in a language which is not an official language of the Member State where the trader is located and then making such service available only in another language without clearly disclosing this to the consumer before the consumer is committed to the transaction.

9. Stating or otherwise creating the impression that a product can legally be sold when it cannot.

10. Presenting rights given to consumers in law as a distinctive feature of the trader's offer.

11. Using editorial content in the media to promote a product where a trader has paid for the promotion without making that clear in the content or by images or sounds clearly identifiable by the consumer (advertorial). This is without prejudice to Council Directive 89/552/EEC [1].

12. Making a materially inaccurate claim concerning the nature and extent of the risk to the personal security of the consumer or his family if the consumer does not purchase the product.

13. Promoting a product similar to a product made by a particular manufacturer in such a manner as deliberately to mislead the consumer into believing that the product is made by that same manufacturer when it is not.

14. Establishing, operating or promoting a pyramid promotional scheme where a consumer gives consideration for the opportunity to receive compensation that is derived primarily from the introduction of other consumers into the scheme rather than from the sale or consumption of products.

15. Claiming that the trader is about to cease trading or move premises when he is not.

16. Claiming that products are able to facilitate winning in games of chance.

17. Falsely claiming that a product is able to cure illnesses, dysfunction or malformations.

18. Passing on materially inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favourable than normal market conditions.

19. Claiming in a commercial practice to offer a competition or prize promotion without awarding the prizes described or a reasonable equivalent.

20. Describing a product as "gratis", "free", "without charge" or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item.

21. Including in marketing material an invoice or similar document seeking payment which gives the consumer the impression that he has already ordered the marketed product when he has not.

22. Falsely claiming or creating the impression that the trader is not acting for purposes relating to his trade, business, craft or profession, or falsely representing oneself as a consumer.

23. Creating the false impression that after-sales service in relation to a product is available in a Member State other than the one in which the product is sold.

Aggressive commercial practices

24. Creating the impression that the consumer cannot leave the premises until a contract is formed.

25. Conducting personal visits to the consumer's home ignoring the consumer's request to leave or not to return except in circumstances and to the extent justified, under national law, to enforce a contractual obligation.

26. Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation. This is without prejudice to Article 10 of

Directive 97/7/EC and Directives 95/46/EC [2] and 2002/58/EC.

27. Requiring a consumer who wishes to claim on an insurance policy to produce documents which could not reasonably be considered relevant as to whether the claim was valid, or failing systematically to respond to pertinent correspondence, in order to dissuade a consumer from exercising his contractual rights.

28. Including in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them. This provision is without prejudice to Article 16 of Directive 89/552/EEC on television broadcasting.

29. Demanding immediate or deferred payment for or the return or safekeeping of products supplied by the trader, but not solicited by the consumer except where the product is a substitute supplied in conformity with Article 7(3) of Directive 97/7/EC (inertia selling).

30. Explicitly informing a consumer that if he does not buy the product or service, the trader's job or livelihood will be in jeopardy.

31. Creating the false impression that the consumer has already won, will win, or will on doing a particular act win, a prize or other equivalent benefit, when in fact either:

- there is no prize or other equivalent benefit,

or

- taking any action in relation to claiming the prize or other equivalent benefit is subject to the consumer paying money or incurring a cost.

[1] Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities (OJ L 298, 17.10.1989, p. 23). Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30.7.1997, p. 60).

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31). Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

20050511

ANNEX II

COMMUNITY LAW PROVISIONS SETTING OUT RULES FOR ADVERTISING AND COMMERCIAL COMMUNICATION

Articles 4 and 5 of Directive 97/7/EC

Article 3 of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours [1]

Article 3(3) of Directive 94/47/EC of the European Parliament and of the Council of 26 October 1994 on the protection of purchasers in respect of certain aspects of contracts relating to the purchase of a right to use immovable properties on a timeshare basis [2]

Article 3(4) of Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection

in the indication of the prices of products offered to consumers [3]

Articles 86 to 100 of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use [4]

Articles 5 and 6 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [5]

Article 1(d) of Directive 98/7/EC of the European Parliament and of the Council of 16 February 1998 amending Council Directive 87/102/EEC for the approximation of the laws, Regulations and administrative provisions of the Member States concerning consumer credit [6]

Articles 3 and 4 of Directive 2002/65/EC

Article 1(9) of Directive 2001/107/EC of the European Parliament and of the Council of 21 January 2002 amending Council Directive 85/611/EEC on the coordination of laws, Regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) with a view to regulating management companies and simplified prospectuses [7]

Articles 12 and 13 of Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation [8]

Article 36 of Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance [9]

Article 19 of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments [10]

Articles 31 and 43 of Council Directive 92/49/EEC of 18 June 1992 on the coordination of laws, Regulations and administrative provisions relating to direct insurance other than life assurance [11] (third non-life insurance Directive)

Articles 5, 7 and 8 of Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading [12]

[1] OJ L 158, 23.6.1990, p. 59.

[2] OJ L 280, 29.10.1994, p. 83.

[3] OJ L 80, 18.3.1998, p. 27.

[4] OJ L 311, 28.11.2001, p. 67. Directive as last amended by Directive 2004/27/EC (OJ L 136, 30.4.2004, p. 34).

[5] OJ L 178, 17.7.2000, p. 1.

[6] OJ L 101, 1.4.1998, p. 17.

[7] OJ L 41, 13.2.2002, p. 20.

[8] OJ L 9, 15.1.2003, p. 3.

[9] OJ L 345, 19.12.2002, p. 1. Directive as amended by Council Directive 2004/66/EC. (OJ L 168, 1.5.2004, p. 35).

[10] OJ L 145, 30.4.2004, p. 1.

[11] OJ L 228, 11.8.1992, p. 1. Directive as last amended by Directive 2002/87/EC of the European Parliament and of the Council (OJ L 35, 11.2.2003, p. 1).

[12] OJ L 345, 31.12.2003, p. 64.

Relevant Case Law on Unfair Commercial Practices Directive

C-122/10, Konsumentombudsmannen v Ving Sverige AB,
(Reference for a preliminary ruling – Directive 2005/29/EC – Articles 2(i) and 7(4) – Commercial communication published in a newspaper – Meaning of invitation to purchase – Entry-level price – Information which an invitation to purchase has to contain).

Ruling:

1. The words 'thereby enables the consumer to make a purchase' in Article 2(i) of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices

in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') must be interpreted as meaning that an invitation to purchase exists as soon as the information on the product advertised and its price is sufficient for the consumer to be able to make a transactional decision, without it being necessary for the commercial communication also to offer an actual opportunity to purchase the product or for it to appear in proximity to and at the same time as such an opportunity.

2. Article 2(i) of Directive 2005/29 must be interpreted as meaning that the requirement relating to the indication of the price of the product may be met if the commercial communication contains an entry-level price, that is to say the lowest price for which the advertised product or category of products can be bought, while the advertised product or category of products are available in other versions or with other content at prices which are not indicated. It is for the national court to ascertain, on the basis of the nature and characteristics of the product and the commercial medium of communication used, whether the reference to an entry-level price enables the consumer to take a transactional decision.

3. Article 2(i) of Directive 2005/29 must be interpreted as meaning that a verbal or visual reference to the product makes it possible to meet the requirement relating to the indication of the product's characteristics, and that includes a situation where such a verbal or visual reference is used to designate a product which is offered in many versions. It is for the national court to ascertain, on a case-by-case basis, taking into account the nature and characteristics of the product and the medium of communication used, whether the consumer has sufficient information to identify and distinguish the product for the purpose of taking a transactional decision.

4. Article 7(4)(a) of Directive 2005/29 must be interpreted as meaning that it may be sufficient for only certain of a product's main characteristics to be given and for the trader to refer in addition to its website, on the condition that on that site there is essential information on the product's main characteristics, price and other terms in accordance with the requirements in Article 7 of that Directive. It is for the national court to assess, on a case-by-case basis, taking into consideration the context of

the invitation to purchase, the medium of communication used and the nature and characteristics of the product, whether a reference only to certain main characteristics of the product enables the consumer to take an informed transactional decision.

5. Article 7(4)(c) of Directive 2005/29 must be interpreted as meaning that a reference only to an entry-level price in an invitation to purchase cannot be regarded, in itself, as constituting a misleading omission. It is for the national court to ascertain whether a reference to an entry-level price is sufficient for the requirements concerning the reference to a price, such as those set out in that provision, to be considered to be met. That court will have to ascertain, *inter alia*, whether the omission of the detailed rules for calculating the final price prevents the consumer from taking an informed transactional decision and, consequently, leads him to take a transactional decision which he would not otherwise have taken. It is also for the national court to take into consideration the limitations forming an integral part of the medium of communication used; the nature and the characteristics of the product and the other measures that the trader has actually taken to make the information available to consumers.

C-657/11, *Belgian Electronic Sorting Technology NV v Bert Peelaers, Visys NV*,

(Directives 84/450/EEC and 2006/114/EC – Misleading and comparative advertising – Definition of 'advertising' – Registration and use of a domain name – Use of metatags in a website's metadata)

Ruling:

Article 2(1) of Council Directive 84/450/EEC of 10 September 1984 concerning misleading and comparative advertising, as amended by Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 and Article 2(a) of Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising, must be interpreted as meaning that the term 'advertising', as defined by those provisions, covers, in a situation such as that at issue in the main proceedings, the use of a domain name and that of metatags in a website's metadata. By contrast, the registration of a domain name, as such, is not encompassed by that term.

II. Competition Law

Treaty on the Functioning of the European Union (101 – 109)

CHAPTER 1: RULES ON COMPETITION SECTION 1: RULES APPLYING TO UNDERTAKINGS

Article 101 (ex Article 81 TEC)

1. The following shall be prohibited as incompatible with the internal market: all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which:

- (a) directly or indirectly fix purchase or selling prices or any other trading conditions;
- (b) limit or control production, markets, technical development, or investment;
- (c) share markets or sources of supply;
- (d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
- (e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

2. Any agreements or decisions prohibited pursuant to this Article shall be automatically void.

3. The provisions of paragraph 1 may, however, be declared inapplicable in the case of:

- any agreement or category of agreements between undertakings,
- any decision or category of decisions by associations of undertakings,
- any concerted practice or category of concerted practices, which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not:

- (a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;
- (b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question.

Article 102 (ex Article 82 TEC)

Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.

Such abuse may, in particular, consist in:

- (a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;
- (b) limiting production, markets or technical development to the prejudice of consumers;
- (c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
- (d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their

nature or according to commercial usage, have no connection with the subject of such contracts.

Article 103 (ex Article 83 TEC)

1. The appropriate Regulations or Directives to give effect to the principles set out in Articles 101 and 102 shall be laid down by the Council, on a proposal from the Commission and after consulting the European Parliament.

2. The Regulations or Directives referred to in paragraph 1 shall be designed in particular:

- (a) to ensure compliance with the prohibitions laid down in Article 101(1) and in Article 102 by making provision for fines and periodic penalty payments;
- (b) to lay down detailed rules for the application of Article 101(3), taking into account the need to ensure effective supervision on the one hand, and to simplify administration to the greatest possible extent on the other;
- (c) to define, if need be, in the various branches of the economy, the scope of the provisions of Articles 101 and 102;
- (d) to define the respective functions of the Commission and of the Court of Justice of the European Union in applying the provisions laid down in this paragraph;
- (e) to determine the relationship between national laws and the provisions contained in this Section or adopted pursuant to this Article.

Article 104 (ex Article 84 TEC)

Until the entry into force of the provisions adopted in pursuance of Article 103, the authorities in Member States shall rule on the admissibility of agreements, decisions and concerted practices and on abuse of a dominant position in the internal market in accordance with the law of their country and with the provisions of Article 101, in particular paragraph 3, and of Article 102.

Article 105 (ex Article 85 TEC)

1. Without prejudice to Article 104, the Commission shall ensure the application of the principles laid down in Articles 101 and 102. On application by a Member State or on its own initiative, and in cooperation with the competent authorities in the Member States, which shall give it their assistance, the Commission shall investigate cases of suspected infringement of these principles. If it finds that there has been an infringement, it shall propose appropriate measures to bring it to an end.

2. If the infringement is not brought to an end, the Commission shall record such infringement of the principles in a reasoned decision. The Commission may publish its decision and authorise Member States to take the measures, the conditions and details of which it shall determine, needed to remedy the situation.

3. The Commission may adopt Regulations relating to the categories of agreement in respect of which the Council has adopted a Regulation or a Directive pursuant to Article 103(2)(b).

Article 106
(ex Article 86 TEC)

1. In the case of public undertakings and undertakings to which Member States grant special or exclusive rights, Member States shall neither enact nor maintain in force any measure contrary to the rules contained in the Treaties, in particular to those rules provided for in Article 18 and Articles 101 to 109.
2. Undertakings entrusted with the operation of services of general economic interest or having the character of a revenue-producing monopoly shall be subject to the rules contained in the Treaties, in particular to the rules on competition, in so far as the application of such rules does not obstruct the performance, in law or in fact, of the particular tasks assigned to them. The development of trade must not be affected to such an extent as would be contrary to the interests of the Union.
3. The Commission shall ensure the application of the provisions of this Article and shall, where necessary, address appropriate Directives or decisions to Member States.

SECTION 2: AIDS GRANTED BY STATES

Article 107
(ex Article 87 TEC)

1. Save as otherwise provided in the Treaties, any aid granted by a Member State or through State resources in any form whatsoever which distorts or threatens to distort competition by favouring certain undertakings or the production of certain goods shall, in so far as it affects trade between Member States, be incompatible with the internal market.
2. The following shall be compatible with the internal market:
 - (a) aid having a social character, granted to individual consumers, provided that such aid is granted without discrimination related to the origin of the products concerned;
 - (b) aid to make good the damage caused by natural disasters or exceptional occurrences;
 - (c) aid granted to the economy of certain areas of the Federal Republic of Germany affected by the division of Germany, in so far as such aid is required in order to compensate for the economic disadvantages caused by that division. Five years after the entry into force of the Treaty of Lisbon, the Council, acting on a proposal from the Commission, may adopt a decision repealing this point.
3. The following may be considered to be compatible with the internal market:
 - (a) aid to promote the economic development of areas where the standard of living is abnormally low or where there is serious underemployment, and of the regions referred to in Article 349, in view of their structural, economic and social situation;
 - (b) aid to promote the execution of an important project of common European interest or to remedy a serious disturbance in the economy of a Member State;
 - (c) aid to facilitate the development of certain economic activities or of certain economic areas, where such aid does not adversely affect trading conditions to an extent contrary to the common interest;
 - (d) aid to promote culture and heritage conservation where such aid does not affect trading conditions and competition in the Union to an extent that is contrary to the common interest;

(e) such other categories of aid as may be specified by decision of the Council on a proposal from the Commission.

Article 108
(ex Article 88 TEC)

1. The Commission shall, in cooperation with Member States, keep under constant review all systems of aid existing in those States. It shall propose to the latter any appropriate measures required by the progressive development or by the functioning of the internal market.
2. If, after giving notice to the parties concerned to submit their comments, the Commission finds that aid granted by a State or through State resources is not compatible with the internal market having regard to Article 107, or that such aid is being misused, it shall decide that the State concerned shall abolish or alter such aid within a period of time to be determined by the Commission.
If the State concerned does not comply with this decision within the prescribed time, the Commission or any other interested State may, in derogation from the provisions of Articles 258 and 259, refer the matter to the Court of Justice of the European Union direct.
On application by a Member State, the Council may, acting unanimously, decide that aid which that State is granting or intends to grant shall be considered to be compatible with the internal market, in derogation from the provisions of Article 107 or from the Regulations provided for in Article 109, if such a decision is justified by exceptional circumstances. If, as regards the aid in question, the Commission has already initiated the procedure provided for in the first subparagraph of this paragraph, the fact that the State concerned has made its application to the Council shall have the effect of suspending that procedure until the Council has made its attitude known.
If, however, the Council has not made its attitude known within three months of the said application being made, the Commission shall give its decision on the case.
3. The Commission shall be informed, in sufficient time to enable it to submit its comments, of any plans to grant or alter aid. If it considers that any such plan is not compatible with the internal market having regard to Article 107, it shall without delay initiate the procedure provided for in paragraph 2. The Member State concerned shall not put its proposed measures into effect until this procedure has resulted in a final decision.
4. The Commission may adopt Regulations relating to the categories of State aid that the Council has, pursuant to Article 109, determined may be exempted from the procedure provided for by paragraph 3 of this Article.

Article 109
(ex Article 89 TEC)

The Council, on a proposal from the Commission and after consulting the European Parliament, may make any appropriate Regulations for the application of Articles 107 and 108 and may in particular determine the conditions in which Article 108(3) shall apply and the categories of aid exempted from this procedure.

Relevant case-law to the Treaty on the Functioning of the EU Art 101-102

C-418/01 IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG

1. Where the national courts give a ruling on agreements or practices which may subsequently be the subject of a decision

by the Commission, they must avoid taking decisions which conflict with those taken or envisaged by the Commission in the implementation of Articles 81 and 82 EC.

(see para. 19)

2. In the assessment of the abusive character of a dominant position, in order to determine whether a product or service is indispensable for enabling an undertaking to carry on business in a particular market, it must be determined whether there are products or services which constitute alternative solutions, even if they are less advantageous, and whether there are technical, legal or economic obstacles capable of making it impossible or at least unreasonably difficult for any undertaking seeking to operate in the market to create, possibly in cooperation with other operators, alternative products or services. In order to accept the existence of economic obstacles, it must be established, at the very least, that the creation of those products or services is not economically viable for production on a scale comparable to that of the undertaking which controls the existing product or service.

It follows that, for the purposes of examining whether the refusal by an undertaking in a dominant position to grant a licence for a brick structure protected by an intellectual property right which it owns is abusive, the degree of participation by users in the development of that structure and the outlay, particularly in terms of cost, on the part of potential users in order to purchase studies on regional sales of pharmaceutical products presented on the basis of an alternative structure are factors which must be taken into consideration in order to determine whether the protected structure is indispensable to the marketing of studies of that kind.

(see paras 28, 30, operative part 1)

3. The refusal by an undertaking which holds a dominant position and owns an intellectual property right in a brick structure indispensable to the presentation of regional sales data on pharmaceutical products in a Member State to grant a licence to use that structure to another undertaking, which also wishes to provide such data in the same Member State, constitutes an abuse of a dominant position within the meaning of Article 82 EC where the following conditions are fulfilled:

- the undertaking which requested the licence intends to offer, on the market for the supply of the data in question, new products or services not offered by the owner of the intellectual property right and for which there is a potential consumer demand;

- the refusal is not justified by objective considerations;

- the refusal is such as to reserve to the owner of the intellectual property right the market for the supply of data on sales of pharmaceutical products in the Member State concerned by eliminating all competition on that market.

(see para. 52, operative part 2).

T-201/04 Microsoft Corp. v Commission of the European Communities

1. Where the national courts give a ruling on agreements or practices which may subsequently be the subject of a decision by the Commission, they must avoid taking decisions which conflict with those taken or envisaged by the Commission in the implementation of Articles 81 and 82 EC.

(see para. 19)

2. In the assessment of the abusive character of a dominant position, in order to determine whether a product or service is indispensable for enabling an undertaking to carry on business in a particular market, it must be determined whether there are products or services which constitute alternative solutions, even if they are less advantageous, and whether there are technical, legal or economic obstacles capable of making it impossible or at least unreasonably difficult for any

undertaking seeking to operate in the market to create, possibly in cooperation with other operators, alternative products or services. In order to accept the existence of economic obstacles, it must be established, at the very least, that the creation of those products or services is not economically viable for production on a scale comparable to that of the undertaking which controls the existing product or service.

It follows that, for the purposes of examining whether the refusal by an undertaking in a dominant position to grant a licence for a brick structure protected by an intellectual property right which it owns is abusive, the degree of participation by users in the development of that structure and the outlay, particularly in terms of cost, on the part of potential users in order to purchase studies on regional sales of pharmaceutical products presented on the basis of an alternative structure are factors which must be taken into consideration in order to determine whether the protected structure is indispensable to the marketing of studies of that kind.

(see paras 28, 30, operative part 1)

3. The refusal by an undertaking which holds a dominant position and owns an intellectual property right in a brick structure indispensable to the presentation of regional sales data on pharmaceutical products in a Member State to grant a licence to use that structure to another undertaking, which also wishes to provide such data in the same Member State, constitutes an abuse of a dominant position within the meaning of Article 82 EC where the following conditions are fulfilled:

- the undertaking which requested the licence intends to offer, on the market for the supply of the data in question, new products or services not offered by the owner of the intellectual property right and for which there is a potential consumer demand;

- the refusal is not justified by objective considerations;

- the refusal is such as to reserve to the owner of the intellectual property right the market for the supply of data on sales of pharmaceutical products in the Member State concerned by eliminating all competition on that market.

(see para. 52, operative part 2).

C-52/07- Kanal 5 Ltd and TV 4 AB v Föreningen Svenska Tonsättares Internationella Musikbyrå (STIM) upa

Summary of the Judgment

1. Competition – Dominant position – Copyright management organisation having a de facto monopoly – Collection of royalties corresponding to part of the revenue of commercial television channels which is proportionate overall to the quantity of musical works broadcast in the absence of other methods enabling the use of those works and the audience to be measured more precisely

(Art. 82 EC)

2. Competition – Dominant position – Copyright management organisation having a de facto monopoly – Collection of royalties calculated in a different manner according to whether the companies are commercial companies or public service undertakings

(Art. 82 EC)

1. Article 82 EC must be interpreted as meaning that a copyright management organisation with a dominant position on a substantial part of the common market does not abuse that position where, with respect to remuneration paid for the

television broadcast of musical works protected by copyright, it applies to commercial television channels a remuneration model according to which the amount of the royalties corresponds partly to the revenue of those channels, provided that that part is proportionate overall to the quantity of musical works protected by copyright actually broadcast or likely to be broadcast, unless another method enables the use of those works and the audience to be identified more precisely without however resulting in a disproportionate increase in the costs incurred for the management of contracts and the supervision of the use of those works.

(see para. 41, operative part 1)

2. Article 82 EC must be interpreted as meaning that, by calculating the royalties with respect to remuneration paid for the broadcast of musical works protected by copyright in a different manner according to whether the companies concerned are commercial companies or public service undertakings, a copyright management organisation is likely to exploit in an abusive manner its dominant position within the meaning of that article if it applies with respect to those companies dissimilar conditions to equivalent services and if it places them as a result at a competitive disadvantage, unless such a practice may be objectively justified.

As regards the examination as to whether such a practice exists account must be taken, where appropriate, of the fact that, unlike commercial television companies, public service undertakings do not have either advertising revenue or revenue relating to subscription contracts and of the fact that the royalties paid by public service undertakings are collected without taking account of the quantity of musical works protected by copyright actually broadcast. Furthermore, it must also be ascertained whether commercial television companies are competitors of public service undertakings on the same market.

As regards the examination of any objective justification, such justification may arise, in particular, from the task and method of financing of public service undertakings.

(see paras 44-48, operative part 2)

C-425/07 P AEPI Elliniki Etaireia pros Prostatian tis Pnevmatikis Idioktiasias AE v Commission of the European Communities

1 Summary of the Judgment

1. Competition – Administrative procedure – Examination of complaints – Assessment of the Community interest in investigating a case

(Arts 81 EC and 82 EC)

2. Competition – Agreements, decisions and concerted practices – Effect on trade between Member States – Meaning

(Arts 81 EC and 82 EC)

3. Appeals – Grounds – Grounds of a judgment vitiated by a confusion between two legal concepts – Operative part well founded on other legal grounds – Rejection

1. The Commission is responsible for defining and implementing Community competition policy and for that purpose has a discretion as to how it deals with complaints lodged with it. When the Commission determines the order of priority for dealing with the complaints brought before it, it may legitimately refer to the Community interest. In this context, it is required to assess in each case how serious the alleged interferences with competition are and how persistent their consequences are. That obligation means in particular

that it must take into account the duration and extent of the infringements complained of and their effect on the competition situation in the European Community.

Consequently, in a situation where intra-Community trade is found to be affected, a complaint relating to infringement of Articles 81 EC and 82 EC will be investigated by the Commission rather than by the national competition authorities if there is sufficient Community interest. That may inter alia apply where the infringement complained of is capable of giving rise to serious impediments to the proper functioning of the common market.

(see paras 31, 53-54)

2. The concepts of, first, an effect on intra-Community trade and, secondly, of serious impediments to the proper functioning of the common market are two separate concepts.

The effect on trade between Member States serves as a criterion to define the scope of Community competition law, in particular Articles 81 EC and 82 EC, as against that of national competition law. If it is established that the alleged infringement is not capable of affecting intra-Community trade or of affecting it only in an insignificant manner, then Community competition law, and more specifically Articles 81 EC and 82 EC, do not apply. Furthermore, if an agreement between undertakings is to be capable of affecting trade between Member States, it must be possible to foresee with a sufficient degree of probability, on the basis of a set of objective factors of law or of fact, that it has an influence, direct or indirect, actual or potential, on the pattern of trade between Member States in a manner which might harm the attainment of the objectives of a single market between Member States.

As for the concept of serious impediments to the proper functioning of the common market, it may constitute one of the criteria for evaluating whether there is sufficient Community interest to necessitate the investigation of a complaint by the Commission.

An effect on intra-Community trade does not in itself give rise to serious impediments to the proper functioning of the common market.

(see paras 48-52)

3. A confusion of concepts by the Court of First Instance in a judgment under appeal is not capable of giving rise to the annulment of that judgment if the operative part of the judgment is shown to be well founded for other legal reasons.

COMP/39.530 Summary of Commission Decision - Microsoft - Webbrowser

Summary of Commission Decision

of 6 March 2013 relating to a proceeding on the imposition of a fine pursuant to Article 23(2)(c) of Council Regulation (EC) No 1/2003 for failure to comply with a commitment made binding by a Commission decision pursuant to Article 9 of Council Regulation (EC) No 1/2003

(Case COMP/39.530 — Microsoft (Tying))
(notified under document C(2013) 1210 final)
(Only English text is authentic)
2013/C 120/06

On 6 March 2013, the Commission adopted a decision relating to a proceeding on the imposition of a fine pursuant to Article 23(2)(c) of Council Regulation (EC) No 1/2003 (1) for failure to comply with a commitment made binding by a Commission decision pursuant to Article 9 of Council Regulation (EC) No 1/2003. In accordance with the provisions of Article 30 of Council Regulation (EC) No 1/2003, the Commission herewith publishes the name of the party and the main content of the

decision, including the penalties imposed, having regard to the legitimate interest of undertaking in the protection of its business secrets.

Background of the case

(1) On 16 December 2009, the Commission adopted a decision relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement pursuant to Article 9(1) of Regulation (EC) No 1/2003, which made binding the commitments offered by Microsoft Corporation ('Microsoft') to meet the Commission's concerns, as set out in a statement of objections of 14 January 2009 ('the commitments') (2).

(2) The Commission's preliminary concerns related to the tying of Microsoft's web browser, Internet Explorer ('IE'), to its dominant client PC operating system, Windows.

(3) In order to address the Commission's preliminary concerns, Microsoft committed in particular to offer Windows users an unbiased choice among different web browsers by means of a choice screen in Windows XP, Windows Vista, Windows 7 and in Windows client PC operating systems sold after Windows 7. Microsoft committed to display the choice screen to Windows users within the European Economic Area ('EEA') that have IE set as the default web browser.

Procedure

(4) On 17 June 2012, the Commission was informed of a possible failure to comply with the commitments by Microsoft. On 4 July 2012, Microsoft acknowledged a failure to display the choice screen to users of Windows 7 Service Pack 1 ('Windows 7 SP 1').

(5) On 16 July 2012, the Commission decided to reopen and initiate proceedings. On 24 October 2012, the Commission adopted a statement of objections. On 6 November 2012, Microsoft was granted access to the Commission's file. On 2 December 2012, Microsoft replied to the statement of objections.

(6) On 4 March 2013, the Advisory Committee on restrictive practices and dominant positions issued a favourable opinion. On 5 March 2013, the Hearing Officer issued a final report.

Legal assessment and fines

(7) The infringement consists of Microsoft's failure to comply with Section 2 of the commitments by not displaying the choice screen to users within the EEA that have IE set as the default web browser.

(8) In light of Microsoft's arguments, the Commission concluded that Microsoft's failure to comply lasted for 14 months from 17 May 2011 until 16 July 2012. The Commission also considered that the number of users affected by

Microsoft's failure to comply with Section 2 of the commitments is approximately 15,3 million.

Negligence

(9) A series of technical errors and omissions led to Microsoft's failure to provide the choice screen to the affected users. Given its resources and know-how, however, Microsoft should have been able to avoid such errors and should have had better processes in place to ensure that the choice screen was correctly displayed to the affected users.

(10) The Commission concluded that Microsoft acted negligently.

Gravity

(11) The Commission underlines that regardless of the specific circumstances of the case, a failure to comply with a commitment decision is, in principle, a serious breach of Union law (3).

(12) In the case at hand, Microsoft's failure to comply with Section 2 of the commitments goes to the core of the Commission's competition concerns and of Microsoft's obligations as set out in the commitments. The number of affected users, approximately 15,3 million, was significant.

(13) The Commission therefore regards the infringement committed by Microsoft as a serious one.

Duration

(14) The duration of Microsoft's failure to comply with Section 2 of the commitments was 14 months. When setting the amount of the fine, the Commission took into account that 14 months is a significant part of the overall duration of Section 2 of the commitments (4 years and 39 weeks).

Mitigating factors

(15) The Decision concluded that the fact that Microsoft helped the Commission to more efficiently investigate the case by providing evidence of the failure to comply is a mitigating factor. Microsoft has deployed resources to conduct a thorough investigation as to the reasons for the failure to comply.

Deterrent effect

(16) In order to ensure that the fine has a deterrent effect, the Commission took into account Microsoft's size and resources. The Commission therefore took into account the fact that Microsoft's turnover in the fiscal year July 2011 to June 2012, Microsoft's last full business year, was USD 73,723 million (EUR 55,088 million).

The fine

(17) In the light of all the factors set out above, the Commission set the level of the fine at EUR 561 000 000, corresponding to 1,02 % of Microsoft's turnover in the fiscal year July 2011 to June 2012.

III. Law of domain names

Uniform Domain Name Dispute Resolution Policy

(As Approved by ICANN on October 24, 1999)

1. Purpose. This Uniform Domain Name Dispute Resolution Policy (the "Policy") has been adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN"), is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us (the registrar) over the registration and use of an Internet domain name registered by you. Proceedings under Paragraph 4 of this Policy will be conducted according to the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules of Procedure"), which are available at www.icann.org/udrp/udrp-rules-24oct99.htm, and the selected administrative-dispute-resolution service provider's supplemental rules.

2. Your Representations. By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or Regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else's rights.

3. Cancellations, Transfers, and Changes. We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances:

- a. subject to the provisions of Paragraph 8, our receipt of written or appropriate electronic instructions from you or your authorized agent to take such action;
- b. our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or
- c. our receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN. (See Paragraph 4(i) and (k) below.)

We may also cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of your Registration Agreement or other legal requirements.

4. Mandatory Administrative Proceeding.

This Paragraph sets forth the type of disputes for which you are required to submit to a mandatory administrative proceeding. These proceedings will be conducted before one of the administrative-dispute-resolution service providers listed at www.icann.org/udrp/approved-providers.htm (each, a "Provider").

a. Applicable Disputes. You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that

(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) you have no rights or legitimate interests in respect of the domain name; and

(iii) your domain name has been registered and is being used in bad faith.

In the administrative proceeding, the complainant must prove that each of these three elements are present.

b. Evidence of Registration and Use in Bad Faith. For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

c. How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name in Responding to a Complaint. When you receive a complaint, you should refer to Paragraph 5 of the Rules of Procedure in determining how your response should be prepared. Any of the following circumstances, in particular but without limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name

corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or

(iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

d. Selection of Provider. The complainant shall select the Provider from among those approved by ICANN by submitting the complaint to that Provider. The selected Provider will administer the proceeding, except in cases of consolidation as described in Paragraph 4(f).

e. Initiation of Proceeding and Process and Appointment of Administrative Panel. The Rules of Procedure state the process for initiating and conducting a proceeding and for appointing the panel that will decide the dispute (the "Administrative Panel").

f. Consolidation. In the event of multiple disputes between you and a complainant, either you or the complainant may petition to consolidate the disputes before a single Administrative Panel. This petition shall be made to the first Administrative Panel appointed to hear a pending dispute between the parties. This Administrative Panel may consolidate before it any or all such disputes in its sole discretion, provided that the disputes being consolidated are governed by this Policy or a later version of this Policy adopted by ICANN.

g. Fees. All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to this Policy shall be paid by the complainant, except in cases where you elect to expand the Administrative Panel from one to three panelists as provided in Paragraph 5(b)(iv) of the Rules of Procedure, in which case all fees will be split evenly by you and the complainant.

h. Our Involvement in Administrative Proceedings. We do not, and will not, participate in the administration or conduct of any proceeding before an Administrative Panel. In addition, we will not be liable as a result of any decisions rendered by the Administrative Panel.

i. Remedies. The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.

j. Notification and Publication. The Provider shall notify us of any decision made by an Administrative Panel with respect to a domain name you have registered with us. All decisions under this Policy will be published in full over the Internet, except when an Administrative Panel determines in an exceptional case to redact portions of its decision.

k. Availability of Court Proceedings. The mandatory administrative proceeding requirements set forth in Paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded. If an Administrative Panel decides that your domain name registration should be canceled or transferred, we will wait ten (10) business days (as observed in the location of our principal office) after we are informed by the applicable Provider of the Administrative Panel's decision before implementing that decision. We will then implement the decision unless we have received from you during that ten (10)

business day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that you have commenced a lawsuit against the complainant in a jurisdiction to which the complainant has submitted under Paragraph 3(b)(xiii) of the Rules of Procedure. (In general, that jurisdiction is either the location of our principal office or of your address as shown in our Whois database. See Paragraphs 1 and 3(b)(xiii) of the Rules of Procedure for details.) If we receive such documentation within the ten (10) business day period, we will not implement the Administrative Panel's decision, and we will take no further action, until we receive (i) evidence satisfactory to us of a resolution between the parties; (ii) evidence satisfactory to us that your lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing your lawsuit or ordering that you do not have the right to continue to use your domain name.

5. All Other Disputes and Litigation. All other disputes between you and any party other than us regarding your domain name registration that are not brought pursuant to the mandatory administrative proceeding provisions of Paragraph 4 shall be resolved between you and such other party through any court, arbitration or other proceeding that may be available.

6. Our Involvement in Disputes. We will not participate in any way in any dispute between you and any party other than us regarding the registration and use of your domain name. You shall not name us as a party or otherwise include us in any such proceeding. In the event that we are named as a party in any such proceeding, we reserve the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend ourselves.

7. Maintaining the Status Quo. We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided in Paragraph 3 above.

8. Transfers During a Dispute.

a. Transfers of a Domain Name to a New Holder. You may not transfer your domain name registration to another holder (i) during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded; or (ii) during a pending court proceeding or arbitration commenced regarding your domain name unless the party to whom the domain name registration is being transferred agrees, in writing, to be bound by the decision of the court or arbitrator. We reserve the right to cancel any transfer of a domain name registration to another holder that is made in violation of this subparagraph.

b. Changing Registrars. You may not transfer your domain name registration to another registrar during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded. You may transfer administration of your domain name registration to another registrar during a pending court action or arbitration, provided that the domain name you have registered with us shall continue to be subject to the proceedings commenced against you in accordance with the terms of this Policy. In the event that you transfer a domain name registration to us during the pendency of a court action or arbitration, such dispute shall remain subject to the domain name dispute policy of the registrar from which the domain name registration was transferred.

9. Policy Modifications. We reserve the right to modify this Policy at any time with the permission of ICANN. We will post our revised Policy at least thirty (30) calendar days before it becomes effective. Unless this Policy has already been invoked by the submission of a complaint to a Provider, in which event

the version of the Policy in effect at the time it was invoked will apply to you until the dispute is over, all such changes will be binding upon you with respect to any domain name registration dispute, whether the dispute arose before, on or after the effective date of our change. In the event that you object to a

change in this Policy, your sole remedy is to cancel your domain name registration with us, provided that you will not be entitled to a refund of any fees you paid to us. The revised Policy will apply to you until you cancel your domain name registration.

Rules for Uniform Domain Name Dispute Resolution Policy

As approved by the ICANN Board of Directors on 30 October 2009.

These Rules are in effect for all UDRP proceedings in which a complaint is submitted to a provider on or after 1 March 2010. The prior version of the Rules, applicable to all proceedings in which a complaint was submitted to a Provider on or before 28 February 2010, is at <http://www.icann.org/en/dndr/udrp/uniform-rules-24oct99-en.htm>. UDRP Providers may elect to adopt the notice procedures set forth in these Rules prior to 1 March 2010.

Administrative proceedings for the resolution of disputes under the Uniform Dispute Resolution Policy adopted by ICANN shall be governed by these Rules and also the Supplemental Rules of the Provider administering the proceedings, as posted on its web site. To the extent that the Supplemental Rules of any Provider conflict with these Rules, these Rules supersede.

Definitions

In these Rules:

Complainant means the party initiating a complaint concerning a domain-name registration.

ICANN refers to the Internet Corporation for Assigned Names and Numbers.

Mutual Jurisdiction means a court jurisdiction at the location of either (a) the principal office of the Registrar (provided the domain-name holder has submitted in its Registration Agreement to that jurisdiction for court adjudication of disputes concerning or arising from the use of the domain name) or (b) the domain-name holder's address as shown for the registration of the domain name in Registrar's Whois database at the time the complaint is submitted to the Provider.

Panel means an administrative panel appointed by a Provider to decide a complaint concerning a domain-name registration.

Panelist means an individual appointed by a Provider to be a member of a Panel.

Party means a Complainant or a Respondent.

Policy means the Uniform Domain Name Dispute Resolution Policy that is incorporated by reference and made a part of the Registration Agreement.

Provider means a dispute-resolution service provider approved by ICANN. A list of such Providers appears at <http://www.icann.org/en/dndr/udrp/approved-providers.htm>.

Registrar means the entity with which the Respondent has registered a domain name that is the subject of a complaint.

Registration Agreement means the agreement between a Registrar and a domain-name holder.

Respondent means the holder of a domain-name registration against which a complaint is initiated.

Reverse Domain Name Hijacking means using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name.

Supplemental Rules means the rules adopted by the Provider administering a proceeding to supplement these Rules. Supplemental Rules shall not be inconsistent with the Policy or these Rules and shall cover such topics as fees, word and page limits and guidelines, file size and format modalities, the means for communicating with the Provider and the Panel, and the form of cover sheets.

Written Notice means hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent by the means specified herein. Written notice does not include a hardcopy of the complaint itself or of any annexes.

Communications

(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and

(ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative, and billing contacts;

(B) `postmaster@<the contested domain name>`; and

(C) if the domain name (or "www." followed by the domain name) resolves to an active web page (other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain-names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and

(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers

and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant under Paragraph 3(b)(v).

(b) Except as provided in Paragraph 2(a), any written communication to Complainant or Respondent provided for under these Rules shall be made electronically via the Internet (a record of its transmission being available), or by any reasonably requested preferred means stated by the Complainant or Respondent, respectively (see Paragraphs 3(b)(iii) and 5(b)(iii)).

(c) Any communication to the Provider or the Panel shall be made by the means and in the manner (including, where applicable, the number of copies) stated in the Provider's Supplemental Rules.

(d) Communications shall be made in the language prescribed in Paragraph 11.

(e) Either Party may update its contact details by notifying the Provider and the Registrar.

(f) Except as otherwise provided in these Rules, or decided by a Panel, all communications provided for under these Rules shall be deemed to have been made:

(i) if via the Internet, on the date that the communication was transmitted, provided that the date of transmission is verifiable; or, where applicable

(ii) if delivered by telecopy or facsimile transmission, on the date shown on the confirmation of transmission; or:

(iii) if by postal or courier service, on the date marked on the receipt.

(g) Except as otherwise provided in these Rules, all time periods calculated under these Rules to begin when a communication is made shall begin to run on the earliest date that the communication is deemed to have been made in accordance with Paragraph 2(f).

(h) Any communication by

(i) a Panel to any Party shall be copied to the Provider and to the other Party;

(ii) the Provider to any Party shall be copied to the other Party; and

(iii) a Party shall be copied to the other Party, the Panel and the Provider, as the case may be.

(i) It shall be the responsibility of the sender to retain records of the fact and circumstances of sending, which shall be available for inspection by affected parties and for reporting purposes. This includes the Provider in sending Written Notice to the Respondent by post and/or facsimile under Paragraph 2(a)(i).

(j) In the event a Party sending a communication receives notification of non-delivery of the communication, the Party shall promptly notify the Panel (or, if no Panel is yet appointed, the Provider) of the circumstances of the notification. Further proceedings concerning the communication and any response shall be as directed by the Panel (or the Provider).

The Complaint

(a) Any person or entity may initiate an administrative proceeding by submitting a complaint in accordance with the Policy and these Rules to any Provider approved by ICANN. (Due to capacity constraints or for other reasons, a Provider's ability to accept complaints may be suspended at times. In that

event, the Provider shall refuse the submission. The person or entity may submit the complaint to another Provider.)

(b) The complaint including any annexes shall be submitted in electronic form and shall:

(i) Request that the complaint be submitted for decision in accordance with the Policy and these Rules;

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Complainant and of any representative authorized to act for the Complainant in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Complainant in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);

(iv) Designate whether Complainant elects to have the dispute decided by a single-member or a three-member Panel and, in the event Complainant elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN-approved Provider's list of panelists);

(v) Provide the name of the Respondent (domain-name holder) and all information (including any postal and e-mail addresses and telephone and telefax numbers) known to Complainant regarding how to contact Respondent or any representative of Respondent, including contact information based on pre-complaint dealings, in sufficient detail to allow the Provider to send the complaint as described in Paragraph 2(a);

(vi) Specify the domain name(s) that is/are the subject of the complaint;

(vii) Identify the Registrar(s) with whom the domain name(s) is/are registered at the time the complaint is filed;

(viii) Specify the trademark(s) or service mark(s) on which the complaint is based and, for each mark, describe the goods or services, if any, with which the mark is used (Complainant may also separately describe other goods and services with which it intends, at the time the complaint is submitted, to use the mark in the future.);

(ix) Describe, in accordance with the Policy, the grounds on which the complaint is made including, in particular,

(1) the manner in which the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which the Complainant has rights; and

(2) why the Respondent (domain-name holder) should be considered as having no rights or legitimate interests in respect of the domain name(s) that is/are the subject of the complaint; and

(3) why the domain name(s) should be considered as having been registered and being used in bad faith

(The description should, for elements (2) and (3), discuss any aspects of Paragraphs 4(b) and 4(c) of the Policy that are applicable. The description shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(x) Specify, in accordance with the Policy, the remedies sought;

(xi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(xii) State that a copy of the complaint, including any annexes, together with the cover sheet as prescribed by the Provider's Supplemental Rules, has been sent or transmitted to the Respondent (domain-name holder), in accordance with Paragraph 2(b);

(xiii) State that Complainant will submit, with respect to any challenges to a decision in the administrative proceeding canceling or transferring the domain name, to the jurisdiction of the courts in at least one specified Mutual Jurisdiction;

(xiv) Conclude with the following statement followed by the signature (in any electronic format) of the Complainant or its authorized representative:

"Complainant agrees that its claims and remedies concerning the registration of the domain name, the dispute, or the dispute's resolution shall be solely against the domain-name holder and waives all such claims and remedies against (a) the dispute-resolution provider and panelists, except in the case of deliberate wrongdoing, (b) the registrar, (c) the registry administrator, and (d) the Internet Corporation for Assigned Names and Numbers, as well as their directors, officers, employees, and agents."

"Complainant certifies that the information contained in this Complaint is to the best of Complainant's knowledge complete and accurate, that this Complaint is not being presented for any improper purpose, such as to harass, and that the assertions in this Complaint are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

(xv) Annex any documentary or other evidence, including a copy of the Policy applicable to the domain name(s) in dispute and any trademark or service mark registration upon which the complaint relies, together with a schedule indexing such evidence.

(c) The complaint may relate to more than one domain name, provided that the domain names are registered by the same domain-name holder.

Notification of Complaint

(a) The Provider shall review the complaint for administrative compliance with the Policy and these Rules and, if in compliance, shall forward the complaint, including any annexes, electronically to the Respondent and shall send Written Notice of the complaint (together with the explanatory cover sheet prescribed by the Provider's Supplemental Rules) to the Respondent, in the manner prescribed by Paragraph 2(a), within three (3) calendar days following receipt of the fees to be paid by the Complainant in accordance with Paragraph 19.

(b) If the Provider finds the complaint to be administratively deficient, it shall promptly notify the Complainant and the Respondent of the nature of the deficiencies identified. The Complainant shall have five (5) calendar days within which to correct any such deficiencies, after which the administrative proceeding will be deemed withdrawn without prejudice to submission of a different complaint by Complainant.

(c) The date of commencement of the administrative proceeding shall be the date on which the Provider completes its responsibilities under Paragraph 2(a) in connection with sending the complaint to the Respondent.

(d) The Provider shall immediately notify the Complainant, the Respondent, the concerned Registrar(s), and ICANN of the date of commencement of the administrative proceeding.

The Response

(a) Within twenty (20) days of the date of commencement of the administrative proceeding the Respondent shall submit a response to the Provider.

(b) The response, including any annexes, shall be submitted in electronic form and shall:

(i) Respond specifically to the statements and allegations contained in the complaint and include any and all bases for the Respondent (domain-name holder) to retain registration and use of the disputed domain name (This portion of the response shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Respondent (domain-name holder) and of any representative authorized to act for the Respondent in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Respondent in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);

(iv) If Complainant has elected a single-member panel in the complaint (see Paragraph 3(b)(iv)), state whether Respondent elects instead to have the dispute decided by a three-member panel;

(v) If either Complainant or Respondent elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN-approved Provider's list of panelists);

(vi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(vii) State that a copy of the response including any annexes has been sent or transmitted to the Complainant, in accordance with Paragraph 2(b); and

(viii) Conclude with the following statement followed by the signature (in any electronic format) of the Respondent or its authorized representative:

"Respondent certifies that the information contained in this Response is to the best of Respondent's knowledge complete and accurate, that this Response is not being presented for any improper purpose, such as to harass, and that the assertions in this Response are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

(ix) Annex any documentary or other evidence upon which the Respondent relies, together with a schedule indexing such documents.

(c) If Complainant has elected to have the dispute decided by a single-member Panel and Respondent elects a three-member Panel, Respondent shall be required to pay one-half of the applicable fee for a three-member Panel as set forth in the Provider's Supplemental Rules. This payment shall be made together with the submission of the response to the Provider. In the event that the required payment is not made, the dispute shall be decided by a single-member Panel.

(d) At the request of the Respondent, the Provider may, in exceptional cases, extend the period of time for the filing of the response. The period may also be extended by written stipulation between the Parties, provided the stipulation is approved by the Provider.

(e) If a Respondent does not submit a response, in the absence of exceptional circumstances, the Panel shall decide the dispute based upon the complaint.

Appointment of the Panel and Timing of Decision

(a) Each Provider shall maintain and publish a publicly available list of panelists and their qualifications.

(b) If neither the Complainant nor the Respondent has elected a three-member Panel (Paragraphs 3(b)(iv) and 5(b)(iv)), the Provider shall appoint, within five (5) calendar days following receipt of the response by the Provider, or the lapse of the time period for the submission thereof, a single Panelist from its list of panelists. The fees for a single-member Panel shall be paid entirely by the Complainant.

(c) If either the Complainant or the Respondent elects to have the dispute decided by a three-member Panel, the Provider shall appoint three Panelists in accordance with the procedures identified in Paragraph 6(e). The fees for a three-member Panel shall be paid in their entirety by the Complainant, except where the election for a three-member Panel was made by the Respondent, in which case the applicable fees shall be shared equally between the Parties.

(d) Unless it has already elected a three-member Panel, the Complainant shall submit to the Provider, within five (5) calendar days of communication of a response in which the Respondent elects a three-member Panel, the names and contact details of three candidates to serve as one of the Panelists. These candidates may be drawn from any ICANN-approved Provider's list of panelists.

(e) In the event that either the Complainant or the Respondent elects a three-member Panel, the Provider shall endeavor to appoint one Panelist from the list of candidates provided by each of the Complainant and the Respondent. In the event the Provider is unable within five (5) calendar days to secure the appointment of a Panelist on its customary terms from either Party's list of candidates, the Provider shall make that appointment from its list of panelists. The third Panelist shall be appointed by the Provider from a list of five candidates submitted by the Provider to the Parties, the Provider's selection from among the five being made in a manner that reasonably balances the preferences of both Parties, as they may specify to the Provider within five (5) calendar days of the Provider's submission of the five-candidate list to the Parties.

(f) Once the entire Panel is appointed, the Provider shall notify the Parties of the Panelists appointed and the date by which, absent exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider.

Impartiality and Independence

A Panelist shall be impartial and independent and shall have, before accepting appointment, disclosed to the Provider any circumstances giving rise to justifiable doubt as to the Panelist's impartiality or independence. If, at any stage during the administrative proceeding, new circumstances arise that could give rise to justifiable doubt as to the impartiality or independence of the Panelist, that Panelist shall promptly disclose such circumstances to the Provider. In such event, the Provider shall have the discretion to appoint a substitute Panelist.

Communication Between Parties and the Panel

No Party or anyone acting on its behalf may have any unilateral communication with the Panel. All communications between a Party and the Panel or the Provider shall be made to a case administrator appointed by the Provider in the manner prescribed in the Provider's Supplemental Rules.

Transmission of the File to the Panel

The Provider shall forward the file to the Panel as soon as the Panelist is appointed in the case of a Panel consisting of a single member, or as soon as the last Panelist is appointed in the case of a three-member Panel.

General Powers of the Panel

(a) The Panel shall conduct the administrative proceeding in such manner as it considers appropriate in accordance with the Policy and these Rules.

(b) In all cases, the Panel shall ensure that the Parties are treated with equality and that each Party is given a fair opportunity to present its case.

(c) The Panel shall ensure that the administrative proceeding takes place with due expedition. It may, at the request of a Party or on its own motion, extend, in exceptional cases, a period of time fixed by these Rules or by the Panel.

(d) The Panel shall determine the admissibility, relevance, materiality and weight of the evidence.

(e) A Panel shall decide a request by a Party to consolidate multiple domain name disputes in accordance with the Policy and these Rules.

Language of Proceedings

(a) Unless otherwise agreed by the Parties, or specified otherwise in the Registration Agreement, the language of the administrative proceeding shall be the language of the Registration Agreement, subject to the authority of the Panel to determine otherwise, having regard to the circumstances of the administrative proceeding.

(b) The Panel may order that any documents submitted in languages other than the language of the administrative proceeding be accompanied by a translation in whole or in part into the language of the administrative proceeding.

Further Statements

In addition to the complaint and the response, the Panel may request, in its sole discretion, further statements or documents from either of the Parties.

In-Person Hearings

There shall be no in-person hearings (including hearings by teleconference, videoconference, and web conference), unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the complaint.

Default

(a) In the event that a Party, in the absence of exceptional circumstances, does not comply with any of the time periods established by these Rules or the Panel, the Panel shall proceed to a decision on the complaint.

(b) If a Party, in the absence of exceptional circumstances, does not comply with any provision of, or requirement under, these Rules or any request from the Panel, the Panel shall draw such inferences therefrom as it considers appropriate.

Panel Decisions

(a) A Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance with the Policy, these Rules and any rules and principles of law that it deems applicable.

(b) In the absence of exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider within fourteen (14) days of its appointment pursuant to Paragraph 6.

(c) In the case of a three-member Panel, the Panel's decision shall be made by a majority.

(d) The Panel's decision shall be in writing, provide the reasons on which it is based, indicate the date on which it was rendered and identify the name(s) of the Panelist(s).

(e) Panel decisions and dissenting opinions shall normally comply with the guidelines as to length set forth in the Provider's Supplemental Rules. Any dissenting opinion shall accompany the majority decision. If the Panel concludes that the dispute is not within the scope of Paragraph 4(a) of the Policy, it shall so state. If after considering the submissions the Panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse Domain Name Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.

Communication of Decision to Parties

(a) Within three (3) calendar days after receiving the decision from the Panel, the Provider shall communicate the full text of the decision to each Party, the concerned Registrar(s), and ICANN. The concerned Registrar(s) shall immediately communicate to each Party, the Provider, and ICANN the date for the implementation of the decision in accordance with the Policy.

(b) Except if the Panel determines otherwise (see Paragraph 4(j) of the Policy), the Provider shall publish the full decision and the date of its implementation on a publicly accessible web site. In any event, the portion of any decision determining a complaint to have been brought in bad faith (see Paragraph 15(e) of these Rules) shall be published.

Settlement or Other Grounds for Termination

(a) If, before the Panel's decision, the Parties agree on a settlement, the Panel shall terminate the administrative proceeding.

(b) If, before the Panel's decision is made, it becomes unnecessary or impossible to continue the administrative proceeding for any reason, the Panel shall terminate the administrative proceeding, unless a Party raises justifiable grounds for objection within a period of time to be determined by the Panel.

Effect of Court Proceedings

(a) In the event of any legal proceedings initiated prior to or during an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, the Panel shall

have the discretion to decide whether to suspend or terminate the administrative proceeding, or to proceed to a decision.

(b) In the event that a Party initiates any legal proceedings during the pendency of an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, it shall promptly notify the Panel and the Provider. See Paragraph 8 above.

Fees

(a) The Complainant shall pay to the Provider an initial fixed fee, in accordance with the Provider's Supplemental Rules, within the time and in the amount required. A Respondent electing under Paragraph 5(b)(iv) to have the dispute decided by a three-member Panel, rather than the single-member Panel elected by the Complainant, shall pay the Provider one-half the fixed fee for a three-member Panel. See Paragraph 5(c). In all other cases, the Complainant shall bear all of the Provider's fees, except as prescribed under Paragraph 19(d). Upon appointment of the Panel, the Provider shall refund the appropriate portion, if any, of the initial fee to the Complainant, as specified in the Provider's Supplemental Rules.

(b) No action shall be taken by the Provider on a complaint until it has received from Complainant the initial fee in accordance with Paragraph 19(a).

(c) If the Provider has not received the fee within ten (10) calendar days of receiving the complaint, the complaint shall be deemed withdrawn and the administrative proceeding terminated.

(d) In exceptional circumstances, for example in the event an in-person hearing is held, the Provider shall request the Parties for the payment of additional fees, which shall be established in agreement with the Parties and the Panel.

Exclusion of Liability

Except in the case of deliberate wrongdoing, neither the Provider nor a Panelist shall be liable to a Party for any act or omission in connection with any administrative proceeding under these Rules.

Amendments

The version of these Rules in effect at the time of the submission of the complaint to the Provider shall apply to the administrative proceeding commenced thereby. These Rules may not be amended without the express written approval of ICANN

Uniform Domain Name Resolution Policy – Relevant Case Law

America Online, Inc. v. Johuathan Investments, Inc., and AOLLNEWS.COM Case No. D 2001-0918

1. The Parties

The Complainant is America Online, Inc., 22000 AOL Way, Dulles, Virginia 20166, USA and represented by James R. Davis II, Arent Fox Kintner Plotkin & Kahn, 1050 Connecticut Avenue, NW., Washington, DC 20036, USA.

The Respondent is Johuathan Investments, Inc., and AOLLNEWS.COM, 62 Cleghorn Street, Belize City, Belize.

2. The Domains Name and Registrars

The Domain Names are <aollnews.com> and <fucknetscape.com>.

The Registrars are TuCows.com, Inc., and BulkRegister.com, Inc.

3. Procedural History

The Complaint was received by WIPO by email on July 17, 2001, and in hardcopy form on July 19, 2001. WIPO issued a Request for Amendment to Complaint on July 27, 2001. The Amended Complaint was received by email on July 30, 2001, and in hard copy form on August 3, 2001. WIPO has verified that the Complaint satisfies the formal requirements of the Policy, the Rules and the Supplemental Rules and that

payment was properly made. The Administrative Panel ("the Panel") is satisfied that this is the case.

The Complaint was properly notified in accordance with the Rules, paragraph 2(a). BulkRegister.com, Inc., has confirmed that <aollnews.com> ("the First Domain Name") was registered through BulkRegister.com, Inc. and that AOLNEWS.COM is the current registrant. Tucows.com, Inc., has confirmed that <fucknetscape.com> ("the Second Domain Name") was registered through Tucows.com, Inc., and that Johuathan Investments, Inc. is the current registrant. The Registrars have further confirmed that the Policy is applicable to the Domain Names.

For the reasons set out below the Panel treats aollnews.com as being a trading name or 'alter ego' of Johuathan Investments, Inc., and hereinafter refers to them both as "the Respondent".

On August 6, 2001, WIPO notified the Respondent of the Complaint in the usual manner and informed the Respondent *inter alia* that the last day for sending its Response to the Complainant and to WIPO was August 26, 2001. No Response was received.

The Panel was properly constituted. The undersigned Panellist submitted Statements of Acceptance and Declarations of Impartiality and Independence.

No further submissions were received by WIPO or the Panel, as a consequence of which the date scheduled for the issuance of the Panel's Decision is September 17, 2001.

4. Factual Background

The Complainant is America Online acting on its own behalf and on behalf of its affiliate Netscape Communications Corporation. In this decision I refer to them together as AOL.

AOL is the proprietor of many trade mark registrations of or incorporating the marks AOL and Netscape.

AOL has been using the mark AOL since at least as early as 1989 and the mark NETSCAPE since at least as early as 1984. Both marks are very well known marks in the area of computer online services and other internet related services. Moreover, they were very well known at the time the Domain names were registered.

Further, AOL is the registered proprietor of trade mark registrations for the mark AOL.COM, a mark it has used since at least 1992, and operates a website at (*inter alia*) www.aolnews.com.

The First Domain Name was registered on June 13, 2000, in the name of aollnews.com. The Second Domain Name was registered on April 23, 2000, in the name of Johuathan Investment Inc. The registrants have different names, but they have the same address in Belize and both have the same contact addresses and telephone numbers.

The Domain Names are connected (directly or indirectly) to commercial sites. The First Domain Name is connected to a website at <point.com>. The Second Domain Name is connected to a pornographic website. Neither of these sites contains any reference within it to either aollnews or fucknetscape.

5. Parties' Contentions

A. Complainant

The Complainant contends that aollnews.com, the registrant of the First Domain Name, and Johuathan Investments, Inc., the registrant of the Second Domain Name, are one and the same and that it is appropriate this complaint should be entertained

as a single complaint on the basis that there is a single respondent to the complaint. The Complainant points to the similarities in the various addresses and telephone numbers in the Whois records for the Domain Names.

The Complainant contends that the Domain Names are each nearly identical and are each confusingly similar to a trade mark or service mark in which the Complainant has rights. The Complainant refers to its rights in the trade marks AOL, AOL.COM and NETSCAPE. It also refers to the AOL operated website at <aolnews.com>.

The Complainant contends that at the time of registering the Domain Names the Respondent was well aware of the Complainant's rights in the aforementioned trade marks.

The Complainant contends that consumers will be likely to believe that, because of the Respondent's use of the Complainant's famous trade marks, the Complainant is in some way associated with the website. The Complainant points to the additional fact that the Whois search for the Second Domain Name shows that the Respondent uses an aol.com email address which will be likely to increase the risk of confusion. The Complainant also points to the fact that the site connected to the First Domain Name offers services similar to those offered by AOL.

The Complainant contends that the Respondent registered the Domain Names with a view to capitalising on the fame of the Complainant's trade marks.

The Complainant asserts that the Respondent has no rights or legitimate interest in respect of the Domain Names. It says that it has not granted a licence to the Respondent to use any of its marks. Further it claims that in light of what is set out in this Complaint the Respondent cannot claim in good faith that it has made a non-commercial or fair use of the Domain Names or that it is commonly known by the name AOL, Aollnews, or Netscape.

The Complainant contends that the Domain Names were registered in bad faith and are being used in bad faith.

In support, the Complainant refers to the matters set out above. The Complainant adds that the Domain Names are being used to attract commercial attention and not to define the content of the sites at <aollnews.com> and <fucknetscape.com>.

The Complainant further refers to the fact that in a previous ICANN proceeding (FA0012000096178 *Sunglass Huat Corporation v. Johuathan Investments Inc*) the Registrant was found guilty of registering the Domain Name in bad faith and using it in bad faith. The Complainant cites the case in support of a contention that it demonstrates a pattern on the part of the Respondent to register domain names with a view to preventing trade mark owners from reflecting those marks in corresponding domain names. The Complainant asserts that this is in violation of paragraph 4(b)(ii) of the Policy.

The Complainant further contends that the use of famous marks of others, particularly when connected to adult material, violates the Policy.

B. Respondent

The Respondent has not responded.

6. Discussion and Findings

According to paragraph 4(a) of the Policy, the Complainant must prove that

(i) The Domain Name is identical or confusingly similar to a trade mark or service mark in which the Complainant has rights; and

(ii) The Respondent has no rights or legitimate interest in respect of the Domain Name; and

(iii) The Domain Name has been registered and is being used in bad faith.

First, however, the Panel has to decide whether or not it was appropriate for this complaint to be entertained in circumstances where the named registrants for the Domain Names have different names. The Complainant's assertion that the registrants are in effect one and the same is clear. The assertion is credible given the domain names in issue and that the contact details (i.e. address and telephone number) for the Domain names are identical. The Panel believes it more than likely that the registrants are one and the same, but recognises that it is not impossible that the address is an accommodation address for a multiplicity of different entities.

The Respondent has elected not to respond. By virtue of Rule 14(b) the Panel is entitled to draw such inferences as it deems appropriate from the failure to respond. In the circumstances the Panel sees no reason not to accept the Complainant's uncontradicted assertion that the registrants of the Domain Names are one and the same. The Panel accepts this complaint as a properly constituted single complaint covering both Domain Names.

Identical or Confusing Similarity

The First Domain Name <aollnews.com>. This Domain Name comprises "AOLL", which is very similar to the Complainant's trade mark AOL, the term "NEWS", which is generic, and the generic dot com suffix. In combination the First Domain name is very similar indeed to the Complainant's domain name, <aolnews.com>, under and by reference to which the Complainant provides a service. The Panel finds that this Domain Name is confusingly similar to trade marks and service marks in which the Complainant has rights.

The Second Domain Name <fucknetscape.com>. This Domain Name comprises the word "FUCK", the Complainant's trade mark "NETSCAPE" and the generic dot com suffix. This Domain Name is not identical to the Complainant's trade mark, but is it confusingly similar to it?

In the trade mark context the term "confusingly similar" refers to confusion as to trade origin. Is it likely therefore that, because of the similarity between the Domain Name on the one hand and the Complainant's trade mark on the other hand, people will believe that the Domain name is associated in some way with the Complainant?

The Panel regards it as inconceivable that anyone looking at this Domain Name will believe that it has anything to do with a company of such high repute as the Complainant. It is manifestly, on its face, a name, which can have nothing whatever to do with the Complainant. It is a name, which, by its very nature, declares that it is hostile to Netscape. The Panel notes that in support of the bad faith claim the Complainant contends that the Respondent has registered this Domain Name in violation of paragraph 4(b)(ii) of the Policy on the basis that it has been done to prevent the Complainant registering the name. The Panel simply does not understand why on earth the Complainant would ever wish to register this Domain Name. There is no evidence before the Panel to support the contention. The Panel is aware that some companies seek to acquire such names, but only to forestall and/or impede the more obvious protest sites, not because they believe people will believe that the domain name in question or any site to which it is connected belongs to or is licensed or endorsed by the trade mark owner.

The Panel finds that the Complainant has failed to prove that this Domain Name is identical or confusingly similar to a trade mark or service mark in which the Complainant has rights.

Rights or Legitimate Interest of the Respondent

The Complainant asserts that it has not granted any licence to the Respondent to use the Complainant's trade marks. The Panel accepts that uncontradicted assertion. The Panel observes that there can be no reason why the Complainant would license use of its trade marks in relation to either of the domain names, one of which includes a mis-spelling and the other of which is offensive.

The Policy gives a respondent an opportunity to demonstrate to the Panel that it has rights or legitimate interests in respect of the domain names in issue. A non-exhaustive list of circumstances, which demonstrate the existence of such rights and legitimate interests, is set out in paragraph 4(c) of the Policy.

The Respondent has made no attempt to demonstrate any of those circumstances or indeed any other circumstances showing that it has rights or legitimate interests in respect of the Domain Names.

The Panel can think of no reason why the Respondent could be said to have rights or legitimate interests in respect of the Domain Names, save that aollnews.com is the registered name of the owner of the First Domain Name.

However, the circumstances are such that the Respondent clearly selected the Domain Names with the Complainant in mind, evidently well aware of the Complainant's trade mark interests in relation to them. The Panel is of the view that the business name, aollnews.com, was selected as a convenient alias for the purpose in hand and is no evidence that the Respondent has been commonly known by that name within the meaning of paragraph 4(c)(ii) of the Policy.

The Panel finds that the Respondent has no rights or legitimate interests in respect of either of the Domain Names.

Bad Faith

The First Domain Name <aollnews.com>. The circumstances are such that the Respondent knew when it registered this Domain name that it was confusingly similar to the Complainant's trade marks and domain name <aolnews.com> referred to above. The Respondent also knew that it had no rights or legitimate interests in respect of this Domain Name. This Domain Name is connected to a commercial site. In the absence of any explanation from the Respondent, the Panel is entitled to infer that the Respondent intended, for a commercial purpose, the natural and probable consequences of having effected the registration, namely confusion of internet users. In the result, the Panel finds that the First Domain Name was registered in bad faith and is being used in bad faith within the meaning of paragraph 4(b)(iv) of the Policy.

The Second Domain Name <fucknetscape.com>. Given the Panel's finding in relation to paragraph 4(a)(i) of the Policy, it is not necessary for the Panel to address this issue. For the record, however, and for the reasons set out above, the Panel rejects the Complainant's contentions that this Domain Name will be likely to lead to any relevant confusion of internet users or has in any way precluded the Complainant from registering a domain name of its choice. If there is any confusion, it will be because people expecting to visit a protest site will find themselves at a porn site. In an obvious sense, perhaps, the registration of this Domain Name is an abuse of the Domain Name System, but not an abuse of a kind covered by the Policy.

For completeness, the Panel addresses the contention by the Complainant that the content of the site to which the domain name in question is connected may have a bearing on the bad faith issue "particularly in connection with adult content". The Panel accepts that the content of a site (adult or otherwise) might well be of relevance to indicate a respondent's good faith/bad faith intentions, but each of the authorities cited by the Complainant in relation to adult material proceeds upon the basis that the domain name in issue is confusingly similar to the Complainant's trade mark. In the case of the Second Domain Name the Panel has found that the Complainant has failed to prove confusing similarity.

7. Decision

In light of the foregoing findings the complaint in respect of the First Domain Name succeeds and the Panel directs that the Domain Name, <aollnews.com>, be transferred to the Complainant. The complaint in respect of the Second Domain Name, <fucknetscape.com>, is dismissed.

Tony Willoughby
Sole Panelist

Dated: September 14, 2001

Wal-Mart Stores, Inc. v. Richard MacLeod d/b/a For Sale Case No. D2000-0662

1. The Parties

The Complainant is Wal-Mart Stores, Inc., a United States corporation with its headquarters in Bentonville, Arkansas, United States of America.

The Respondent is Richard MacLeod d/b/a For Sale, 21 Simpson Avenue, Toronto, ON M8Z1C9, United States of America.

2. The Domain Name and Registrar

The domain name at issue is wal-martsucks.com. The domain name is registered with Register.com.

3. Factual Background

The Panel has reviewed the Complainant's Complaint and Respondent's Response. The following facts appear to be undisputed: The Complainant operates over 2,500 stores worldwide. All its trading operations, advertisements and promotions are conducted under the mark "Wal-Mart," and it has used this mark continuously since 1962. Its Internet addresses include walmart.com, wal-mart.com, and walmartstores.com. Its businesses include discount retail stores, grocery stores, pharmacies, membership warehouse clubs, and deep discount warehouse outlets.

Complainant holds registrations for the mark "Wal-Mart" in the United States, Switzerland, the United Kingdom, Denmark, and numerous other countries. The Respondent has no rights granted by the Complainant in any of the marks involving the word "Wal-Mart".

The Respondent registered the domain name wal-martsucks.com on February 12, 2000.

4. Procedural Background

Complainant filed its Complaint by email on June 22, 2000. Because of a deficiency noted by the Center (Complainant had failed to comply with Rule 3(b)(xiii)), Complainant filed an Amended Complaint, which was received in hardcopy by the Center on July 10, 2000.

On July 14, 2000, the Center formally commenced this proceeding and notified Respondent that its Response would be due by August 2, 2000. Respondent timely filed its Response, which was received by the Center in hardcopy on July 26, 2000. Meanwhile, on July 20, 2000, the Center released a decision in Wal-Mart Stores, Inc. v. Walsucks and Walmarket Puerto Rico, Case No. D2000-0477, which involved the same Complainant. The Panel in that case ruled that the domain names wal-martcanadasucks.com, walmartcanadasucks.com,

walmartuksucks.com, walmartpuertorico.com and walmartpuertoricosucks.com were confusingly similar to Complainant's Wal-Mart trademark, that the respondent in that case lacked a legitimate interest in the domain names, and that the domain names were registered and used in bad faith. The Panel thus ordered that the domain names be transferred to the Complainant.

On July 25, 2000, Complainant in this case requested leave to submit a reply in light of the decision in Case No. D2000-0447. On July 26, 2000, the Respondent indicated that he would not object to the filing of a reply, and requested that he be allowed to submit a sur-reply.

On August 4, 2000, the Center appointed a Panel. The Panelist thereafter developed a conflict of interest, and recused himself. On September 6, 2000, the Center appointed David H. Bernstein as a substitute Panelist. Neither party requested a three-member Panel.

On September 6, 2000, the Panel issued an order denying the Complainant's request for leave to file a reply, except that the Panel took note of the decision in Case No. D2000-0447, and denying as moot the Respondent's request to submit a sur-reply. On September 17, 2000, the Respondent asked that he be allowed to submit a statement regarding Case No. D2000-0447. In particular, Respondent requested the right to supplement his Response because, "[s]hould this case be used against me, I believe it would be fair to give me a chance to submit a few comments about that case."

The Panel denies Respondent's request to supplement his Response. First, the request is moot because Case No. D2000-0447 has not been "used against" him; the issues in this case are quite different and, although this Panel has read the decision in Case No. D2000-0447, that decision has not affected the Panel's findings and conclusions in this case. More generally, Respondent's request is inconsistent with the expedited process created by ICANN. If parties were allowed to supplement their submissions based solely on the issuance of a decision by another Panel, it would, given the pace with which UDRP decisions are issued, allow parties endlessly to drag out the UDRP process with replies and sur-replies and sur-sur-replies. See Document Technologies, Inc. v. International Electronic Communications, Inc., Case No. D2000-0270 (WIPO, June 6, 2000) (denying Complainant's request to file reply where proposed reply raised no new legal or factual authority, and thus would unnecessarily delay the final adjudication). When a new, relevant decision is issued (whether by another Panel or by a court), the appropriate course instead is for a party to bring the decision to the Panel's attention, without providing additional, substantive argument, so that the Panel can review the decision and use its own judgment as to whether that decision is relevant to the issues in the case before the Panel and, if so, how it affects the decision in the instant case. See Pet Warehouse v. Pets.Com, Inc., Case No. D2000-0105 (WIPO, Apr. 13, 2000) (accepting supplemental submission comprised of a new decision by another UDRP Panel that was submitted "without any argument").

5. Parties' Allegations

The Complainant submits that its mark is famous throughout the United States and all those other countries in which it trades. It further argues that the domain name is identical to its "Wal-Mart" mark because the domain name wholly incorporates "Wal-Mart" and also is confusingly similar to its "Wal-Mart" marks because "Wal-Mart" is so famous that buyers "would be likely to think that any commercial site connected with the domain name wal-martsucks.com, particularly a site selling consumer products," or "any domain name incorporating the Wal-Mart name (or a close approximation thereof)" originates with the Complainant.

The Complainant argues that Respondent has no rights or legitimate interests in respect of the domain name. First, Respondent is not currently using the domain name in connection with any ongoing business. Second, to the best of the Complainant's knowledge, Respondent has no rights to any use of the term Wal-Mart.

The Complainant further submits that the domain name wal-

martsucks.com was registered and is used in bad faith. Improper use of the name is shown by the Respondent's attempt to sell the name through the Great Domains website for \$530,000 and on Respondent's website for \$545,000.

The Respondent focuses his response on the first factor of the ICANN policy, arguing that wal-martsucks.com is neither identical to nor confusingly similar to "Wal-Mart." He relies on *Bally Total Fitness Holding Corp. v. Faber*, 29 F. Supp. 2d 1161 (C.D. Cal. 1998), which concluded that the addition of the word "sucks" prevents any reasonably prudent user from confusing a "sucks" website with an authorized website.

Respondent concedes that his original intention upon registration of wal-martsucks.com was to sell the name for profit, and concedes that this constitutes registration in bad faith, but claims that he had a "change of heart" when he learned of Wal-Mart's abusive employment and consumer practices, so that the website no longer is being "used" in bad faith. He further claims that Wal-Mart cannot prove that it was actually Respondent who offered wal-martsucks.com for sale because Great Domains does not verify sellers. Thus, he claims that Complainant has insufficient evidence to show bad faith. Finally, he suggests that Complainant knew of the availability of the wal-martsucks.com domain name long before he registered it and should have done so when the name was available.

6. Discussion and Findings

The burden for the Complainant under paragraph 4(a) of the ICANN Policy is to prove:

(a) That the domain name registered by the Respondent is identical or confusingly similar to a trademark or service mark in which the Complainant has rights;

(b) That the Respondent has no rights or legitimate interests in respect of the domain name; and

(c) The domain name has been registered and used in bad faith. Initially, the Panel rejects any suggestion that Complainant's failure to register wal-martsucks.com before Respondent did so precludes this Complaint under any theory, including laches. Trademark owners are not required to create "libraries" of domain names in order to protect themselves, and there are strong policy reasons against encouraging this behavior. Moreover, as human creativity reaches its utmost where disparagement (not to mention money) is involved, any such attempt by a trademark owner would be futile, and thus Respondent has no equitable argument against Complainant.

The second and third elements of the Policy are easily disposed of in this case. Respondent's sole argument with respect to the second element is that he is using wal-martsucks.com to criticize Wal-Mart. Respondent could potentially have a legitimate interest in using wal-martsucks.com as a site critical of Wal-Mart; the Policy specifically provides that "a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark," can establish legitimate rights and interests in a domain name. Policy paragraph 4(c)(iii). In this case, however, Complainant alleges, and Respondent does not deny, that before Complainant initiated the present proceeding, he was using the site solely for the purpose of selling it. While Respondent claims to have had a "change of heart," this change appears to have been driven by his domain name disputes with Complainant, and it is too little, too late.

Respondent admits that he registered the domain name in bad faith. The Panel specifically rejects Respondent's argument that Complainant produced insufficient evidence of bad faith use. Though Respondent questions the reliability of the information on the Great Domains website (Respondent claims that anyone can list a domain name for sale on that site, and thus Complainant has not proven that it is Respondent who offered the name for sale), he never actually denies that it was he who listed wal-martsucks.com on Great Domains, nor does he deny that he offered the domain name for sale on his own site. Indeed, the Respondent's intent is made clear by the name in which he registered the domain name: "For Sale." See *Unibanco v. Vendo Domain Sale*, Case No. D2000-0671 (WIPO, Aug. 31, 2000). Combined with Respondent's own admission, this is

ample evidence of bad faith use. Again, Respondent's newly developed critical use of the site during the pendency of this proceeding is insufficient to erase the prior bad faith use.

The difficult question in this case is whether Complainant has shown that wal-martsucks.com "is identical or confusingly similar to" Complainant's mark under Paragraph 4(a)(1) of the Policy. In prior cases, this Panel has held that a domain name that incorporates a mark but also adds another word is not "identical" to the mark under the Policy. See, e.g., *EAuto, L.L.C. v. Triple S. Auto Parts d/b/a Kung Fu Yea Enterprises, Inc.*, No. D2000-0047 (WIPO, Mar. 24, 2000). This Panel has also held that incorporating a distinctive mark in its entirety creates sufficient similarity between the mark and the domain name to render it confusingly similar. *Id.*

Following this reasoning, Complainant contends that consumers are likely to believe that any domain name incorporating the sequence "Wal-Mart" or a close approximation thereof is associated with Complainant. In the ordinary case, when a generic term is appended to the trademark (such as the domain name *walmartstores.com*), this would be so. But the fame of a mark does not always mean that consumers will associate all use of the mark with the mark's owner. No reasonable speaker of modern English would find it likely that Wal-Mart would identify itself using *wal-martsucks.com*. Complainant has no evidence of any potential confusion. The Panel specifically rejects Complainant's argument that consumers are likely to be confused as to the sponsorship or association of a domain name that combines a famous mark with a term casting opprobrium on the mark.

Nevertheless, the Panel understands the phrase "identical or confusingly similar" to be greater than the sum of its parts. The Policy was adopted to prevent the extortionate behavior commonly known as "cybersquatting," in which parties registered domain names in which major trademark owners had a particular interest in order to extort money from those trademark owners. This describes Respondent's behavior. Thus, the Panel concludes that a domain name is "identical or confusingly similar" to a trademark for purposes of the Policy when the domain name includes the trademark, or a confusingly similar approximation, regardless of the other terms in the domain name. In other words, the issue under the first factor is not whether the domain name causes confusion as to source (a factor more appropriately considered in connection with the legitimacy of interest and bad faith factors), but instead whether the mark and domain name, when directly compared, have confusing similarity. Having so concluded, Respondent's use of the domain name *wal-martsucks.com* meets all three of the conditions necessary to justify a transfer of the domain name to Complainant.

The Panel is cognizant of the importance of protecting protest sites that use a trademark to identify the object of their criticism. The "legitimate interest" and "bad faith" factors should adequately insulate true protest sites from vulnerability under the Policy, especially as the Complainant retains the burden of proof on each factor. Where, as here, a domain name registrant does not use a site for protest but instead offers it for sale for substantially more than the costs of registration, the site does not further the goal of legitimate protest; rather, it constitutes trademark piracy.

7. Decision

For the foregoing reasons, the Panel decides:

(a) that the domain name *wal-martsucks.com* is identical or confusingly similar to the Wal-Mart trademark in which the Complainant has rights;

(b) that the Respondent has no rights or legitimate interests in respect of the domain name; and

(c) the Respondent's domain name has been registered and is being used in bad faith.

Accordingly, pursuant to paragraph 4(i) of the Policy, the Panel requires that the registration of the domain name *wal-martsucks.com* be transferred to the Complainant.

David H. Bernstein

Sole Panelist

Dated: September 19, 2000

FC Bayern München AG v. Peoples Net Services Ltd. Case No. D2003-0464

1. The Parties

The Complainant is FC Bayern München AG, of Munich, Germany, represented by Beiten Burkhardt Goerdeler of Germany.

The Respondent is Peoples Net Services Ltd., Mr. Sam Rosen, Director, of London, United Kingdom of Great Britain and Northern Ireland.

2. The Domain Names and Registrar

The disputed domain names <bayernmuenchen.net> and <bayernmunchen.net> are registered with Domain Bank.

3. Procedural History

The Complaint was filed with the WIPO Arbitration and Mediation Center (the "Center") on June 16, 2003. On June 18, 2003, the Center transmitted by email to Domain Bank a request for registrar verification in connection with the domain names at issue. On June 19, 2003, Domain Bank transmitted by email to the Center its verification response confirming that the Respondent is listed as the registrant and providing the contact details for the administrative and technical contact. The Center verified that the Complaint satisfied the formal requirements of the Uniform Domain Name Dispute Resolution Policy (the "Policy"), the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules"), and the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy (the "Supplemental Rules").

In accordance with the Rules, paragraphs 2(a) and 4(a), the Center formally notified the Respondent of the Complaint, and the proceedings commenced on June 24, 2003. In accordance with the Rules, paragraph 5(a), the due date for Response was July 14, 2003. The Response was filed with the Center on June 24, 2003.

The Center appointed Peter G. Nitter as the sole panelist in this matter on July 1, 2003. The Panel finds that it was properly constituted. The Panel has submitted the Statement of Acceptance and Declaration of Impartiality and Independence, as required by the Center to ensure compliance with the Rules, paragraph 7.

4. Factual Background

The Complainant is FC Bayern München AG, a stock corporation which since 2002, operates the soccer activities of FC Bayern München e.V., a registered association founded in 1900.

All trademarks and name rights formerly held by FC Bayern München e.V. were transferred to FC Bayern München AG January 5, 2002.

The Complainant has activities in all major sports, but is particularly known for its football team. The football team Bayern Muenchen is one of the most successful teams in the world and the most famous team in Germany.

The Complainant's trademark FC BAYERN MÜNCHEN E.V with the club logo forms the subject-matter of trademark registrations in about 30 countries. Among these is a registration in the UK (register no. 2004623) with a priority date of November 4, 1994, inter alia registered for numerous merchandising goods and printed matter, and a Community Trademark CTM000494187 with a priority date of November 23, 1998.

The Complainant uses the trademarks by granting the right to use the trademark to a third party (licensing). The licensees produce and distribute a wide variety of products with the trademarks.

5. Parties' Contentions

A. Complainant

Confusingly Similar

BAYERN MÜNCHEN is the specifying part of the club logo. Apart from the specifying part, the logo contains two descriptive elements: "FC" is the abbreviation for "football club" and "e.V." stands for "registered association".

BAYERN MÜNCHEN is also the name of the Complainant.

The Complainant has a worldwide reputation and is also very well-known in the UK.

A study done by a consulting firm presented by the Complainant concluded that the Complainant is in the Top Ten of the world's best-known and most valuable brand names in sports.

As the letter (umlaut) "ü" is not used outside Germany, the common international way to spell words with umlauts is to replace the "ü" by "ue", so that it reads "Bayern Muenchen". This in particular applies to domain names, as umlauts cannot be used in domain names. Sometimes, the dots on the "ü" are overlooked, and the "ü" is simply replaced by a "u", so that it reads "Bayern Munchen". Both ways to spell the name are common and widely used.

The Complainant is also the registered owner of numerous international Internet domains which contain its name, for example these which are most similar to the domain name in dispute:

<bayernmuenchen.com>

<bayernmuenchen.de>

<bayern-muenchen.com>

The domain names <bayernmuenchen.net> and <bayernmunchen.net> are nothing but the international spelling of "Bayern München" and thus identical to the specifying part of the numerous trademarks of the Complainant used worldwide.

No Rights or Legitimate Interests

The Respondent has no legitimate right to use the disputed domain names.

The Respondent is not commonly known by the domain names. The Respondent offers email services, where the user can choose from "hundreds of domain names". The Respondent offers approximately 1600 domain names, including several which includes the word "football" etc.

With the commercial service provided by the Respondent, any user who is willing to pay the fees may use an email address with any of the domain names as the last part of an email address. Accordingly, the Respondent also offers email addresses like john@bayernmuenchen.net and tickets@bayernmuenchen.net.

The use of such email addresses may lead to considerable confusion as it appears to be an official email address of the Complainant itself. The use of such email addresses is beyond the control of the Complainant and endangers the reputation of the name and trademarks of the Complainant.

The Respondent also makes use of the well-known name for his own business activities. Any user who enters the sites at the disputed domain names is led to the web page of the Respondent, on which he offers his commercial service. This is an obvious attempt to divert customers and fans of the Complainant to promote the business of the Respondent.

Bad Faith

The domain names clearly refer to the Complainant as the famous soccer club.

When registering the domain names, it was of course known to the Respondent that these domains use the name of the world-famous soccer club. The Complainant is also famous in the UK. The Respondent is familiar with football, as his other football domains demonstrate.

The Respondent intentionally attempted to attract, for commercial gain, Internet users to the Respondent's web site by creating a likelihood of confusion with the Complainant's mark and name as to the sponsorship, affiliation, or endorsement of the Respondent's web site or the services constituting the Respondent's business activities. The Respondent hoped that soccer fans would want to use an email address with the name of their favorite club, and thus attempted to use the famous name of the Complainant for his own profit.

B. Respondent

Confusingly Similar

The Complainant may have registered trademarks identical to the disputed domain names for Football Club purposes and associated activities only.

The disputed domains mean Bavaria Munich and are therefore generic in nature like Paris France or London England.

The Respondent never sought to use the domains in any connection with the Complainant's business or other activities. Rights or Legitimate Interests

The Respondent has full rights over the disputed domain names as they are generic in nature and in the public domain in so far as they relate to geographical place names.

Bad Faith

The disputed domain names have never nor will ever be used in bad faith. They are currently used to provide e-mail addresses to our customers of "www.Okmail.com". There has never been an offer by the Respondent to sell or otherwise transfer the domains to the Complainant.

6. Discussion and Findings

Paragraph 4(a) of the Policy lists three tests, which a complainant must satisfy in order to succeed. The Complainant must satisfy that:

(i) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) the respondent has no rights or legitimate interests in respect of such domain name; and

(iii) the domain name has been registered in bad faith and is being used in bad faith.

A. Identical or Confusingly Similar

The domain names in dispute are <bayernmuenchen.net> and <bayernmunchen.net>.

The Complainant's trademark is FC BAYERN MÜNCHEN E.V with the club logo is registered in about 30 countries. Among these, there is a registration in the UK (register no. 2004623) with a priority date of November 4, 1994, and a Community Trademark CTM000494187 with a priority date of November 23, 1998.

The two descriptive elements in the trademark: "FC" which is the abbreviation for "football club" and "e.V." which stands for "registered association" can not be taken into account.

The conclusion is that the disputed domain names both are confusingly similar to Complainant's registered trademarks.

B. Rights or Legitimate Interests

The disputed domain names contain geographical place names. But in the Panel's opinion the name BAYERN MÜNCHEN has a secondary meaning, namely the famous soccer club of the Complainant.

The Respondent is not commonly known by the domain names. The Respondent uses the well-known name BAYERN MÜNCHEN for his own business activities, which has no connection to the geographical areas Bayern or München. The Respondent offers commercial email services on the sites which the domain names leads to. The Panel finds that this is an attempt to divert Internet users for commercial gain.

A user who enters the Respondent's sites can choose from a large number of domain names. A user who pays the fees can use an email address with any of the domain names as the last part of an email-address. The Respondent offers email addresses like tickets@bayernmuenchen.net, which may lead to considerable confusion as it appears to be an official email address of the Complainant itself.

The Respondent has no right or legitimate interests to use the disputed domain names.

C. Registered and Used in Bad Faith

There is no evidence that the Respondent has offered to sell or otherwise transfer the domains to the Complainant.

However, the domain name include the well-known name of the Complainant and the well-known trademarks of the Complainant.

When registering the domain names, this must have been obvious to the Respondent, as the Complainant is also famous in the UK. It is likely that the Respondent is familiar with football, as he has several other football domains, but even if this was not the case it would be likely that he knew about the Complainant and the Complainant's trademarks.

The Panel finds that the Respondent intentionally attempted to attract, for commercial gain, Internet users to the Respondent's web site by creating a likelihood of confusion with the Complainant's mark and name as to the sponsorship, affiliation,

or endorsement of the Respondent's web site or the services constituting the Respondent's business activities.

The Panel finds that the domain names were registered and used in bad faith.

7. Decision

For all the foregoing reasons, in accordance with Paragraphs 4(i) of the Policy and 15 of the Rules, the Panel orders that the domain names, <bayernmuenchen.net> and <bayernmunchen.net> be transferred to the Complainant.

Peter G. Nitter

Dr. Michael Crichton v. In Stealth Mode Case No: D2002-0874

1. The Parties

The Complainant is Dr. Michael Crichton of United States of America, represented by White O'Connor Curry & Avanzado LLP of United States of America.

The Respondent is In Stealth Mode of Maryland, United States of America.

2. The Domain Name and Registrar

The disputed domain name <michael-crichton.com> is registered with Stargate Communications.

3. Procedural History

This is an administrative proceeding pursuant to the Uniform Domain Name Dispute Resolution Policy ("the Policy") adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN") on August 26, 1999, the Rules for Uniform Domain Name Dispute Resolution Policy, approved by ICANN on October 24, 1999, ("the Rules") and the Supplemental Rules for Uniform Domain Name Dispute Resolution Policy ("the Supplemental Rules") of the WIPO Arbitration and Mediation Center ("the Center").

The Complaint was filed with the WIPO Arbitration and Mediation Center (the "Center") on September 18, 2002, by email, and in hard copy. Next day the Center acknowledged its receipt and transmitted by email to the Registrar a request for registrar verification in connection with the disputed domain name. On September 26, 2002, the Registrar confirmed that the Respondent is the registrant and that the record was created on June 4, 2002. The Registrar provided contact details for the administrative, billing, and technical contacts and informed the Center that the Policy applies to the disputed domain name, which is locked during the proceedings; that the language of the registration agreement is English and that the registrant has submitted to the jurisdiction at the location of the principal office of the Registrar for court adjudication of disputes concerning or arising from the use of the domain name. The Center satisfied itself that the Complaint complied with the formal requirements of the Policy, the Rules and the Supplemental Rules.

In accordance with the Rules, paragraphs 2(a) and 4(a), the Center formally notified the Respondent of the Complaint and the proceedings commenced on September 27, 2002. In accordance with the Rules, paragraph 5(a), the due date for Response was October 17, 2002. The Respondent did not submit any Response. Accordingly, the Center notified the parties of the Respondent's default on October 18, 2002.

The Center appointed Richard W. Page, Esq., Jeffrey M. Samuels, Esq., and Alan L. Limbury Esq., as Panelists on November 12, 2002. The Panel finds that it was properly constituted. Each member of the Panel has submitted the Statement of Acceptance and Declaration of Impartiality and Independence, as required by the Center to ensure compliance with the Rules, paragraph 7.

The language of the proceeding was English, being the language of the registration agreement.

4. Factual Background (uncontested facts)

Complainant is a well-known author and director who has published numerous books, screenplays and other works under his own name. These include:

Novels:

"The Andromeda Strain", published in 1969;
"The Great Train Robbery", published in 1975;
"Congo", published in 1980;
"Sphere", published in 1987;
"Jurassic Park", published in 1990;
"Rising Sun", published in 1992;
"Disclosure", published in 1993;
"Airframe", published in 1996; and
"Timeline", published in 1999.

Non-fiction Books:

"Five Patients", published in 1970;
"Jasper Johns", published in 1977;
"Electronic Life", published in 1983; and
"Travels", published in 1988.

Motion Pictures:

"The Andromeda Strain", released in 1971;
"Westworld", released in 1973;
"Coma", released in 1977;
"The Great Train Robbery", released in 1978;
"Runaway", released in 1984;
"Rising Sun", released in 1993;
"Jurassic Park", released in 1993;
"Disclosure", released in 1995;
"Twister", released in 1996; and
"The Lost World", released in 1997.

Television:

"ER", broadcast from 1994 through the present.

Respondent registered the disputed domain name on June 4, 2002. It connects Internauts to Respondent's <ebuzz.com> website, which carries nothing about Complainant or his works but advertises commercial services, such as its "matchmaker" and messaging services.

Respondent is not, and has never been, personally or professionally known as Michael Crichton. Respondent does not transact in goods or services related to Michael Crichton, and is not otherwise authorized or permitted to use the name Michael Crichton. Complainant contacted Respondent requesting the transfer of the disputed domain name, but Respondent failed to reply.

5. Parties' Contentions

A. Complainant

Complainant's name has become a famous common law trademark. The disputed domain name is identical to the mark. Respondent has no rights or legitimate interests in the disputed domain name, which was registered and is being used in bad faith.

B. Respondent

The Respondent did not reply to the Complainant's contentions.

6. Discussion and Findings

Under paragraph 15(a) of the Rules, the Panel must decide this Complaint on the basis of the statements and documents submitted and in accordance with the Policy, the Rules and any rules and principles of law that it deems applicable.

To qualify for cancellation or transfer, a Complainant must prove each element of paragraph 4(a) of the Policy, namely:

- (i) the disputed domain name is identical or confusingly similar to a trademark or service mark in which Complainant has rights; and
- (ii) Respondent has no rights or legitimate interests in respect of the domain name; and
- (iii) the disputed domain name has been registered and is being used in bad faith.

Failure to File a Response

A respondent is not obliged to participate in a domain name dispute proceeding, but if it were to fail to do so, asserted facts that are not unreasonable would be taken as true and the respondent would be subject to the inferences that flow naturally from the information provided by the complainant: Reuters Limited v. Global Net 2000, Inc., WIPO Case No. D2000-0441. See also Hewlett-Packard Company v. Full System, NAF Case No. FA 0094637; David G. Cook v. This Domain is For Sale, NAF Case No. FA0094957 and Gorstew Jamaica and Unique Vacations, Inc. v. Travel Concierge, NAF Case No. FA0094925.

A. Identical or Confusingly Similar

In light of the Second WIPO Domain Name Process, it is clear that the Policy is not intended to apply to personal names that have not been used commercially and acquired secondary meaning as the source of goods and/or services, i.e. common law trademark rights: The Reverend Dr. Jerry Falwell and The Liberty Alliance v. Gary Cohn, Prolife.net and God.info, WIPO Case No. D2002-0184; Israel Harold Asper v. Communication X Inc., WIPO Case No. D2001-0540; Kathleen Kennedy Townsend v. B. G. Birt, WIPO Case No. D2002-0030; R.E. 'Ted' Turner and Ted Turner Film Properties, LLC v. Mazen Fahmi, WIPO Case No. D2002-0251.

To establish common law rights in a personal name, it is necessary to show use of that name as an indication of the source of goods or services supplied in trade or commerce and that, as a result of such use, the name has become distinctive of that source. Upon such proof, a celebrity's name can serve as a trademark when used to identify the celebrity's performance services: Kevin Spacey v. Alberta Hot Rods, NAF Case No. FA0205000114437.

Complainant has claimed to be the author of the numerous works already identified. Respondent has not contested this. The Panel therefore infers that Complainant has, through use, acquired common law trademark rights in his name. The Panel finds the disputed domain name is identical to Complainant's mark. Complainant has established this element of his case.

B. Rights or Legitimate Interests

Likewise, in the absence of a Response, the Panel accepts that Respondent is not known by the disputed domain name, does not transact in goods or services related to Complainant and is not authorized by Complainant to use his mark. These circumstances are sufficient to constitute a prima facie showing by Complainant of absence of rights or legitimate interests in the disputed domain name on the part of Respondent. The evidentiary burden, therefore, shifts to Respondent to show that it does have rights or legitimate interests in the domain name, whether by reference to the examples set out in paragraph 4(c) of the Policy or otherwise: Do The Hustle, LLC v. Tropic Web, WIPO Case No. D2000-0624 and the cases there cited. Respondent has made no such showing.

Internet users who access the disputed domain name are automatically transported to Respondent's commercial website at <ebuzz.com>. In similar circumstances, the Panel in Stephanie Seymour v. Jeff Burgar d/b/a Stephanie Seymour Club, NAF Case No. FA0104000097112 held that by virtue of serving only as a portal, such a website "evidences no bona fide authorized offering of goods and services whatsoever and does nothing but misappropriate Complainant's trademark in order to lure Internet users to Respondent's commercial site". Likewise in Michael Andretti v. Alberta Hot Rods, NAF Case No. FA0108000099084.

Here, as in Stephanie Seymour and Michael Andretti, Complainant's name is well-known as a trademark. Accordingly, Respondent's unauthorized use of the disputed domain name to lead to the <ebuzz.com> site cannot be accepted as bona fide use.

The Panel finds Respondent has no rights or legitimate interest in the disputed domain name. Complainant has established this element of its case.

C. Registered and Used in Bad Faith

Internauts entering a domain name of a celebrity famously associated in commerce with the supply of goods or services expect to find a site offering goods or services associated with the celebrity's trademark. Here they find a site that has no association with Complainant or his mark. It follows that the Panel finds Respondent has used the disputed domain name intentionally to attempt to attract, for commercial gain, Internauts to its website by creating a likelihood of confusion with Complainant's mark as to the source, sponsorship, affiliation or endorsement of its website. Under paragraph 4(c)(iv) of the Policy, this shall be evidence of both bad faith registration and use.

7. Decision
For all the foregoing reasons, in accordance with paragraphs 4(i) of the Policy and 15 of the Rules, the Panel orders that the

domain name <michael-crichton.com> be transferred to Complainant.

1. The Parties

Uniform Rapid Suspension System ("URS") Rules

1. Complaint

1.1 Filing the Complaint

Proceedings are initiated by electronically filing with a URS Provider a Complaint outlining the trademark rights and the actions complained of entitling the trademark holder to relief. Each Complaint must be accompanied by the appropriate fee, which is under consideration. The fees are non-refundable. One Complaint is acceptable for multiple related companies against one Registrant, but only if the companies complaining are related. Multiple Registrants can be named in one Complaint only if it can be shown that they are in some way related.

1.2 Contents of the Complaint

The Complaint will be submitted using a form made available by the Provider. The Form Complaint shall include space for the following:

Name, email address and other contact information for the Complaining Party (Parties).

Name, email address and contact information for any person authorized to act on behalf of Complaining Parties.

Name of Registrant (i.e. relevant information available from Whois) and Whois listed available contact information for the relevant domain name(s).

The specific domain name(s) that are the subject of the Complaint. For each domain name, the Complainant shall include a copy of the currently available Whois information and a description and copy, if available, of the offending portion of the website content associated with each domain name that is the subject of the Complaint.

The specific trademark/service marks upon which the Complaint is based and pursuant to which the Complaining Parties are asserting their rights to them, for which goods and in connection with what services.

An indication of the grounds upon which the Complaint is based setting forth facts showing that the Complaining Party is entitled to relief, namely: that the registered domain name is identical or confusingly similar to a word mark: (i) for which the Complainant holds a valid national or regional registration and that is in current use; or (ii) that has been validated through court proceedings; or (iii) that is specifically protected by a statute or treaty in effect at the time the URS complaint is filed.

a. Use can be shown by demonstrating that evidence of use - which can be a declaration and one specimen of current use in commerce - was submitted to, and validated by, the Trademark Clearinghouse)

b. Proof of use may also be submitted directly with the URS Complaint.

and
that the Registrant has no legitimate right or interest to the domain name;

and
that the domain was registered and is being used in bad faith.

A non-exclusive list of circumstances that demonstrate bad faith registration and use by the Registrant include:

Registrant has registered or acquired the domain name primarily for the purpose of selling, renting or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of documented out-of-pocket costs directly related to the domain name; or

Registrant has registered the domain name in order to prevent the trademark holder or service mark from reflecting the mark in a corresponding domain name, provided that Registrant has engaged in a pattern of such conduct; or

Registrant registered the domain name primarily for the purpose of disrupting the business of a competitor; or

By using the domain name Registrant has intentionally attempted to attract for commercial gain, Internet users to Registrant's web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of Registrant's web site or location or of a product or service on that web site or location.1.2.7 A box in which the Complainant may submit up to 500 words of explanatory free form text.

An attestation that the Complaint is not being filed for any improper basis and that there is a sufficient good faith basis for filing the Complaint.

2. Fees

Fees as set for in the Provider's fee schedule shall be submitted with the filed Complaint.

Complaints listing fifteen (15) or more disputed domain names registered by the same registrant will be subject to a Response Fee which will be refundable to the prevailing party. Under no circumstances shall the Response Fee exceed the fee charged to the Complainant.

3. Administrative Review

Complaints will be subjected to an initial administrative review by the URS Provider for compliance with the filing requirements. This is a review to determine that the Complaint contains all of the necessary information, and is not a determination as to whether a prima facie case has been established.

The Administrative Review shall be conducted within two (2) business days of submission of the Complaint to the URS Provider.

Given the rapid nature of this Procedure, and the intended low level of required fees, there will be no opportunity to correct inadequacies in the filing requirements.

If a Complaint is deemed non-compliant with filing requirements, the Complaint will be dismissed without prejudice to the Complainant filing a new complaint. The initial filing fee shall not be refunded in these circumstances.

4. Notice and Locking of Domain

Upon completion of the Administrative Review, the URS Provider must immediately notify the Registry Operator (via email) after the Complaint has been deemed compliant with

the filing requirements. Registry Operator notice shall include a copy of the Complaint. Within 24 hours of receipt of the Notice of Complaint from the URS Provider, the Registry Operator shall "lock" the domain, meaning the registry shall restrict all changes to the registration data, including transfer and deletion of the domain names, but the name will continue to resolve. The Registry Operator will notify the URS Provider immediately upon locking the domain name ("Notice of Lock").

Within 24 hours after receiving Notice of Lock from the Registry Operator, the URS Provider shall notify the Registrant of the Complaint ("Notice of Complaint"), sending a hard copy of the Notice of Complaint to the addresses listed in the Whois contact information, and providing an electronic copy of the Complaint, advising of the locked status, as well as the potential effects if the Registrant fails to respond and defend

against the Complaint. Notices must be clear and understandable to Registrants located globally. The Notice of Complaint shall be in English and translated by the Provider into the predominant language used in the Registrant's country or territory.

The Notice of Complaint to the Registrant shall be sent through email, fax (where available) and postal mail. The Complaint and accompanying exhibits, if any, shall be served electronically.

The URS Provider shall also electronically notify the Registrar of record for the domain name at issue via the addresses the registrar has on file with ICANN.

5. The Response

A Registrant will have 14 Calendar Days from the date the URS Provider sent its Notice of Complaint to the Registrant to electronically file a Response with the URS Provider. Upon receipt, the Provider will electronically send a copy of the Response, and accompanying exhibits, if any, to the Complainant.

Respondent shall pay a Response Fee as set forth in section 2.2 above if the Complaint lists fifteen (15) or more disputed domain names against the same Registrant. In the case of fifteen (15) or more disputed domain names, the Response Fee will be refundable to the prevailing party. No additional filing fee will be charged if the Registrant files its Response prior to being declared in default or not more than thirty (30) Calendar Days following a Default Determination. For Responses filed more than thirty (30) Calendar Days after a Default Determination, regardless of the number of domain names in the Complaint, shall pay a reasonable non-refundable fee set forth in the Provider Supplemental Rules for re-examination (in addition to any applicable Response Fee required in URS Procedure 2.2).

Upon request by the Registrant, a limited extension of time to respond may be granted by the URS Provider if there is a good faith basis for doing so and if the request is received during the Response period, after Default, or not more than thirty (30) Calendar Days after Determination. In no event shall the extension be for more than seven (7) Calendar Days.

The Response shall be no longer than 2,500 words, excluding attachments, and the content of the Response should include the following:

Confirmation of Registrant data.

Specific admission or denial of each of the grounds upon which the Complaint is based.

Any defense which contradicts the Complainant's claims.

A statement that the contents are true and accurate.

In keeping with the intended expedited nature of the URS and the remedy afforded to a successful Complainant, affirmative claims for relief by the Registrant will not be permitted except for an allegation that the Complainant has filed an abusive Complaint.

Once the Response is filed, and the URS Provider determines that the Response is compliant with the filing requirements of a Response (which shall be on the same day), the Complaint, Response and supporting materials will immediately be sent to a qualified Examiner, selected by the URS Provider, for review and Determination. All materials submitted are considered by the Examiner.

The Response can contain any facts refuting the claim of bad faith registration by setting out any of the following circumstances:

Before any notice to Registrant of the dispute, Registrant's use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

Registrant (as an individual, business or other organization) has been commonly known by the domain name, even if Registrant has acquired no trademark or service mark rights; or

Registrant is making a legitimate or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

Such claims, if found by the Examiner to be proved based on its evaluation of all evidence, shall result in a finding in favor of the Registrant.

The Registrant may also assert Defenses to the Complaint to demonstrate that the Registrant's use of the domain name is not in bad faith by showing, for example, one of the following:

The domain name is generic or descriptive and the registrant is making fair use of it.

The domain name sites are operated solely in tribute to or in criticism of a person or business that is found by the Examiner to be fair use.

Registrant's holding of the domain name is consistent with an express term of a written agreement entered into by the disputing Parties and that is still in effect.

The domain name is not part of a wider pattern or series of abusive registrations because the Domain Name is of a significantly different type or character to other domain names registered by the Registrant.

Other factors for the Examiner to consider:

Trading in domain names for profit, and holding a large portfolio of domain

names, are of themselves not indicia of bad faith under the URS. Such conduct, however, may be abusive in a given case depending on the circumstances of the dispute. The Examiner must review each case on its merits.

Sale of traffic (i.e. connecting domain names to parking pages and earning click-per-view revenue) does not in and of itself constitute bad faith under the URS. Such conduct, however, may be abusive in a given case depending on the circumstances of the dispute. The Examiner will take into account:

the nature of the domain name;

the nature of the advertising links on any parking page associated with the domain name; and

that the use of the domain name is ultimately the Registrant's responsibility.

6. Default

If at the expiration of the 14 Calendar Day Response period (or extended period if granted),

the

Registrant does not submit an answer, the Complaint proceeds to Default.

In either case, the Provider shall provide Notice of Default via email to the Complainant and Registrant, and via mail and fax to Registrant. During the Default period, the Registrant will be prohibited from changing content found on the site to argue that it is now a legitimate use and will also be prohibited from changing the Whois information.

All Default cases proceed to Examination for review on the merits of the claim.

If after Examination in Default cases, the Examiner rules in favor of Complainant, Registrant shall have the right to seek relief from Default via de novo review by filing a Response at any time up to six months after the date of the Notice of Default. The Registrant will also be entitled to request an extension of an additional six months if the extension is requested before the expiration of the initial six-month period.

If a Response is filed after: (i) the Respondent was in Default (so long as the Response is filed in accordance with 6.4 above); and (ii) proper notice is provided in accordance with the notice requirements set forth above, the domain name shall again resolve to the original IP address as soon as practical, but shall remain locked as if the Response had been filed in a timely manner before Default. The filing of a Response after Default is not an appeal; the case is considered as if responded to in a timely manner.

If after Examination in Default case, the Examiner rules in favor of Registrant, the Provider shall notify the Registry Operator to unlock the name and return full control of the domain name registration to the Registrant.

7. Examiners

7.1 One Examiner selected by the Provider will preside over a URS proceeding.

7.2 Examiners should have demonstrable relevant legal background, such as in trademark law, and shall be trained and certified in URS proceedings. Specifically, Examiners shall be provided with instructions on the URS elements and defenses and how to conduct the examination of a URS proceeding.

7.3 Examiners used by any given URS Provider shall be rotated to the extent feasible to avoid forum or examiner shopping. URS Providers are strongly encouraged to work equally with all certified Examiners, with reasonable exceptions (such as language needs, nonperformance, or malfeasance) to be determined on a case by case analysis.

8. Examination Standards and Burden of Proof

8.1 The standards that the qualified Examiner shall apply when rendering its Determination are whether:

8.1.2 The registered domain name is identical or confusingly similar to a word mark: (i) for which the Complainant holds a valid national or regional registration and that is in current use; or (ii) that has been validated through court proceedings; or (iii) that is specifically protected by a statute or treaty currently in effect and that was in effect at the time the URS Complaint is filed; and

8.1.2.1 Use can be shown by demonstrating that evidence of use - which can be a declaration and one specimen of current use - was submitted to, and validated by, the Trademark Clearinghouse.

8.1.2.2 Proof of use may also be submitted directly with the URS Complaint.

8.1.2 The Registrant has no legitimate right or interest to the domain name; and

8.1.3 The domain was registered and is being used in a bad faith.

The burden of proof shall be clear and convincing evidence. For a URS matter to conclude in favor of the Complainant, the Examiner shall render a Determination that there is no genuine issue of material fact. Such Determination may include that: (i) the Complainant has rights to the name; and (ii) the Registrant has no rights or legitimate interest in the name. This means that the Complainant must present adequate evidence to substantiate its trademark rights in the

domain name (e.g., evidence of a trademark registration and evidence that the domain name was registered and is being used in bad faith in violation of the URS).

If the Examiner finds that the Complainant has not met its burden, or that genuine issues of material fact remain in regards to any of the elements, the Examiner will reject the Complaint under the relief available under the URS. That is, the Complaint shall be dismissed if the Examiner finds that evidence was presented or is available to the Examiner to indicate that the use of the domain name in question is a non-infringing use or fair use of the trademark.

8.5 Where there is any genuine contestable issue as to whether a domain name registration and use of a trademark are in bad faith, the Complaint will be denied, the URS proceeding will be terminated without prejudice, e.g., a URS Appeal, UDRP, or a court proceeding may be utilized. The URS is not intended for use in any proceedings with open questions of fact, but only clear cases of trademark abuse.

8.6 To restate in another way, if the Examiner finds that all three standards are satisfied by clear and convincing evidence and that there is no genuine contestable issue, then the Examiner shall issue a Determination in favor of the Complainant. If the Examiner finds that any of the standards have not been satisfied, then the Examiner shall deny the relief requested, thereby terminating the URS proceeding without prejudice to the Complainant to proceed with an action in court of competent jurisdiction or under the UDRP.

9. Determination

There will be no discovery or hearing; the evidence will be the materials submitted with the Complaint and the Response, and those materials will serve as the entire record used by the Examiner to make a Determination.

If the Complainant satisfies the burden of proof, the Examiner will issue a Determination in favor of the Complainant. The Determination will be published on the URS Provider's website. However, there should be no other preclusive effect of the Determination other than the URS proceeding to which it is rendered.

If the Complainant does not satisfy the burden of proof, the URS proceeding is terminated and full control of the domain name registration shall be returned to the Registrant.

Determinations resulting from URS proceedings will be published by the URS Provider on the Provider's website in accordance with the Rules.

Determinations shall also be emailed by the URS Provider to the Registrant, the Complainant, the Registrar, and the Registry Operator, and shall specify the remedy and required actions of the Registry Operator to comply with the Determination.

To conduct URS proceedings on an expedited basis, examination should begin immediately upon the earlier of the expiration of a fourteen (14) day Response period (or extended period if granted), or upon the submission of the Response. A Determination shall be rendered on an expedited basis, with the stated goal that it be rendered within three (3) Business Days from when Examination began. Absent extraordinary circumstances, however, Determinations must be issued no later than five (5) days after the Response is filed.

10. Remedy

If the Determination is in favor of the Complainant, the decision shall be immediately transmitted to the Registry Operator, the Complainant, the Respondent and the Registrar. Immediately upon receipt of the Determination, the Registry Operator shall suspend the domain name, which shall remain suspended for the balance of the registration period and would not resolve to the original web site. The Registry Operator shall cause the nameservers to redirect to an informational web page provided by the URS Provider about the URS. The URS Provider shall not be allowed to offer any

other services on such page, nor shall it directly or indirectly use the web page for advertising purposes (either for itself or any other third party). The Whois for the domain name shall continue to display all of the information of the original Registrant except for the redirection of the nameservers. In addition, the Registry Operator shall cause the Whois to reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration.

There shall be an option for a successful Complainant to extend the registration period for one additional year at commercial rates.

No other remedies should be available in the event of a Determination in favor of the Complainant.

If the Examiner rules in favor of Respondent, the Provider shall notify the Registry Operator to unlock the name and return full control of the domain name registration to the Registrant.

11. Abusive Complaints

The URS shall incorporate penalties for abuse of the process by trademark holders.

A Complaint may be deemed abusive if the Examiner determines:

it was presented solely for improper purpose such as to harass, cause unnecessary delay, or needlessly increase the cost of doing business; and

(i) the claims or other assertions were not warranted by any existing law or the URS standards; or (ii) the factual contentions lacked any evidentiary support

An Examiner may find that Complaint contained a deliberate material falsehood if it contained an assertion of fact, which at the time it was made, was made with the knowledge that it was false and which, if true, would have an impact on the outcome on the URS proceeding.

In the event a party is deemed to have filed two (2) abusive Complaints, or one (1) "deliberate material falsehood," that party shall be barred from utilizing the URS for one-year following the date of issuance of a Determination finding a complainant to have: (i) filed its second abusive complaint; or (ii) filed a deliberate material falsehood.

Two findings of "deliberate material falsehood" shall permanently bar the Complainant from utilizing the URS.

URS Providers shall identify and track barred parties, and parties whom Examiners have determined submitted abusive complaints or deliberate material falsehoods.

The dismissal of a complaint for administrative reasons or a ruling on the merits, in itself, shall not be evidence of filing an abusive complaint.

A finding that filing of a complaint was abusive or contained a deliberate material falsehood can be appealed solely on the grounds that an Examiner abused his/her discretion, or acted in an arbitrary or capricious manner.

12. Appeal

Either party shall have a right to seek a de novo appeal of the Determination based on the existing record within the URS proceeding for a reasonable fee to cover the costs of the appeal. An appellant must identify the specific grounds on which the party is appealing, including why the appellant claims the Examiner's Determination was incorrect.

The fees for an appeal shall be borne by the appellant. A limited right to introduce new admissible evidence that is material to the Determination will be allowed upon payment of an additional fee, provided the evidence clearly pre-dates the filing of the Complaint. The Appeal Panel, to be selected by the Provider, may request, in its sole discretion, further statements or documents from either of the Parties.

Filing an appeal shall not change the domain name's resolution. For example, if the domain name no longer resolves to the original nameservers because of a Determination in favor of the Complainant, the domain name shall continue to point to the informational page provided by the URS Provider. If the domain name resolves to the original nameservers because of a Determination in favor of the registrant, it shall continue to resolve during the appeal process.

An Appeal must be filed within fourteen (14) days after a Default or Final Determination is issued and any Response must be filed fourteen (14) days after an appeal is filed.

Notice of Appeal and findings by the Appeals Panel shall be sent by the URS Provider electronically to the Registrant, the Complainant, the Registrar, and the Registry Operator.

The Providers' rules and procedures for appeals, other than those stated above, shall apply.

13. Other Available Remedies

The URS Determination shall not preclude any other remedies available to the appellant, such as UDRP (if appellant is the Complainant), or other remedies as may be available in a court of competent jurisdiction. A URS Determination for or against a party shall not prejudice the party in UDRP or any other proceedings.

14. Review of URS
A review of the URS procedure will be initiated one year after the first Examiner Determination is issued. Upon completion of the review, a report shall be published regarding the usage of the procedure, including statistical information, and posted for public comment on the usefulness and effectiveness of the procedure.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission, Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (2),

Whereas:

(1) The content of Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks (3) has been amended (4). In the interests of clarity and rationality the said Directive should be codified.

(2) The trade mark laws applicable in the Member States before the entry into force of Directive 89/104/EEC contained disparities which may have impeded the free movement of goods and freedom to provide services and may have

distorted competition within the common market. It was therefore necessary to approximate the laws of the Member States in order to ensure the proper functioning of the internal market.

(3) It is important not to disregard the solutions and advantages which the Community trade mark system may afford to undertakings wishing to acquire trade marks.

(4) It does not appear to be necessary to undertake full-scale approximation of the trade mark laws of the Member States. It will be sufficient if approximation is limited to those national provisions of law which most directly affect the functioning of the internal market.

(5) This Directive should not deprive the Member States of the right to continue to protect trade marks acquired through use but should take them into account only in regard to the relationship between them and trade marks acquired by registration.

(6) Member States should also remain free to fix the provisions of procedure concerning the registration, the revocation and the invalidity of trade marks acquired by registration. They can, for example, determine the form of trade mark registration and invalidity procedures, decide whether earlier rights should be invoked either in the registration procedure or in the invalidity procedure or in both and, if they allow earlier rights to be invoked in the registration procedure, have an opposition procedure or an ex officio examination procedure or both. Member States should remain free to determine the effects of revocation or invalidity of trade marks.

(7) This Directive should not exclude the application to trade marks of provisions of law of the Member States other than trade mark law, such as the provisions relating to unfair competition, civil liability or consumer protection.

(8) Attainment of the objectives at which this approximation of laws is aiming requires that the conditions for obtaining and continuing to hold a registered trade mark be, in general, identical in all Member States. To this end, it is necessary to list examples of signs which may constitute a trade mark, provided that such signs are capable of distinguishing the goods or services of one undertaking from those of other undertakings. The grounds for refusal or invalidity concerning the trade mark itself, for example, the absence of any distinctive character, or concerning conflicts between the trade mark and earlier rights, should be listed in an exhaustive manner, even if some of these grounds are listed as an option for the Member States which should therefore be able to maintain or introduce those grounds in their legislation. Member States should be able to maintain or introduce into their legislation grounds of refusal or invalidity linked to conditions for obtaining and continuing to hold a trade mark for which there is no provision of approximation, concerning, for example, the eligibility for the grant of a trade mark, the renewal of the trade mark or rules on fees, or related to the non-compliance with procedural rules.

(9) In order to reduce the total number of trade marks registered and protected in the Community and, consequently, the number of conflicts which arise between them, it is essential to require that registered trade marks must actually be used or, if not used, be subject to revocation. It is necessary to provide that a trade mark cannot be invalidated on the basis of the existence of a non-used earlier trade mark, while the Member States should remain free to apply the same principle in respect of the registration of a trade mark or to provide that a trade mark may not be successfully invoked in infringement proceedings if it is established as a result of a plea that the trade mark could be revoked. In all these cases it is up to the Member States to establish the applicable rules of procedure.

(10) It is fundamental, in order to facilitate the free movement of goods and services, to ensure that registered trade marks enjoy the same protection under the legal systems of all the Member States. This should not, however, prevent the Member States from granting at their option extensive protection to those trade marks which have a reputation.

(11) The protection afforded by the registered trade mark, the function of which is in particular to guarantee the trade mark as an indication of origin, should be absolute in the case of identity between the mark and the sign and the goods or services. The protection should apply also in the case of similarity between the mark and the sign and the goods or services. It is indispensable to give an interpretation of the concept of similarity in relation to the likelihood of confusion. The likelihood of confusion, the appreciation of which depends on numerous elements and, in particular, on the recognition of the trade mark on the market, the association which can be made with the used or registered sign, the degree of similarity between the trade mark and the sign and between the goods or services identified, should constitute the specific condition for such protection. The ways in which likelihood of confusion may be established, and in particular the onus of proof, should be a matter for national procedural rules which should not be prejudiced by this Directive.

(12) It is important, for reasons of legal certainty and without inequitably prejudicing the interests of a proprietor of an earlier trade mark, to provide that the latter may no longer request a declaration of invalidity nor may he oppose the use of a trade mark subsequent to his own of which he has knowingly tolerated the use for a substantial length of time, unless the application for the subsequent trade mark was made in bad faith.

(13) All Member States are bound by the Paris Convention for the Protection of Industrial Property. It is necessary that the provisions of this Directive should be entirely consistent with those of the said Convention. The obligations of the Member States resulting from that Convention should not be affected by this Directive. Where appropriate, the second paragraph of Article 307 of the Treaty should apply.

(14) This Directive should be without prejudice to the obligations of the Member States relating to the time limit for transposition into national law of Directive 89/104/EEC set out in Annex I, Part B,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope

This Directive shall apply to every trade mark in respect of goods or services which is the subject of registration or of an application in a Member State for registration as an individual trade mark, a collective mark or a guarantee or certification mark, or which is the subject of a registration or an application for registration in the Benelux Office for Intellectual Property or of an international registration having effect in a Member State.

Article 2

Signs of which a trade mark may consist

A trade mark may consist of any signs capable of being represented graphically, particularly words, including personal names, designs, letters, numerals, the shape of goods or of their packaging, provided that such signs are capable of distinguishing the goods or services of one undertaking from those of other undertakings.

Article 3

Grounds for refusal or invalidity

1. The following shall not be registered or, if registered, shall be liable to be declared invalid:

- (a) signs which cannot constitute a trade mark;
- (b) trade marks which are devoid of any distinctive character;
- (c) trade marks which consist exclusively of signs or indications which may serve, in trade, to designate the kind, quality, quantity, intended purpose, value, geographical origin, or the time of production of the goods or of rendering of the service, or other characteristics of the goods or services;
- (d) trade marks which consist exclusively of signs or indications which have become customary in the current

language or in the bona fide and established practices of the trade;

- (e) signs which consist exclusively of:
- (i) the shape which results from the nature of the goods themselves;
 - (ii) the shape of goods which is necessary to obtain a technical result;
 - (iii) the shape which gives substantial value to the goods;
- (f) trade marks which are contrary to public policy or to accepted principles of morality;
- (g) trade marks which are of such a nature as to deceive the public, for instance as to the nature, quality or geographical origin of the goods or service;
- (h) trade marks which have not been authorised by the competent authorities and are to be refused or invalidated pursuant to Article 6 ter of the Paris Convention for the Protection of Industrial Property, hereinafter referred to as the 'Paris Convention'.

2. Any Member State may provide that a trade mark shall not be registered or, if registered, shall be liable to be declared invalid where and to the extent that:

- (a) the use of that trade mark may be prohibited pursuant to provisions of law other than trade mark law of the Member State concerned or of the Community;
- (b) the trade mark covers a sign of high symbolic value, in particular a religious symbol;
- (c) the trade mark includes badges, emblems and escutcheons other than those covered by Article 6 ter of the Paris Convention and which are of public interest, unless the consent of the competent authority to their registration has been given in conformity with the legislation of the Member State;
- (d) the application for registration of the trade mark was made in bad faith by the applicant.

3. A trade mark shall not be refused registration or be declared invalid in accordance with paragraph 1(b), (c) or (d) if, before the date of application for registration and following the use which has been made of it, it has acquired a distinctive character. Any Member State may in addition provide that this provision shall also apply where the distinctive character was acquired after the date of application for registration or after the date of registration.

4. Any Member State may provide that, by derogation from paragraphs 1, 2 and 3, the grounds of refusal of registration or invalidity in force in that State prior to the date of entry into force of the provisions necessary to comply with Directive 89/104/EEC, shall apply to trade marks for which application has been made prior to that date.

Article 4

Further grounds for refusal or invalidity concerning conflicts with earlier rights

1. A trade mark shall not be registered or, if registered, shall be liable to be declared invalid:

- (a) if it is identical with an earlier trade mark, and the goods or services for which the trade mark is applied for or is registered are identical with the goods or services for which the earlier trade mark is protected;
- (b) if because of its identity with, or similarity to, the earlier trade mark and the identity or similarity of the goods or services covered by the trade marks, there exists a likelihood of confusion on the part of the public; the likelihood of confusion includes the likelihood of association with the earlier trade mark.

2. 'Earlier trade marks' within the meaning of paragraph 1 means:

- (a) trade marks of the following kinds with a date of application for registration which is earlier than the date of application for registration of the trade mark, taking account, where appropriate, of the priorities claimed in respect of those trade marks;
- (i) Community trade marks;

(ii) trade marks registered in the Member State or, in the case of Belgium, Luxembourg or the Netherlands, at the Benelux Office for Intellectual Property;

(iii) trade marks registered under international arrangements which have effect in the Member State;

(b) Community trade marks which validly claim seniority, in accordance with Council Regulation (EC) No 40/94 (5) of 20 December 1993 on the Community trade mark, from a trade mark referred to in (a)(ii) and (iii), even when the latter trade mark has been surrendered or allowed to lapse;

(c) applications for the trade marks referred to in points (a) and (b), subject to their registration;

(d) trade marks which, on the date of application for registration of the trade mark, or, where appropriate, of the priority claimed in respect of the application for registration of the trade mark, are well known in a Member State, in the sense in which the words 'well known' are used in Article 6 bis of the Paris Convention.

3. A trade mark shall furthermore not be registered or, if registered, shall be liable to be declared invalid if it is identical with, or similar to, an earlier Community trade mark within the meaning of paragraph 2 and is to be, or has been, registered for goods or services which are not similar to those for which the earlier Community trade mark is registered, where the earlier Community trade mark has a reputation in the Community and where the use of the later trade mark without due cause would take unfair advantage of, or be detrimental to, the distinctive character or the repute of the earlier Community trade mark.

4. Any Member State may, in addition, provide that a trade mark shall not be registered or, if registered, shall be liable to be declared invalid where, and to the extent that:

- (a) the trade mark is identical with, or similar to, an earlier national trade mark within the meaning of paragraph 2 and is to be, or has been, registered for goods or services which are not similar to those for which the earlier trade mark is registered, where the earlier trade mark has a reputation in the Member State concerned and where the use of the later trade mark without due cause would take unfair advantage of, or be detrimental to, the distinctive character or the repute of the earlier trade mark;

(b) rights to a non-registered trade mark or to another sign used in the course of trade were acquired prior to the date of application for registration of the subsequent trade mark, or the date of the priority claimed for the application for registration of the subsequent trade mark, and that non-registered trade mark or other sign confers on its proprietor the right to prohibit the use of a subsequent trade mark;

(c) the use of the trade mark may be prohibited by virtue of an earlier right other than the rights referred to in paragraph 2 and point (b) of this paragraph and in particular:

- (i) a right to a name;
- (ii) a right of personal portrayal;
- (iii) a copyright;

(iv) an industrial property right;

(d) the trade mark is identical with, or similar to, an earlier collective trade mark conferring a right which expired within a period of a maximum of three years preceding application;

(e) the trade mark is identical with, or similar to, an earlier guarantee or certification mark conferring a right which expired within a period preceding application the length of which is fixed by the Member State;

(f) the trade mark is identical with, or similar to, an earlier trade mark which was registered for identical or similar goods or services and conferred on them a right which has expired for failure to renew within a period of a maximum of two years preceding application, unless the proprietor of the earlier trade mark gave his agreement for the registration of the later mark or did not use his trade mark;

(g) the trade mark is liable to be confused with a mark which was in use abroad on the filing date of the application and which is still in use there, provided that at the date of the application the applicant was acting in bad faith.

5. The Member States may permit that in appropriate circumstances registration need not be refused or the trade mark need not be declared invalid where the proprietor of the earlier trade mark or other earlier right consents to the registration of the later trade mark.

6. Any Member State may provide that, by derogation from paragraphs 1 to 5, the grounds for refusal of registration or invalidity in force in that State prior to the date of the entry into force of the provisions necessary to comply with Directive 89/104/EEC, shall apply to trade marks for which application has been made prior to that date.

Article 5

Rights conferred by a trade mark

1. The registered trade mark shall confer on the proprietor exclusive rights therein. The proprietor shall be entitled to prevent all third parties not having his consent from using in the course of trade:

(a) any sign which is identical with the trade mark in relation to goods or services which are identical with those for which the trade mark is registered;

(b) any sign where, because of its identity with, or similarity to, the trade mark and the identity or similarity of the goods or services covered by the trade mark and the sign, there exists a likelihood of confusion on the part of the public; the likelihood of confusion includes the likelihood of association between the sign and the trade mark.

2. Any Member State may also provide that the proprietor shall be entitled to prevent all third parties not having his consent from using in the course of trade any sign which is identical with, or similar to, the trade mark in relation to goods or services which are not similar to those for which the trade mark is registered, where the latter has a reputation in the Member State and where use of that sign without due cause takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trade mark.

3. The following, *inter alia*, may be prohibited under paragraphs 1 and 2:

(a) affixing the sign to the goods or to the packaging thereof;

(b) offering the goods, or putting them on the market or stocking them for these purposes under that sign, or offering or supplying services thereunder;

(c) importing or exporting the goods under the sign;

(d) using the sign on business papers and in advertising.

4. Where, under the law of the Member State, the use of a sign under the conditions referred to in paragraph 1(b) or paragraph 2 could not be prohibited before the date of entry into force of the provisions necessary to comply with Directive 89/104/EEC in the Member State concerned, the rights conferred by the trade mark may not be relied on to prevent the continued use of the sign.

5. Paragraphs 1 to 4 shall not affect provisions in any Member State relating to the protection against the use of a sign other than for the purposes of distinguishing goods or services, where use of that sign without due cause takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trade mark.

Article 6

Limitation of the effects of a trade mark

1. The trade mark shall not entitle the proprietor to prohibit a third party from using, in the course of trade:

(a) his own name or address;

(b) indications concerning the kind, quality, quantity, intended purpose, value, geographical origin, the time of production of goods or of rendering of the service, or other characteristics of goods or services;

(c) the trade mark where it is necessary to indicate the intended purpose of a product or service, in particular as accessories or spare parts;

provided he uses them in accordance with honest practices in industrial or commercial matters.

2. The trade mark shall not entitle the proprietor to prohibit a third party from using, in the course of trade, an earlier right

which only applies in a particular locality if that right is recognised by the laws of the Member State in question and within the limits of the territory in which it is recognised.

Article 7

Exhaustion of the rights conferred by a trade mark

1. The trade mark shall not entitle the proprietor to prohibit its use in relation to goods which have been put on the market in the Community under that trade mark by the proprietor or with his consent.

2. Paragraph 1 shall not apply where there exist legitimate reasons for the proprietor to oppose further commercialisation of the goods, especially where the condition of the goods is changed or impaired after they have been put on the market.

Article 8

Licensing

1. A trade mark may be licensed for some or all of the goods or services for which it is registered and for the whole or part of the Member State concerned. A licence may be exclusive or non-exclusive.

2. The proprietor of a trade mark may invoke the rights conferred by that trade mark against a licensee who contravenes any provision in his licensing contract with regard to:

(a) its duration;

(b) the form covered by the registration in which the trade mark may be used;

(c) the scope of the goods or services for which the licence is granted;

(d) the territory in which the trade mark may be affixed; or

(e) the quality of the goods manufactured or of the services provided by the licensee.

Article 9

Limitation in consequence of acquiescence

1. Where, in a Member State, the proprietor of an earlier trade mark as referred to in Article 4(2) has acquiesced, for a period of five successive years, in the use of a later trade mark registered in that Member State while being aware of such use, he shall no longer be entitled on the basis of the earlier trade mark either to apply for a declaration that the later trade mark is invalid or to oppose the use of the later trade mark in respect of the goods or services for which the later trade mark has been used, unless registration of the later trade mark was applied for in bad faith.

2. Any Member State may provide that paragraph 1 shall apply *mutatis mutandis* to the proprietor of an earlier trade mark referred to in Article 4(4)(a) or an other earlier right referred to in Article 4(4)(b) or (c).

3. In the cases referred to in paragraphs 1 and 2, the proprietor of a later registered trade mark shall not be entitled to oppose the use of the earlier right, even though that right may no longer be invoked against the later trade mark.

Article 10

Use of trade marks

1. If, within a period of five years following the date of the completion of the registration procedure, the proprietor has not put the trade mark to genuine use in the Member State in connection with the goods or services in respect of which it is registered, or if such use has been suspended during an uninterrupted period of five years, the trade mark shall be subject to the sanctions provided for in this Directive, unless there are proper reasons for non-use.

The following shall also constitute use within the meaning of the first subparagraph:

(a) use of the trade mark in a form differing in elements which do not alter the distinctive character of the mark in the form in which it was registered;

(b) affixing of the trade mark to goods or to the packaging thereof in the Member State concerned solely for export purposes.

2. Use of the trade mark with the consent of the proprietor or by any person who has authority to use a collective mark or a guarantee or certification mark shall be deemed to constitute use by the proprietor.

3. In relation to trade marks registered before the date of entry into force in the Member State concerned of the provisions necessary to comply with Directive 89/104/EEC:

(a) where a provision in force prior to that date attached sanctions to non-use of a trade mark during an uninterrupted period, the relevant period of five years mentioned in the first subparagraph of paragraph 1 shall be deemed to have begun to run at the same time as any period of non-use which is already running at that date;

(b) where there was no use provision in force prior to that date, the periods of five years mentioned in the first subparagraph of paragraph 1 shall be deemed to run from that date at the earliest.

Article 11

Sanctions for non-use of a trade mark in legal or administrative proceedings

1. A trade mark may not be declared invalid on the ground that there is an earlier conflicting trade mark if the latter does not fulfil the requirements of use set out in Article 10(1) and (2), or in Article 10(3), as the case may be.

2. Any Member State may provide that registration of a trade mark may not be refused on the ground that there is an earlier conflicting trade mark if the latter does not fulfil the requirements of use set out in Article 10(1) and (2) or in Article 10(3), as the case may be.

3. Without prejudice to the application of Article 12, where a counter-claim for revocation is made, any Member State may provide that a trade mark may not be successfully invoked in infringement proceedings if it is established as a result of a plea that the trade mark could be revoked pursuant to Article 12(1).

4. If the earlier trade mark has been used in relation to part only of the goods or services for which it is registered, it shall, for purposes of applying paragraphs 1, 2 and 3, be deemed to be registered in respect only of that part of the goods or services.

Article 12

Grounds for revocation

1. A trade mark shall be liable to revocation if, within a continuous period of five years, it has not been put to genuine use in the Member State in connection with the goods or services in respect of which it is registered, and there are no proper reasons for non-use.

However, no person may claim that the proprietor's rights in a trade mark should be revoked where, during the interval between expiry of the five-year period and filing of the application for revocation, genuine use of the trade mark has been started or resumed.

The commencement or resumption of use within a period of three months preceding the filing of the application for revocation which began at the earliest on expiry of the continuous period of five years of non-use shall be disregarded where preparations for the commencement or resumption occur only after the proprietor becomes aware that the application for revocation may be filed.

2. Without prejudice to paragraph 1, a trade mark shall be liable to revocation if, after the date on which it was registered:

(a) in consequence of acts or inactivity of the proprietor, it has become the common name in the trade for a product or service in respect of which it is registered;

(b) in consequence of the use made of it by the proprietor of the trade mark or with his consent in respect of the goods or services for which it is registered, it is liable to mislead the public, particularly as to the nature, quality or geographical origin of those goods or services.

Article 13

Grounds for refusal or revocation or invalidity relating to only some of the goods or services

Where grounds for refusal of registration or for revocation or invalidity of a trade mark exist in respect of only some of the goods or services for which that trade mark has been applied for or registered, refusal of registration or revocation or invalidity shall cover those goods or services only.

Article 14

Establishment a posteriori of invalidity or revocation of a trade mark

Where the seniority of an earlier trade mark which has been surrendered or allowed to lapse is claimed for a Community trade mark, the invalidity or revocation of the earlier trade mark may be established a posteriori.

Article 15

Special provisions in respect of collective marks, guarantee marks and certification marks

1. Without prejudice to Article 4, Member States whose laws authorise the registration of collective marks or of guarantee or certification marks may provide that such marks shall not be registered, or shall be revoked or declared invalid, on grounds additional to those specified in Articles 3 and 12 where the function of those marks so requires.

2. By way of derogation from Article 3(1)(c), Member States may provide that signs or indications which may serve, in trade, to designate the geographical origin of the goods or services may constitute collective, guarantee or certification marks. Such a mark does not entitle the proprietor to prohibit a third party from using in the course of trade such signs or indications, provided he uses them in accordance with honest practices in industrial or commercial matters; in particular, such a mark may not be invoked against a third party who is entitled to use a geographical name.

Article 16

Communication

Member States shall communicate to the Commission the text of the main provisions of national law adopted in the field governed by this Directive.

Article 17

Repeal

Directive 89/104/EEC, as amended by the Decision listed in Annex I, Part A, is repealed, without prejudice to the obligations of the Member States relating to the time limit for transposition into national law of that Directive, set out in Annex I, Part B.

References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table in Annex II.

Article 18

Entry into force

This Directive shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

Article 19

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 22 October 2008.

For the European Parliament

The President

H.-G. PÖTTERING

For the Council

The President

J.-P. JOUYET

(1) OJ C 161, 13.7.2007, p. 44.

(2) Opinion of the European Parliament of 19 June 2007 (OJ C 146 E, 12.6.2008, p. 76) and Council Decision of 25 September 2008.

(3) OJ L 40, 11.2.1989, p. 1.

(4) See Annex I, Part A.

(5) OJ L 11, 14.1.1994, p. 1.

Regulation (EC) No 733/2002 of the European Parliament and of the council of 22 April 2002 on the implementation of the .eu Top Level Domain

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 156 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Following consultation of the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

(1)

The creation of the .eu Top Level Domain (TLD) is included as one of the targets to accelerate electronic commerce in the e-Europe initiative as endorsed by the European Council at its meeting in Lisbon on 23 and 24 March 2000.

(2)

The communication from the Commission to the Council and the European Parliament on the organisation and management of the Internet refers to the creation of the .eu TLD and the Council resolution of 3 October 2000 on the organisation and management of the Internet (4) charges the Commission to encourage the coordination of policies in relation to the management of the Internet.

(3)

TLDs are an integral part of the Internet infrastructure. They are an essential element of the global interoperability of the World Wide Web ('WWW' or 'the Web'). The connection and presence permitted by the allocation of domain names and the related addresses allow users to locate computers and websites on the Web. TLDs are also an integral part of every Internet e-mail address.

(4)

The .eu TLD should promote the use of, and access to, the Internet networks and the virtual market place based on the Internet, in accordance with Article 154(2) of the Treaty, by providing a complementary registration domain to existing country code Top Level Domains (ccTLDs) or global registration in the generic Top Level Domains, and should in consequence increase choice and competition.

(5)

The .eu TLD should improve the interoperability of trans-European networks, in accordance with Articles 154 and 155 of the Treaty, by ensuring the availability of .eu name servers in the Community. This will affect the topology and technical infrastructure of the Internet in Europe which will benefit from an additional set of name servers in the Community.

(6)

Through the .eu TLD, the Internal market should acquire higher visibility in the virtual market place based on the Internet. The .eu TLD should provide a clearly identified link with the Community, the associated legal framework, and the European market place. It should enable undertakings, organisations and natural persons within the Community to register in a specific domain which will make this link obvious. As such, the .eu TLD will not only be a key building block for electronic commerce in Europe but will also support the objectives of Article 14 of the Treaty.

(7)

The .eu TLD can accelerate the benefits of the information society in Europe as a whole, play a role in the integration of future Member States into the European Union, and help combat the risk of digital divide with neighbouring countries. It is therefore to be expected that this Regulation will be extended to the European Economic Area and that amendments may be sought to the existing arrangements between the European Union and European third countries, with a view to accommodating the requirements of the .eu TLD so that entities in those countries may participate in it.

(8)

This Regulation is without prejudice to Community law in the field of personal data protection. This Regulation should be implemented in compliance with the principles relating to privacy and the protection of personal data.

(9)

Internet management has generally been based on the principles of non-interference, self-management and self-Regulation. To the extent possible and without prejudice to Community law, these principles should also apply to the .eu ccTLD. The implementation of the .eu TLD may take into consideration best practices in this regard and could be supported by voluntary guidelines or codes of conduct where appropriate.

(10)

The establishment of the .eu TLD should contribute to the promotion of the European Union image on the global information networks and bring an added value to the Internet naming system in addition to the national ccTLDs.

(11)

The objective of this Regulation is to establish the conditions of implementation of the .eu TLD, to provide for the designation of a Registry and establish the general policy framework within which the Registry will function. National ccTLDs are not covered by this Regulation.

(12)

The Registry is the entity charged with the organisation, administration and management of the .eu TLD, including maintenance of the corresponding databases and the associated public query services, the accreditation of Registrars, the registration of domain names applied for by accredited Registrars, the operation of the TLD name servers and the dissemination of TLD zone files. Public query services associated with the TLD are referred to as 'Who is' queries. 'Who is'-type databases should be in conformity with Community law on data protection and privacy. Access to these databases provides information on a domain name holder and is an essential tool in boosting user confidence.

(13)

After publishing a call for expressions of interest in the Official Journal of the European Communities, the Commission should, on the basis of an open, transparent and non-discriminatory selection procedure, designate a Registry. The Commission should enter into a contract with the selected Registry which should specify the conditions applying to the Registry for the organisation, administration and management of the .eu TLD and which should be limited in time and renewable.

(14)

The Commission, acting on behalf of the Community, has requested the delegation of the EU code for the purpose of creating an Internet ccTLD. On 25 September 2000, the Internet Corporation for Assigned Names and Numbers (ICANN) issued a resolution providing that 'alpha-2 codes are delegable as ccTLDs only in cases where the ISO 3166 Maintenance Agency, on its exceptional reservation list, has issued a reservation of

the code that covers any application of ISO 3166-1 that needs a coded representation in the name of the country, territory or area involved'. Such conditions are met by the EU code which is therefore 'delegable' to the Community.

(15)

ICANN is at present responsible for coordinating the delegation of codes representing ccTLD to Registries. The Council resolution of 3 October 2000 encourages the implementation of the principles applied to ccTLD Registries adopted by the Governmental Advisory Committee (GAC). The Registry should enter into a contract with ICANN respecting the GAC principles.

(16)

The adoption of a public policy addressing speculative and abusive registration of domain names should provide that holders of prior rights recognised or established by national and/or Community law and public bodies will benefit from a specific period of time (a 'sunrise period') during which the registration of their domain names is exclusively reserved to such holders of prior rights recognised or established by national and/or Community law and public bodies.

(17)

Domain names should not be revoked arbitrarily. A revocation may, however, be obtained in particular should a domain name be manifestly contrary to public order. The revocation policy should nevertheless provide for a timely and efficient mechanism.

(18)

Rules should be adopted on the question of bona vacantia to address the status of domain names the registration of which is not renewed or which, for example because of succession law, are left without holder.

(19)

The new .eu TLD registry should not be empowered to create second-level domains using alpha-2 codes representing countries.

(20)

Within the framework established by this Regulation, the public policy rules concerning the implementation and functions of the .eu TLD and the public policy principles on registration, various options including the 'first come, first served' method should be considered when registration policy is formulated.

(21)

When reference is made to interested parties, provision should be made for consultation encompassing, in particular, public authorities, undertakings, organisations and natural persons. The Registry could establish an advisory body to organise such consultation.

(22)

The measures necessary for the implementation of this Regulation, including criteria for the selection procedure of the Registry, the designation of the Registry, as well as the adoption of public policy rules, should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (5).

(23)

Since the objective of the proposed action, namely to implement the .eu TLD, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective,

HAVE ADOPTED THIS REGULATION:

Article 1

Objective and scope

1. The objective of this Regulation is to implement the .eu country code Top Level Domain (ccTLD) within the

Community. The Regulation sets out the conditions for such implementation, including the designation of a Registry, and establishes the general policy framework within which the Registry will function.

2. This Regulation shall apply without prejudice to arrangements in Member States regarding national ccTLDs.

Article 2

Definitions

For the purposes of this Regulation:

(a) 'Registry' means the entity entrusted with the organisation, administration and management of the .eu TLD including maintenance of the corresponding databases and the associated public query services, registration of domain names, operation of the Registry of domain names, operation of the Registry TLD name servers and dissemination of TLD zone files;

(b) 'Registrar' means a person or entity that, via contract with the Registry, provides domain name registration services to registrants.

Article 3

Characteristics of the Registry

1. The Commission shall:

▼M1

(a) establish the criteria and the procedure for the designation of the Registry. That measure, designed to amend non-essential elements of this Regulation by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 6(3). On imperative grounds of urgency, the Commission may have recourse to the urgency procedure referred to in Article 6(4);

▼B

(b) designate, in accordance with the procedure referred to in Article 6(2), the Registry after publishing a call for expressions of interest in the Official Journal of the European Communities and after the procedure for such call has been completed;

(c) enter into, in accordance with the procedure referred to in Article 6(2), a contract which shall specify the conditions according to which the Commission supervises the organisation, administration and management of the .eu TLD by the Registry. The contract between the Commission and the Registry shall be limited in time and renewable.

The Registry may not accept registrations until the registration policy is in place.

2. The Registry shall be a non-profit organisation, formed in accordance with the law of a Member State and having its registered office, central administration and principal place of business within the Community.

3. Having obtained the prior consent of the Commission, the Registry shall enter into the appropriate contract providing for the delegation of the .eu ccTLD code. To this effect the relevant principles adopted by the Governmental Advisory Committee shall be taken into account.

4. The .eu TLD Registry shall not act itself as Registrar.

Article 4

Obligations of the Registry

1. The Registry shall observe the rules, policies and procedures laid down in this Regulation and the contracts referred to in Article 3. The Registry shall observe transparent and non-discriminatory procedures.

2. The Registry shall:

(a) organise, administer and manage the .eu TLD in the general interest and on the basis of principles of quality, efficiency, reliability and accessibility;

(b) register domain names in the .eu TLD through any accredited .eu Registrar requested by any:

(i) undertaking having its registered office, central administration or principal place of business within the Community, or

- (ii) organisation established within the Community without prejudice to the application of national law, or
- (iii) natural person resident within the Community;
- (c) impose fees directly related to costs incurred;
- (d) implement the extra-judicial settlement of conflicts policy based on recovery of costs and a procedure to resolve promptly disputes between domain name holders regarding rights relating to names including intellectual property rights as well as disputes in relation to individual decisions by the Registry. This policy shall be adopted in accordance with Article 5(1) and take into consideration the recommendations of the World Intellectual Property Organisation. The policy shall provide adequate procedural guaranties for the parties concerned, and shall apply without prejudice to any court proceeding;
- (e) adopt procedures for, and carry out, accreditation of .eu Registrars and ensure effective and fair conditions of competition among .eu Registrars;
- (f) ensure the integrity of the databases of domain names.

Article 5

Policy framework

▼M1

1. After consulting the Registry, the Commission shall adopt public policy rules concerning the implementation and function of the .eu TLD and public policy principles on registration. Those measures, designed to amend non-essential elements of this Regulation by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 6(3).

1. Public policy shall include:

1.

- (a) an extra-judicial settlement of conflicts policy;
- (b) public policy on speculative and abusive registration of domain names, including the possibility of registration of domain names in a phased manner to ensure appropriate temporary opportunities for the holders of prior rights recognised or established by national and/or Community law and public bodies to register their names;
- (c) policy on possible revocation of domain names, including the question of bona vacantia;
- (d) issues of language and geographical concepts;
- (e) treatment of intellectual property and other rights.

▼B

2. Within three months of the entry into force of this Regulation, Member States may notify to the Commission and to the other Member States a limited list of broadly-recognised names which affect their political or territorial organisation that may either:

- (a) not be registered, or
- (b) be registered only under a second level domain according to the public policy rules.

The Commission shall notify to the Registry without delay the list of notified names to which such criteria apply. The Commission shall publish the list at the same time as it notifies the Registry.

Where a Member State or the Commission within 30 days of publication raises an objection to an item included in a notified list, the Commission shall take measures, in accordance with the procedure referred to in Article 6(3), to remedy the situation.

3. Before starting registration operations, the Registry shall adopt the initial registration policy for the .eu TLD in (6) OJ L 108, 24.4.2002, p. 33.

Amended by:

consultation with the Commission and other interested parties. The Registry shall implement in the registration policy the public policy rules adopted pursuant to paragraph 1 taking into account the exception lists referred to in paragraph 2.

4. The Commission shall periodically inform the Committee referred to in Article 6 on the activities referred to in paragraph 3 of this Article.

▼M1

Article 6

Committee procedure

1. The Commission shall be assisted by the Communications Committee established by Article 22(1) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (6)

2. Where reference is made to this paragraph, Articles 3 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

4. Where reference is made to this paragraph, Article 5a(1), (2), (4) and (6) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

▼B

Article 7

Reservation of rights

The Community shall retain all rights relating to the .eu TLD including, in particular, intellectual property rights and other rights to the Registry databases required to ensure the implementation of this Regulation and the right to re-designate the Registry.

Article 8

Implementation report

The Commission shall submit a report to the European Parliament and the Council on the implementation, effectiveness and functioning of the .eu TLD one year after the adoption of this Regulation and thereafter every two years.

Article 9

Entry into force

This Regulation shall enter into force on the day of its publication in the Official Journal of the European Communities.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

(1) OJ C 96 E, 27.3.2001, p. 333.

(2) OJ C 155, 29.5.2001, p. 10.

(3) Opinion of the European Parliament of 4 July 2001 (OJ C 65 E, 14.3.2002, p. 147), Council Common Position of 6 November 2001 (OJ C 45 E, 19.2.2002, p. 53) and Decision of the European Parliament of 28 February 2002 (not yet published in the Official Journal). Council Decision of 25 March 2002.

(4) OJ C 293, 14.10.2000, p. 3.

(5) OJ L 184, 17.7.1999, p. 23.

Relevant case law on Regulation no. 733/2002 - on the implementation of the .eu Top Level Domain

C-483/07 P - Galileo Lebensmittel v Commission

(Appeal - Action for annulment - Reservation by the Commission of the domain 'galileo.eu' - Fourth paragraph of Article 230 EC - Decision of individual concern to a natural or legal person - Appeal clearly unfounded)

In C-483/07 P,

APPEAL under Article 56 of the Statute of the Court of Justice, brought on 5 November 2007,

Galileo Lebensmittel GmbH & Co. KG, established in Trierweiler (Germany), represented by K. Bott, Rechtsanwalt, appellant,

the other party to the proceedings being:

Commission of the European Communities, represented by G. Braun and E. Montaguti, acting as Agents, with an address for service in Luxembourg,

defendant at first instance,

THE COURT (Sixth Chamber),

composed of J.-C. Bonichot (Rapporteur), President of the Chamber, P. Kūris and L. Bay Larsen, Judges,

Advocate General: D. Ruiz-Jarabo Colomer,

Registrar: R. Grass,

after hearing the Advocate General,

makes the following

Order

1 By its appeal, Galileo Lebensmittel GmbH & Co. KG ('Galileo Lebensmittel' or 'the appellant') seeks the setting aside of the order of 28 August 2007 in Case T-46/06 Galileo Lebensmittel v Commission ('the order under appeal'), by which the Court of First Instance dismissed as inadmissible the action for annulment of the Commission's decision to reserve - pursuant to Article 9 of Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (OJ 2004 L 162, p. 40) - the internet domain name 'galileo.eu' as a .eu Top Level Domain ('TLD') for use by the Community institutions and bodies ('the contested decision').

Legal context

...

2. Facts

11 The background to the dispute was set out as follows in paragraphs 11 to 16 of the order under appeal:

'International system of internet domains

11 The internet Domain Name System (DNS) consists of a registry with a hierarchical structure which [contains] the names of all domains and the computers connected with them which are registered for certain undertakings and persons using the internet. The domain name is an electronic text which brings the internet user to a given page. The [TLD] is the part of the domain name on the right, after the last dot in the name. It designates the highest level of the geographical and organisational structure of the internet domain name system used for addresses. On the internet, the TLD is either the ISO two-letter country code or an abbreviation in English, for example, '.com', '.net' or '.org'. The allocation of codes for the various TLD names (for example, the ISO country code '.lu' for Luxembourg) is coordinated by the body responsible for the allocation of internet names and addresses, the Internet Corporation for Assigned Names and Numbers (ICANN), a

non-profit corporation incorporated under US law.

12 On the basis of that system, the ICANN Board of Directors authorised the allocation of the new ".eu" TLD on 21 May 2005 and authorised the President of ICANN to conclude an agreement with the European Registry for Internet Domains (EURid). EURid is a non-profit association incorporated under Belgian law which was designated by the Commission to manage the ".eu" TLD (see Commission Decision 2002/375/EC of 21 May 2003 on the designation of the .eu Top Level Domain Registry (OJ 2003 L 128, p. 29)).

Background to the dispute

13 Galileo Lebensmittel holds a licence, dated 13 February 2006, for the exclusive use of various trade marks registered on behalf of IFD Italian Food Distribution SA, established at Mertert (Luxembourg), including the word mark Galileo, registered with the German Patent and Trade Mark Office under number 2071982. IFD Italian Food Distribution, the holding company which owns Galileo Lebensmittel, does not engage in any business activities.

14 On 1 December 2005, Galileo Lebensmittel applied to EURid on the basis of Article 10(1) of Regulation No 874/2004 and through a German undertaking, 1&1 Internet AG, for registration of the domain name "galileo.eu". On 7 December 2005, the 1&1 internet registration bureau lodged the application for registration with EURid electronically.

15 The applicant also applied for registration of the domain name "galileo-food.eu". EURid acknowledged receipt of that application, but not of the application relating to the domain name "galileo.eu".

16 EURid did not grant the application, nor did it acknowledge receipt thereof, because the domain name "galileo.eu" had been reserved for the Commission since 7 November 2005. EURid informed the applicant accordingly on 2 February 2006. In its message, EURid states that it had duly reserved that domain name on the basis of Article 9 of Regulation No 874/2004. That reservation had not been decided on by EURid but by the Commission. Given that the latter had reserved the domain name "galileo.eu", note was no longer taken of the order in which applications for registration of that domain name were received.'

The action before the Court of First Instance and the order under appeal

12 On 13 February 2006, Galileo Lebensmittel brought an action before the Court of First Instance for annulment of the Commission's decision to reserve the domain name 'galileo.eu' for use by the Community institutions and bodies.

13 By the order under appeal, the Court of First Instance dismissed the action as inadmissible on the ground that the decision, which was not addressed to Galileo Lebensmittel, was also not 'of individual concern' to it, within the meaning of the fourth paragraph of Article 230 EC.

14 The Court of First Instance referred to the case-law according to which the fact that it is possible to determine more or less precisely the number, or even the identity, of the persons to whom a measure applies does not mean that that measure must be regarded as being of individual concern to those persons so long as it is established that the measure applies to them by virtue of an objective legal or factual situation defined therein.

15 The Court of First Instance went on to point out that, in

order for the contested measure to be of individual concern to Galileo Lebensmittel, that company had to be a member of a limited class of traders and it had to be entitled to particular protection. The Court of First Instance ruled that neither of those conditions was satisfied in the case before it.

16 With regard to the matter of particular protection, the Court of First Instance held that there was no provision under which the Commission was required to take account of Galileo Lebensmittel's interests.

17 With regard to the question whether Galileo Lebensmittel was a member of a limited class of traders by reason of characteristics specific to the members of that class, the Court of First Instance held that, at the time when the list was drawn up, the number and identity of the persons likely to be concerned by the reservation was neither definitively known nor even determinable.

18 Each domain name on the list is reserved not just vis-à-vis holders of prior rights, such as the applicant claims to be, and public bodies, which is a very large group but which it is possible to identify, but also vis-à-vis the general public. Even supposing that no application is introduced during the period scheduled for early and privileged registration, it is always possible that such an application may be introduced during the period scheduled for general registration.

19 The Court of First Instance stated in that regard that the date to be taken into consideration for the purposes of determining whether there was a limited class of traders concerned was the date on which the contested measure was adopted.

Forms of order sought

20 In its appeal, Galileo Lebensmittel claims that the Court should:

- set aside the order under appeal and annul the contested decision;
- order the Commission to pay the costs of both sets of proceedings;
- in the alternative, set aside the order under appeal, refer the case back to the Court of First Instance and order the Commission to pay the costs of the appeal proceedings.

.....

Findings of the Court

28 The fourth paragraph of Article 230 EC makes it possible for any natural or legal person to bring an action for annulment in the case of two types of decision: (i) decisions addressed to that person and (ii) decisions which, albeit in the form of a Regulation or of a decision addressed to another, are of direct and individual concern to that person.

29 The essential distinguishing factor lies in whether or not the applicant for annulment is the addressee of the decision being challenged. If that is not so, the applicant must, in order to be able to bring an action for annulment, be directly and individually concerned by that decision. The case-law on that concept of individual concern applies, therefore, where the decision being challenged is not addressed to the applicant.

30 Consequently, and without there being any need to determine the exact nature of the contested decision, it is sufficient to note that it was not addressed to Galileo Lebensmittel. The Court of First Instance was fully entitled, therefore, in the case before it, to apply the case-law on the concept of individual concern for the purposes of determining whether Galileo Lebensmittel had locus standi.

31 The first plea in law must therefore be rejected as clearly unfounded.

The second plea, alleging that the order under appeal does not take account of the fact that the word mark which the appellant claims to own is entitled to particular protection

Arguments of the parties

.....

Findings of the Court

41 Natural or legal persons can claim to be concerned individually only if the contested provision affects them by reason of certain attributes which are peculiar to them or by reason of circumstances in which they are differentiated from any other person and by virtue of those factors distinguishes

them individually just as in the case of the addressee of a decision (Case 25/62 Plaumann v Commission [1963] ECR 95, at p. 107).

42 As was pointed out in the order under appeal, the Court has held in that regard that, where a contested measure affects a group of persons who were identified or identifiable at the time when that measure was adopted, by reason of criteria specific to the members of the group, those persons may be individually concerned by that measure inasmuch as they form part of a limited class of traders (Piraiki-Patraiki and Others v Commission, paragraph 31, and Joined Cases C-182/03 and C-217/03 Belgium and Forum 187 v Commission [2006] ECR I-5479, paragraph 60).

43 On that point, the Court of First Instance was fully entitled to hold that the number and the identity of the persons potentially concerned by the reservation of the domain name was neither definitively known nor even determinable. The Court of First Instance proceeded on the basis of a correct analysis of the procedure provided for in Regulation No 874/2004 when it pointed out that each domain name on the list is reserved not merely vis-à-vis holders of prior rights but also vis-à-vis the general public.

44 In that regard, the appellant cannot compare its situation with the circumstances under consideration in Piraiki-Patraiki and Others v Commission. In that judgment, the Court accepted as admissible an action for the annulment of a Commission decision – authorising a Member State to introduce protective measures with regard to imports of a product – brought by applicants who, before the adoption of that decision, had entered into contracts for the sale of the product concerned, performance of which could not be carried out, in whole or in part, because of that decision. In the present case, the contested decision in no way impedes the performance of contracts to which the appellant is a party. Accordingly, the situation on which it relies cannot give rise to the application of the case-law developed in Piraiki-Patraiki and Others v Commission.

45 Nor can the appellant rely on the fact that, in Codorniu v Council, the Court recognised, in favour of the company concerned in that case, the existence of a situation which differentiated that company from all other traders with regard to a legislative provision of general scope, inasmuch as that provision ultimately prevented the company from using its figurative mark in commerce. It is sufficient to point out in that regard that the contested decision does not prevent the appellant from using its trade mark, which means that its situation cannot be compared with that under consideration in Codorniu v Council.

46 Similarly, although it is possible under the case-law for a person to be regarded as individually concerned by a measure because that person forms part of a limited class of traders, where the measure alters rights which the person had acquired prior to its adoption (see Joined Cases 106/63 and 107/63 Toepfer and Getreide-Import Gesellschaft v Commission [1965] ECR 405, at 411, and Commission v Infront, paragraph 72), the contested decision does not, in the present case, alter any acquired right to the disadvantage of the appellant, since the only right on which the appellant relies relates to the Galileo trade mark, which is governed by different rules.

47 Lastly, although the appellant claims, essentially, that the contested decision seriously impairs its economic interests, that fact alone is not sufficient to make the appellant 'individually concerned' within the meaning of Plaumann v Commission, and as a consequence to call into question the analysis made by the Court of First Instance, which merely applied that case-law.

48 In those circumstances, there is no basis for the appellant's claim that the Court of First Instance erred in considering that it did not form part of a 'limited class of traders' within the meaning of the case-law referred to above.

49 The first branch of the second plea in law must therefore be rejected as clearly unfounded.

50 Similarly, the Court of First Instance was fully entitled to

assess the question whether the persons concerned by the contested decision were identified or identifiable by reference to the date on which that decision was adopted (see, by analogy, Case 97/85 Union Deutsche Lebensmittelwerke and Others v Commission [1987] ECR 2265, paragraph 11).

51 The second branch of the second plea in law is therefore clearly unfounded.

52 Lastly, the appellant cannot claim that, in the order under appeal, the Court of First Instance failed to have due regard for the right to particular protection which the appellant claims to enjoy on the basis of the procedure under which the contested decision was adopted.

53 The Court has held that the fact that a person participates in the process by which a Community measure is adopted does not distinguish that person individually with regard to the measure in question unless provision has been made under the Community rules for procedural guarantees in favour of that person. Thus, where a provision of Community law requires that, for the purposes of adopting a decision, a procedure must be followed in respect of which a natural or legal person may assert rights, such as the right to be heard, the special legal position which that person enjoys has the effect of distinguishing him individually for the purposes of Article 230 EC (see, by analogy, Case 191/82 Fediol v Commission [1983] ECR 2913, paragraph 31, and C-263/02 P Commission v Jégo-Quéré [2004] ECR I-3425, paragraphs 47 and 48).

54 In the present case, although Regulation No 874/2004 admittedly sets aside in favour of holders of prior rights, such as the appellant claims to be, a period for the early and privileged registration of domain names, it provides no procedural guarantee which could be construed as a right in favour of Galileo Lebensmittel. Consequently, the appellant cannot rely on the provisions of Regulation No 874/2004 in order to argue that they 'distinguish' it for the purposes of the fourth paragraph of Article 230 EC.

55 The third branch of the second plea in law must therefore be rejected as clearly unfounded.

56 It follows from the foregoing that, independently of the question whether the appellant was indeed the holder of a prior right at the time of applying for the 'galileo.eu' domain name, there is in any event no basis for the appellant's claim that that name is entitled to particular protection, in order to argue that the Court of First Instance erred in holding that the contested decision was not of individual concern to it.

57 The three branches of the second plea in law must therefore be rejected as clearly unfounded.

The third plea, alleging a right to effective judicial protection
.....

Findings of the Court

59 The conditions for the admissibility of an action for annulment cannot be set aside on the basis of the applicant's interpretation of the right to effective judicial protection (see, to that effect, C-50/00 P Unión de Pequeños Agricultores v Council [2002] ECR I-6677, paragraph 44; Commission v Jégo-Quéré, paragraph 36; the order of 8 March 2007 in C-237/06 P Strack v Commission, paragraph 108; and the order of 13 March 2007 in C-150/06 P Arizona Chemical and Others v Commission, paragraph 40).

60 Accordingly, an individual to whom a Commission decision is not of direct and individual concern and whose interests are therefore unaffected by that measure cannot invoke the right to judicial protection in relation to that decision (see, to that effect, the order of 1 October 2004 in C-379/03 P Pérez Escobar v Commission, paragraph 41).

61 Since the appellant has failed to establish that the contested decision is of individual concern to it, there is no basis for its claim that the order under appeal undermines its right to effective judicial protection.

62 The third plea in law must therefore be rejected as clearly unfounded.

63 Since none of the pleas in law relied upon are well founded, the appeal must be dismissed.

....

On those grounds, the Court (Sixth Chamber) hereby orders:

1. The appeal is dismissed.
Galileo Lebensmittel GmbH & Co. KG is ordered to pay the costs.

C-569/08 - Internetportal und Marketing

1. Article 21(3) of Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration must be interpreted as meaning that bad faith can be established by circumstances other than those listed in Article 21(3)(a) to (e) of that Regulation.

2. In order to assess whether there is conduct in bad faith within the meaning of Article 21(1)(b) of Regulation No 874/2004, read in conjunction with Article 21(3) thereof, the national court must take into consideration all the relevant factors specific to the particular case and, in particular, the conditions under which registration of the trade mark was obtained and those under which the .eu top level domain name was registered.

With regard to the conditions under which registration of the trade mark was obtained, the national court must take into consideration, in particular:

- the intention not to use the trade mark in the market for which protection was sought;
- the presentation of the trade mark;
- the fact of having registered a large number of other trade marks corresponding to generic terms; and
- the fact of having registered the trade mark shortly before the beginning of phased registration of .eu top level domain names.

With regard to the conditions under which the .eu top level domain name was registered, the national court must take into consideration, in particular:

- the abusive use of special characters or punctuation marks, within the meaning of Article 11 of Regulation No 874/2004, for the purposes of applying the transcription rules laid down in that article;
- registration during the first part of the phased registration provided for in that Regulation on the basis of a mark acquired in circumstances such as those in the main proceedings; and
- the fact of having applied for registration of a large number of domain names corresponding to generic terms.

C-376/11 - Pie Optiek

Question for a preliminary ruling:

'(1) Must Article 12(2) of [Regulation No 874/2004] be interpreted as meaning that, in a situation where the prior right concerned is a trade mark right, the words "licensees of prior rights" may refer to a person who has been authorised by the proprietor of the trade mark solely to register, in his own name but on behalf of the licensor, a domain name identical or similar to the trade mark, but without being authorised to put the trade mark to other uses or to use the sign as a trade mark — for example, for the purpose of marketing of goods or services under the trade mark?'

(2) If that question is answered in the affirmative, must Article 21(1)(a) of [Regulation No 874/2004] be interpreted as meaning that "rights or legitimate interest" exist even if the "licensee of prior rights" has obtained registration of the .eu domain name in his own name but on behalf of the proprietor of the trade mark where the latter is not eligible in accordance with Article 4(2)(b) of Regulation [No 733/2002]?'
Judgement:

The third subparagraph of Article 12(2) of Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration must be interpreted as meaning that, in a situation where the prior right concerned is a trade mark right, the words 'licensees of prior rights' do not refer to a

person who has been authorised by the proprietor of the trade mark concerned solely to register, in his own name but on behalf of that proprietor, a domain name identical or similar

to that trade mark, but without that person being authorised to use the trade mark commercially in a manner consistent with its functions.

Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration

(Text with EEA relevance)

COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain (1), and in particular Article 5(1) thereof,

Having consulted the Registry in accordance with Article 5(1) of Regulation (EC) No 733/2002,

Whereas:

(1)

The initial implementation stages of the .eu Top Level Domain (TLD), to be created pursuant to Regulation (EC) No 733/2002, have been completed by designating a legal entity, established within the Community to administer and manage the .eu TLD Registry function. The Registry, designated by Commission Decision 2003/375/EC (2), is required to be a non-profit organisation that should operate and provide services on a cost covering basis and at an affordable price.

(2)

Requesting a domain name should be possible through electronic means in a simple, speedy and efficient procedure, in all official languages of the Community, through accredited registrars.

(3)

Accreditation of registrars should be carried out by the Registry following a procedure that ensures fair and open competition between Registrars. The accreditation process should be objective, transparent and non-discriminatory. Only parties who meet certain basic technical requirements to be determined by the Registry should be eligible for accreditation.

(4)

Registrars should only accept applications for the registration of domain names filed after their accreditation and should forward them in the chronological order in which they were received.

(5)

To ensure better protection of consumers' rights, and without prejudice to any Community rules concerning jurisdiction and applicable law, the applicable law in disputes between registrars and registrants on matters concerning Community titles should be the law of one of the Member States.

(6)

Registrars should require accurate contact information from their clients, such as full name, address of domicile, telephone number and electronic mail, as well as information concerning a natural or legal person responsible for the technical operation of the domain name.

(7)

The Registry policy should promote the use of all the official languages of the Community.

(8)

Pursuant to Regulation (EC) No 733/2002, Member States may request that their official name and the name under which they

are commonly known should not be registered directly under .eu TLD otherwise than by their national government. Countries that are expected to join the European Union later than May 2004 should be enabled to block their official names and the names under which they are commonly known, so that they can be registered at a later date.

(9)

A Member State should be authorised to designate an operator that will register as a domain name its official name and the name under which it is commonly known. Similarly, the Commission should be authorised to select domain names for use by the institutions of the Community, and to designate the operator of those domain names. The Registry should be empowered to reserve a number of specified domain names for its operational functions.

(10)

In accordance with Article 5(2) of Regulation (EC) No 733/2002, a number of Member States have notified to the Commission and to other Member States a limited list of broadly-recognised names with regard to geographical and/or geopolitical concepts which affect their political or territorial organisation. Such lists include names that could either not be registered or which could be registered only under the second level domain in accordance with the public policy rules. The names included in these lists are not subject to the first-come first-served principle.

(11)

The principle of first-come-first-served should be the basic principle for resolving a dispute between holders of prior rights during the phased registration. After the termination of the phased registration the principle of first come first served should apply in the allocation of domain names.

(12)

In order to safeguard prior rights recognised by Community or national law, a procedure for phased registration should be put in place. Phased registration should take place in two phases, with the aim of ensuring that holders of prior rights have appropriate opportunities to register the names on which they hold prior rights. The Registry should ensure that validation of the rights is performed by appointed validation agents. On the basis of evidence provided by the applicants, validation agents should assess the right which is claimed for a particular name. Allocation of that name should then take place on a first-come, first-served basis if there are two or more applicants for a domain name, each having a prior right.

(13)

The Registry should enter into an appropriate escrow agreement to ensure continuity of service, and in particular to ensure that in the event of re-delegation or other unforeseen circumstances it is possible to continue to provide services to the local Internet community with minimum disruption. The Registry should also comply with the relevant data protection rules, principles, guidelines and best practices, notably concerning the amount and type of data displayed in the WHOIS database. Domain names considered by a Member State court to be defamatory, racist or contrary to public policy should be

blocked and eventually revoked once the court decision becomes final. Such domain names should be blocked from future registrations.

(14)

In the event of the death or insolvency of a domain name holder, if no transfer has been initiated at the expiry of the registration period, the domain name should be suspended for 40 calendar days. If the heirs or administrators concerned have not registered the name during that period it should become available for general registration.

(15)

Domain names should be open to revocation by the Registry on a limited number of specified grounds, after giving the domain name holder concerned an opportunity to take appropriate measures. Domain names should also be capable of revocation through an alternative dispute resolution (ADR) procedure.

(16)

The Registry should provide for an ADR procedure which takes into account the international best practices in this area and in particular the relevant World Intellectual Property Organization (WIPO) recommendations, to ensure that speculative and abusive registrations are avoided as far as possible.

(17)

The Registry should select service providers that have appropriate expertise on the basis of objective, transparent and non-discriminatory criteria. ADR should respect a minimum of uniform procedural rules, similar to the ones set out in the Uniform Dispute Resolution Policy adopted by the Internet Corporation of Assigned Names and Numbers (ICANN).

(18)

In view of the impending enlargement of the Union it is imperative that the system of public policy rules set up by this Regulation enter into force without delay.

(19)

The measures provided for in this Regulation are in accordance with the opinion of the Communications Committee established by Article 22(1) of Directive 2002/21/EC of the European Parliament and of the Council (3),
HAS ADOPTED THIS REGULATION:

CHAPTER I

SUBJECT MATTER

Article 1

Subject matter

This Regulation sets out the public policy rules concerning the implementation and functions of the .eu Top Level Domain (TLD) and the public policy principles on registration referred to in Article 5(1) of Regulation (EC) No 733/2002.

CHAPTER II

PRINCIPLES ON REGISTRATION

Article 2

Eligibility and general principles for registration

An eligible party, as listed in Article 4(2)(b) of Regulation (EC) No 733/2002, may register one or more domain names under .eu TLD.

Without prejudice to Chapter IV, a specific domain name shall be allocated for use to the eligible party whose request has been received first by the Registry in the technically correct manner and in accordance with this Regulation. For the purposes of this Regulation, this criterion of first receipt shall be referred to as the 'first-come-first-served' principle.

Once a domain name is registered it shall become unavailable for further registration until the registration expires without renewal, or until the domain name is revoked.

Unless otherwise specified in this Regulation, domain names shall be registered directly under the .eu TLD.

Domain name registration shall be valid only after the appropriate fee has been paid by the requesting party.

Domain names registered under the .eu TLD shall only be transferable to parties that are eligible for registration of .eu domain names.

Article 3

Requests for domain name registration

The request for domain name registration shall include all of the following:

(a) the name and address of the requesting party;

(b) a confirmation by electronic means from the requesting party that it satisfies the general eligibility criteria set out in Article 4(2)(b) of Regulation (EC) No 733/2002;

(c) an affirmation by electronic means from the requesting party that to its knowledge the request for domain name registration is made in good faith and does not infringe any rights of a third party;

(d) an undertaking by electronic means from the requesting party that it shall abide by all the terms and conditions for registration, including the policy on the extra-judicial settlement of conflicts set out in Chapter VI.

Any material inaccuracy in the elements set out in points (a) to (d) shall constitute a breach of the terms of registration.

Any verification by the Registry of the validity of registration applications shall take place subsequently to the registration at the initiative of the Registry or pursuant to a dispute for the registration of the domain name in question, except for applications filed in the course of the phased registration procedure under Articles 10, 12, and 14.

Article 4

Accreditation of registrars

Only registrars accredited by the Registry shall be permitted to offer registration services for names under the .eu TLD.

The procedure for the accreditation of registrars shall be determined by the Registry and shall be reasonable, transparent and non-discriminatory, and shall ensure effective and fair conditions of competition.

Registrars are required to access and use the Registry's automated registration systems. The Registry may set further basic technical requirements for the accreditation of registrars. The Registry may ask registrars for advance payment of registration fees, to be set annually by the Registry based on a reasonable market estimate.

The procedure, terms of accreditation of registrars and the list of accredited registrars shall be made publicly available by the Registry in readily accessible form.

Each registrar shall be bound by contract with the Registry to observe the terms of accreditation and in particular to comply with the public policy principles set out in this Regulation.

Article 5

Provisions for registrars

Without prejudice to any rule governing jurisdiction and applicable law, agreements between the Registrar and the registrant of a domain name cannot designate, as applicable law, a law other than the law of one of the Member States, nor can they designate a dispute-resolution body, unless selected by the Registry pursuant to Article 23, nor an arbitration court or a court located outside the Community.

A registrar who receives more than one registration request for the same name shall forward those requests to the Registry in the chronological order in which they were received.

Only applications received after the date of accreditation shall be forwarded to the Registry.

Registrars shall require all applicants to submit accurate and reliable contact details of at least one natural or legal person responsible for the technical operation of the domain name that is requested.

Registrars may develop label, authentication and trustmark schemes in order to promote consumer confidence in the reliability of information that is available under a domain name

that is registered by them, in accordance with applicable national and Community law.

CHAPTER III LANGUAGES AND GEOGRAPHICAL CONCEPTS

Article 6 Languages

►M3 1. ◀ Registrations of .eu domain names shall start only after the Registry has informed the Commission that the filing of applications for the registration of .eu domain names and communications of decisions concerning registration is possible in all official languages of the Community, hereinafter referred to as 'official languages'.

►M3 2. ◀ For any communication by the Registry that affects the rights of a party in conjunction with a registration, such as the grant, transfer, cancellation or revocation of a domain, the Registry shall ensure that these communications are possible in all official languages.

►M3 3. ◀ The Registry shall perform the registration of domain names in all the alphabetic characters of the official languages when adequate international standards become available.

▼M3

4. If it becomes technically possible to register names in the official languages under the .eu TLD using alphabetic characters which were not available for registration at the beginning of the phased registration period provided for in Chapter IV, the Registry shall announce on its website that it will be possible to register names under the .eu TLD containing those characters. The announcement shall contain a list of the characters in question and set out the date from which it will be possible to register .eu domain names using them.

The announcement shall be made three months before that date at the latest.

5. The Registry shall not be required to perform functions using languages other than the official languages.

▼B

Article 7

Procedure for reserved geographical and geopolitical names

For the procedure of raising objections to the lists of broadly recognised names in accordance with the third subparagraph of Article 5(2) of Regulation (EC) No 733/2002, objections shall be notified to the members of the Communications Committee established by Article 22(1) of Directive 2002/21/EC and to the Director-General of the Commission's Directorate-General Information Society. The members of the Communications Committee and the Director-General may designate other contact points for these notifications.

Objections and designations of contact points shall be notified in the form of electronic mail, delivery by courier or in person, or by postal delivery effected by way of registered letter and acknowledgement of receipt.

Upon the resolution of any objections, the Registry shall publish on its web site two lists of names. The one list shall contain the list of names that the Commission shall have notified as 'not registrable'. The other list shall contain the list of names that the Commission shall have notified to the Registry as 'registrable only under a second level domain'.

▼M1

Article 8

Reservation of names by countries and alpha-2 codes representing countries

1. The list of names set out in the Annex to this Regulation shall only be reserved or registered as second level domain names directly under the .eu TLD by the countries indicated in the list.

2. Alpha-2 codes representing countries shall not be registered as second level domain names directly under the .eu TLD.

▼B

Article 9

Second level domain name for geographical and geopolitical names

►M3 1. ◀ Registration of geographical and geopolitical concepts as domain names in accordance with Article 5(2)(b) of Regulation (EC) No 733/2002 may be provided for by a Member State that has notified the names. This may be done under any domain name that has been registered by that Member State.

►M3 2. ◀ The Commission may ask the Registry to introduce domain names directly under the .eu TLD for use by the Community institutions and bodies. After the entry into force of this Regulation and not later than a week before the beginning of the phased registration period provided for in Chapter IV, the Commission shall notify the Registry of the names that are to be reserved and the bodies that represent the Community institutions and bodies in registering the names.

▼M3

3. If it becomes technically possible to register names in the official languages under the .eu TLD using alphabetic characters which were not available for registration at the beginning of the phased registration period provided for in Chapter IV, the Registry shall notify the Commission thereof.

That notification shall be made at the latest one month prior to the day of the announcement referred to in Article 6(4) and shall indicate the date of the announcement.

At the latest 10 working days before the date indicated in the announcement made in accordance with Article 6(4), the Commission shall ask the Registry to introduce any domain names containing one or more of those characters which it wishes to reserve for use by the Community institutions and bodies, directly under the .eu TLD.

▼B

CHAPTER IV

PHASED REGISTRATION

Article 10

Eligible parties and the names they can register

1. Holders of prior rights recognised or established by national and/or Community law and public bodies shall be eligible to apply to register domain names during a period of phased registration before general registration of .eu domain starts.

'Prior rights' shall be understood to include, inter alia, registered national and community trademarks, geographical indications or designations of origin, and, in as far as they are protected under national law in the Member-State where they are held: unregistered trademarks, trade names, business identifiers, company names, family names, and distinctive titles of protected literary and artistic works.

'Public bodies' shall include: institutions and bodies of the Community, national and local governments, governmental bodies, authorities, organisations and bodies governed by public law, and international and intergovernmental organisations.

2. The registration on the basis of a prior right shall consist of the registration of the complete name for which the prior right exists, as written in the documentation which proves that such a right exists.

3. The registration by a public body may consist of the complete name of the public body or the acronym that is generally used. Public bodies that are responsible for governing a particular geographic territory may also register the complete name of the territory for which they are responsible, and the name under which the territory is commonly known.

Article 11

Special characters

As far as the registration of complete names is concerned, where such names comprise a space between the textual or word elements, identity shall be deemed to exist between such complete names and the same names written with a hyphen between the word elements or combined in one word in the domain name applied for.

Where the name for which prior rights are claimed contains special characters, spaces, or punctuations, these shall be eliminated entirely from the corresponding domain name, replaced with hyphens, or, if possible, rewritten.

Special character and punctuations as referred to in the second paragraph shall include the following:

~ @ # \$ % ^ & * () + = < > { } [] \ / : ; ' , . ?

Without prejudice to ►M3 Article 6(3) ◀, if the prior right name contains letters which have additional elements that cannot be reproduced in ASCII code, such as ä, é or ñ, the letters concerned shall be reproduced without these elements (such as a, e, n), or shall be replaced by conventionally accepted spellings (such as ae). In all other respects, the domain name shall be identical to the textual or word elements of the prior right name.

Article 12

Principles for phased registration

1. ►M1 Phased registration shall not start before the requirement of ►M3 Article 6(1) ◀ is fulfilled. ◀

The Registry shall publish the date on which phased registration shall start at least two months in advance and shall inform all accredited Registrars accordingly.

The Registry shall publish on its website two months before the beginning of the phased registration a detailed description of all the technical and administrative measures that it shall use to ensure a proper, fair and technically sound administration of the phased registration period.

2. The duration of the phased registration period shall be four months. General registration of domain names shall not start prior to the completion of the phased registration period.

Phased registration shall be comprised of two parts of two months each.

During the first part of phased registration, only registered national and Community trademarks, geographical indications, and the names and acronyms referred to in Article 10(3), may be applied for as domain names by holders or licensees of prior rights and by the public bodies mentioned in Article 10(1).

During the second part of phased registration, the names that can be registered in the first part as well as names based on all other prior rights can be applied for as domain names by holders of prior rights on those names.

3. The request to register a domain name based on a prior right under Article 10(1) and (2) shall include a reference to the legal basis in national or Community law for the right to the name, as well as other relevant information, such as trademark registration number, information concerning publication in an official journal or government gazette, registration information at professional or business associations and chambers of commerce.

4. The Registry may make the requests for domain name registration subject to payment of additional fees, provided that these serve merely to cover the costs generated by the application of this Chapter. The Registry may charge differential fees depending upon the complexity of the process required to validate prior rights.

5. At the end of the phased registration an independent audit shall be performed at the expense of the Registry and shall report its findings to the Commission. The auditor shall be appointed by the Registry after consulting the Commission. The purpose of the audit shall be to confirm the fair, appropriate and sound operational and technical administration of the phased registration period by the Registry.

6. To resolve a dispute over a domain name the rules provided in Chapter VI shall apply.

Article 13

Selection of validation agents

Validation agents shall be legal persons established within the territory of the Community. Validation agents shall be reputable bodies with appropriate expertise. The Registry shall select the validation agents in an objective, transparent and non-discriminatory manner, ensuring the widest possible geographical diversity. The Registry shall require the validation agent to execute the validation in an objective, transparent and non-discriminatory manner.

Member States shall provide for validation concerning the names mentioned in Article 10(3). To that end, the Member States shall send to the Commission within two months following entry into force of this Regulation, a clear indication of the addresses to which documentary evidence is to be sent for verification. The Commission shall notify the Registry of these addresses.

The Registry shall publish information about the validation agents at its website.

Article 14

Validation and registration of applications received during phased registration

All claims for prior rights under Article 10(1) and (2) must be verifiable by documentary evidence which demonstrates the right under the law by virtue of which it exists.

The Registry, upon receipt of the application, shall block the domain name in question until validation has taken place or until the deadline passes for receipt of documentation. If the Registry receives more than one claim for the same domain during the phased registration period, applications shall be dealt with in strict chronological order.

The Registry shall make available a database containing information about the domain names applied for under the procedure for phased registration, the applicants, the Registrar that submitted the application, the deadline for submission of validation documents, and subsequent claims on the names.

Every applicant shall submit documentary evidence that shows that he or she is the holder of the prior right claimed on the name in question. The documentary evidence shall be submitted to a validation agent indicated by the Registry. The applicant shall submit the evidence in such a way that it shall be received by the validation agent within forty days from the submission of the application for the domain name. If the documentary evidence has not been received by this deadline, the application for the domain name shall be rejected.

Validation agents shall time-stamp documentary evidence upon receipt.

Validation agents shall examine applications for any particular domain name in the order in which the application was received at the Registry.

The relevant validation agent shall examine whether the applicant that is first in line to be assessed for a domain name and that has submitted the documentary evidence before the deadline has prior rights on the name. If the documentary evidence has not been received in time or if the validation agent finds that the documentary evidence does not substantiate a prior right, he shall notify the Registry of this.

If the validation agent finds that prior rights exist regarding the application for a particular domain name that is first in line, he shall notify the Registry accordingly.

This examination of each claim in chronological order of receipt shall be followed until a claim is found for which prior rights on the name in question are confirmed by a validation agent.

The Registry shall register the domain name, on the first come first served basis, if it finds that the applicant has demonstrated a prior right in accordance with the procedure set out in the second, third and fourth paragraphs.

CHAPTER V

RESERVATIONS, WHOIS DATA AND IMPROPER REGISTRATIONS

Article 15

Escrow agreement

1. The Registry shall, at its own expense, enter into an agreement with a reputable trustee or other escrow agent established within the territory of the Community designating the Commission as the beneficiary of the escrow agreement. The Commission shall give its consent to that agreement before it is concluded. The Registry shall submit to the escrow agent on a daily basis an electronic copy of the current content of the .eu database.

2. The agreement shall provide that the data shall be held by the escrow agent on the following terms and conditions:

(a) the data shall be received and held in escrow, undergoing no procedure other than verification that it is complete, consistent, and in proper format, until it is released to the Commission;

(b) the data shall be released from escrow upon expiration without renewal or upon termination of the contract between the Registry and the Commission for any of the reasons described therein and irrespectively of any disputes or litigation between the Commission and the Registry;

(c) in the event that the escrow is released, the Commission shall have the exclusive, irrevocable, royalty-free right to exercise or to have exercised all rights necessary to re-designate the Registry;

(d) if the contract with the Registry is terminated the Commission, with the cooperation of the Registry, shall take all necessary steps to transfer the administrative and operational responsibility for the .eu TLD and any reserve funds to such party as the Commission may designate: in that event, the Registry shall make all efforts to avoid disruption of the service and shall in particular continue to update the information that is subject to the escrow until the time of completion of the transfer.

Article 16

WHOIS database

The purpose of the WHOIS database shall be to provide reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names under the .eu TLD.

The WHOIS database shall contain information about the holder of a domain name that is relevant and not excessive in relation to the purpose of the database. In as far as the information is not strictly necessary in relation to the purpose of the database, and if the domain name holder is a natural person, the information that is to be made publicly available shall be subject to the unambiguous consent of the domain name holder. The deliberate submission of inaccurate information, shall constitute grounds for considering the domain name registration to have been in breach of the terms of registration.

Article 17

Names reserved by the Registry

The following names shall be reserved for the operational functions of the Registry:

eurid.eu, registry.eu, nic.eu, dns.eu, internic.eu, whois.eu, das.eu, coc.eu, eurethix.eu, eurethics.eu, euthics.eu

Article 18

Improper registrations

Where a domain name is considered by a Court of a Member State to be defamatory, racist or contrary to public policy, it shall be blocked by the Registry upon notification of a Court decision and shall be revoked upon notification of a final court decision. The Registry shall block from future registration those names which have been subject to such a court order for as long as such order remains valid.

Article 19

Death and winding up

1. If the domain name holder dies during the registration period of the domain name, the executors of his or her estate, or his or her legal heirs, may request transfer of the name to the heirs along with submission of the appropriate documentation. If, on expiry of the registration period, no transfer has been initiated, the domain name shall be suspended for a period of 40 calendar days and shall be published on the Registry's website. During this period the executors or the legal heirs may apply to register the name along with submission of the appropriate documentation. If the heirs have not registered the name during that 40-day period, the domain name shall thereafter become available for general registration.

2. If the domain name holder is an undertaking, a legal or natural person, or an organisation that becomes subject to insolvency proceedings, winding up, cessation of trading, winding up by court order or any similar proceeding provided for by national law, during the registration period of the domain name, then the legally appointed administrator of the domain name holder may request transfer to the purchaser of the domain name holders assets along with submission of the appropriate documentation. If, on expiry of the registration period, no transfer has been initiated, the domain name shall be suspended for a period of forty calendar days and shall be published on the registry's website. During this period the administrator may apply to register the name along with submission of appropriate documentation. If the administrator has not registered the name during that 40-day period, the domain name shall thereafter become available for general registration.

CHAPTER VI

REVOCATION AND SETTLEMENT OF CONFLICTS

Article 20

Revocation of domain names

The Registry may revoke a domain name at its own initiative and without submitting the dispute to any extrajudicial settlement of conflicts, exclusively on the following grounds:

(a) outstanding unpaid debts owed to the Registry;

(b) holder's non-fulfilment of the general eligibility criteria pursuant to Article 4(2)(b) of Regulation (EC) 733/2002;

(c) holder's breach of the terms of registration under Article 3.

The Registry shall lay down a procedure in accordance with which it may revoke domain names on these grounds. This procedure shall include a notice to the domain name holder and shall afford him an opportunity to take appropriate measures. Revocation of a domain name, and where necessary its subsequent transfer, may also be effected in accordance with a decision issued by an extrajudicial settlement body.

Article 21

Speculative and abusive registrations

1. A registered domain name shall be subject to revocation, using an appropriate extra-judicial or judicial procedure, where that name is identical or confusingly similar to a name in respect of which a right is recognised or established by national and/or Community law, such as the rights mentioned in Article 10(1), and where it:

(a) has been registered by its holder without rights or legitimate interest in the name; or

(b) has been registered or is being used in bad faith.

2. A legitimate interest within the meaning of point (a) of paragraph 1 may be demonstrated where:

(a) prior to any notice of an alternative dispute resolution (ADR) procedure, the holder of a domain name has used the domain name or a name corresponding to the domain name in

connection with the offering of goods or services or has made demonstrable preparation to do so;

(b) the holder of a domain name, being an undertaking, organisation or natural person, has been commonly known by the domain name, even in the absence of a right recognised or established by national and/or Community law;

(c) the holder of a domain name is making a legitimate and non-commercial or fair use of the domain name, without intent to mislead consumers or harm the reputation of a name on which a right is recognised or established by national and/or Community law.

3. Bad faith, within the meaning of point (b) of paragraph 1 may be demonstrated, where:

(a) circumstances indicate that the domain name was registered or acquired primarily for the purpose of selling, renting, or otherwise transferring the domain name to the holder of a name in respect of which a right is recognised or established by national and/or Community law or to a public body; or

(b) the domain name has been registered in order to prevent the holder of such a name in respect of which a right is recognised or established by national and/or Community law, or a public body, from reflecting this name in a corresponding domain name, provided that:

(i) a pattern of such conduct by the registrant can be demonstrated; or

(ii) the domain name has not been used in a relevant way for at least two years from the date of registration; or

(iii) in circumstances where, at the time the ADR procedure was initiated, the holder of a domain name in respect of which a right is recognised or established by national and/or Community law or the holder of a domain name of a public body has declared his/its intention to use the domain name in a relevant way but fails to do so within six months of the day on which the ADR procedure was initiated;

(c) the domain name was registered primarily for the purpose of disrupting the professional activities of a competitor; or

(d) the domain name was intentionally used to attract Internet users, for commercial gain, to the holder of a domain name website or other on-line location, by creating a likelihood of confusion with a name on which a right is recognised or established by national and/or Community law or a name of a public body, such likelihood arising as to the source, sponsorship, affiliation or endorsement of the website or location or of a product or service on the website or location of the holder of a domain name; or

(e) the domain name registered is a personal name for which no demonstrable link exists between the domain name holder and the domain name registered.

4. The provisions in paragraphs 1, 2 and 3 may not be invoked so as to obstruct claims under national law.

Article 22

Alternative dispute resolution (ADR) procedure

1. An ADR procedure may be initiated by any party where:

(a) the registration is speculative or abusive within the meaning of Article 21; or

(b) a decision taken by the Registry conflicts with this Regulation or with Regulation (EC) No 733/2002.

2. Participation in the ADR procedure shall be compulsory for the holder of a domain name and the Registry.

3. A fee for the ADR shall be paid by the complainant.

4. Unless otherwise agreed by the parties, or specified otherwise in the registration agreement between registrar and domain name holder, the language of the administrative proceeding shall be the language of that agreement. This rule shall be subject to the authority of the panel to determine otherwise, having regard to the circumstances of the case.

5. The complaints and the responses to those complaints must be submitted to an ADR provider chosen by the complainant from the list referred to in the first paragraph of Article 23. That submission shall be made in accordance with this Regulation

and the published supplementary procedures of the ADR provider.

6. As soon as a request for ADR is properly filed with the ADR provider and the appropriate fee is paid, the ADR provider shall inform the Registry of the identity of the complainant and the domain name involved. The Registry shall suspend the domain name involved from cancellation or transfer until the dispute resolution proceedings or subsequent legal proceedings are complete and the decision has been notified to the Registry.

7. The ADR provider shall examine the complaint for compliance with its rules of procedure, with the provisions of this Regulation and with Regulation (EC) No 733/2002, and, unless non-compliance is established, shall forward the complaint to the respondent within five working days following receipt of the fees to be paid by the complainant.

8. Within 30 working days of the date of receipt of the complaint the respondent shall submit a response to the provider.

9. Any written communication to a complainant or respondent shall be made by the preferred means stated by the complainant or respondent, respectively, or in the absence of such specification electronically via the Internet, provided that a record of transmission is available.

All communications concerning the ADR procedure to the holder of a domain name that is subject to an ADR procedure shall be sent to the address information that is available to the Registrar that maintains the registration of the domain name in accordance with the terms and conditions of registration.

10. Failure of any of the parties involved in an ADR procedure to respond within the given deadlines or appear to a panel hearing may be considered as grounds to accept the claims of the counterparty.

11. In the case of a procedure against a domain name holder, the ADR panel shall decide that the domain name shall be revoked, if it finds that the registration is speculative or abusive as defined in Article 21. The domain name shall be transferred to the complainant if the complainant applies for this domain name and satisfies the general eligibility criteria set out in Article 4(2)(b) of Regulation (EC) No 733/2002.

In the case of a procedure against the Registry, the ADR panel shall decide whether a decision taken by the Registry conflicts with this Regulation or with Regulation (EC) No 733/2002. The ADR panel shall decide that the decision shall be annulled and may decide in appropriate cases that the domain name in question shall be transferred, revoked or attributed, provided that, where necessary, the general eligibility criteria set out in Article 4(2)(b) of Regulation (EC) No 733/2002 are fulfilled. The decision of the ADR panel shall state the date for implementation of the decision.

Decisions of the panel are taken by simple majority. The alternative dispute panel shall issue its decision within one month from the date of receipt of the response by the ADR provider. The decision shall be duly motivated. The decisions of the panel shall be published.

12. Within three working days after receiving the decision from the panel, the provider shall notify the full text of the decision to each party, the concerned registrar(s) and the Registry. The decision shall be notified to the Registry and the complainant by registered post or other equivalent electronic means.

13. The results of ADR shall be binding on the parties and the Registry unless court proceedings are initiated within 30 calendar days of the notification of the result of the ADR procedure to the parties.

Article 23

Selection of providers and panellists for alternative dispute resolution

1. The Registry may select ADR providers, who shall be reputable bodies with appropriate expertise in an objective, transparent and non-discriminatory manner. A list of the ADR providers shall be published on the Registry's website.

2. A dispute which is submitted to the ADR procedure shall be examined by arbitrators appointed to a panel of one or three members.

The panellists shall be selected in accordance to the internal procedures of the selected ADR providers. They shall have appropriate expertise and shall be selected in an objective, transparent and non-discriminatory manner. Each provider shall maintain a publicly available list of panellists and their qualifications.

A panellist shall be impartial and independent and shall have, before accepting appointment, disclosed to the provider any circumstances giving rise to justifiable doubt as to their impartiality or independence. If, at any stage during the administrative proceedings, new circumstances arise that could give rise to justifiable doubt as to the impartiality or independence of the panellist, that panellist shall promptly disclose such circumstances to the provider.

Amended by:

	Official Journal	
	No	page date
►M1 <u>Commission Regulation (EC) No 1654/2005 of 10 October 2005</u>	L 266	35 11.10.2005
M2 <u>Commission Regulation (EC) No 1255/2007 of 25 October 2007</u>	L 282	16 26.10.2007
►M3 <u>Commission Regulation (EC) No 560/2009 of 26 June 2009</u>	L 166	3 27.6.2009

Corrected by:

In such event, the provider shall appoint a substitute panellist.

CHAPTER VII

FINAL PROVISIONS

Article 24

Entry into force

This Regulation shall enter into force on the day of its publication in the Official Journal of the European Union. This Regulation shall be binding in its entirety and directly applicable in all Member States.

▼M3

►C1

Corrigendum, OJ L 291, 7.11.2009, p. 42 (560/09)

IV. Public Sector Information

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the European Economic and Social Committee (2),

Having regard to the opinion of the Committee of the Regions (3),

Acting in accordance with the procedure set out in Article 251 of the Treaty (4),

Whereas:

(1) The Treaty provides for the establishment of an internal market and of a system ensuring that competition in the internal market is not distorted. Harmonisation of the rules and practices in the Member States relating to the exploitation of public sector information contributes to the achievement of these objectives.

(2) The evolution towards an information and knowledge society influences the life of every citizen in the Community, inter alia, by enabling them to gain new ways of accessing and acquiring knowledge.

(3) Digital content plays an important role in this evolution. Content production has given rise to rapid job creation in recent years and continues to do so. Most of these jobs are created in small emerging companies.

(4) The public sector collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, economic, geographical, weather, tourist, business, patent and educational information.

(5) One of the principal aims of the establishment of an internal market is the creation of conditions conducive to the development of Community-wide services. Public sector information is an important primary material for digital content products and services and will become an even more important content resource with the development of wireless content services. Broad cross-border geographical coverage will also be essential in this context. Wider possibilities of re-using public sector information should inter alia allow European companies to exploit its potential and contribute to economic growth and job creation.

(6) There are considerable differences in the rules and practices in the Member States relating to the exploitation of public sector information resources, which constitute barriers to bringing out the full economic potential of this key document resource. Traditional practice in public sector bodies in exploiting public sector information has developed in very disparate ways. That should be taken into account. Minimum harmonisation of national rules and practices on the re-use of public sector documents should therefore be undertaken, in cases where the differences in national Regulations and practices or the absence of clarity hinder the smooth functioning of the internal market and the proper development of the information society in the Community.

(7) Moreover, without minimum harmonisation at Community level, legislative activities at national level, which have already been initiated in a number of Member States in order to respond to the technological challenges, might result in even

more significant differences. The impact of such legislative differences and uncertainties will become more significant with the further development of the information society, which has already greatly increased cross-border exploitation of information.

(8) A general framework for the conditions governing re-use of public sector documents is needed in order to ensure fair, proportionate and non-discriminatory conditions for the re-use of such information. Public sector bodies collect, produce, reproduce and disseminate documents to fulfil their public tasks. Use of such documents for other reasons constitutes a re-use. Member States' policies can go beyond the minimum standards established in this Directive, thus allowing for more extensive re-use.

(9) This Directive does not contain an obligation to allow re-use of documents. The decision whether or not to authorise re-use will remain with the Member States or the public sector body concerned. This Directive should apply to documents that are made accessible for re-use when public sector bodies license, sell, disseminate, exchange or give out information. To avoid cross-subsidies, re-use should include further use of documents within the organisation itself for activities falling outside the scope of its public tasks. Activities falling outside the public task will typically include supply of documents that are produced and charged for exclusively on a commercial basis and in competition with others in the market. The definition of 'document' is not intended to cover computer programmes. The Directive builds on the existing access regimes in the Member States and does not change the national rules for access to documents. It does not apply in cases in which citizens or companies can, under the relevant access regime, only obtain a document if they can prove a particular interest. At Community level, Articles 41 (right to good administration) and 42 of the Charter of Fundamental Rights of the European Union recognise the right of any citizen of the Union and any natural or legal person residing or having its registered office in a Member State to have access to European Parliament, Council and Commission documents. Public sector bodies should be encouraged to make available for re-use any documents held by them. Public sector bodies should promote and encourage re-use of documents, including official texts of a legislative and administrative nature in those cases where the public sector body has the right to authorise their re-use.

(10) The definitions of 'public sector body' and 'body governed by public law' are taken from the public procurement Directives (92/50/EEC (5), 93/36/EEC (6) and 93/37/EEC (7) and 98/4/EC (8)). Public undertakings are not covered by these definitions.

(11) This Directive lays down a generic definition of the term 'document', in line with developments in the information society. It covers any representation of acts, facts or information — and any compilation of such acts, facts or information — whatever its medium (written on paper, or stored in electronic form or as a sound, visual or audiovisual recording), held by public sector bodies. A document held by a public sector body is a document where the public sector body has the right to authorise re-use.

(12) The time limit for replying to requests for re-use should be reasonable and in line with the equivalent time for requests to

access the document under the relevant access regimes. Reasonable time limits throughout the Union will stimulate the creation of new aggregated information products and services at pan-European level. Once a request for re-use has been granted, public sector bodies should make the documents available in a timeframe that allows their full economic potential to be exploited. This is particularly important for dynamic content (e.g. traffic data), the economic value of which depends on the immediate availability of the information and of regular updates. Should a licence be used, the timely availability of documents may be a part of the terms of the licence.

(13) The possibilities for re-use can be improved by limiting the need to digitise paper-based documents or to process digital files to make them mutually compatible. Therefore, public sector bodies should make documents available in any pre-existing format or language, through electronic means where possible and appropriate. Public sector bodies should view requests for extracts from existing documents favourably when to grant such a request would involve only a simple operation. Public sector bodies should not, however, be obliged to provide an extract from a document where this involves disproportionate effort. To facilitate re-use, public sector bodies should make their own documents available in a format which, as far as possible and appropriate, is not dependent on the use of specific software. Where possible and appropriate, public sector bodies should take into account the possibilities for the re-use of documents by and for people with disabilities.

(14) Where charges are made, the total income should not exceed the total costs of collecting, producing, reproducing and disseminating documents, together with a reasonable return on investment, having due regard to the self-financing requirements of the public sector body concerned, where applicable. Production includes creation and collation, and dissemination may also include user support. Recovery of costs, together with a reasonable return on investment, consistent with applicable accounting principles and the relevant cost calculation method of the public sector body concerned, constitutes an upper limit to the charges, as any excessive prices should be precluded. The upper limit for charges set in this Directive is without prejudice to the right of Member States or public sector bodies to apply lower charges or no charges at all, and Member States should encourage public sector bodies to make documents available at charges that do not exceed the marginal costs for reproducing and disseminating the documents.

(15) Ensuring that the conditions for re-use of public sector documents are clear and publicly available is a pre-condition for the development of a Community-wide information market. Therefore all applicable conditions for the re-use of the documents should be made clear to the potential re-users. Member States should encourage the creation of indices accessible on line, where appropriate, of available documents so as to promote and facilitate requests for re-use. Applicants for re-use of documents should be informed of available means of redress relating to decisions or practices affecting them. This will be particularly important for SMEs which may not be familiar with interactions with public sector bodies from other Member States and corresponding means of redress.

(16) Making public all generally available documents held by the public sector — concerning not only the political process but also the legal and administrative process — is a fundamental instrument for extending the right to knowledge, which is a basic principle of democracy. This objective is applicable to institutions at every level, be it local, national or international.

(17) In some cases the re-use of documents will take place without a licence being agreed. In other cases a licence will be issued imposing conditions on the re-use by the licensee dealing with issues such as liability, the proper use of documents, guaranteeing non-alteration and the acknowledgement of source. If public sector bodies license documents for re-use, the licence conditions should be fair and transparent. Standard licences that are available online may

also play an important role in this respect. Therefore Member States should provide for the availability of standard licences.

(18) If the competent authority decides to no longer make available certain documents for re-use, or to cease updating these documents, it should make these decisions publicly known, at the earliest opportunity, via electronic means whenever possible.

(19) Conditions for re-use should be non-discriminatory for comparable categories of re-use. This should, for example, not prevent the exchange of information between public sector bodies free of charge for the exercise of public tasks, whilst other parties are charged for the re-use of the same documents. Neither should it prevent the adoption of a differentiated charging policy for commercial and non-commercial re-use.

(20) Public sector bodies should respect competition rules when establishing the principles for re-use of documents avoiding as far as possible exclusive agreements between themselves and private partners. However, in order to provide a service of general economic interest, an exclusive right to re-use specific public sector documents may sometimes be necessary. This may be the case if no commercial publisher would publish the information without such an exclusive right.

(21) This Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data (9).

(22) The intellectual property rights of third parties are not affected by this Directive. For the avoidance of doubt, the term 'intellectual property rights' refers to copyright and related rights only (including sui generis forms of protection). This Directive does not apply to documents covered by industrial property rights, such as patents, registered designs and trademarks. The Directive does not affect the existence or ownership of intellectual property rights of public sector bodies, nor does it limit the exercise of these rights in any way beyond the boundaries set by this Directive. The obligations imposed by this Directive should apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (the Berne Convention) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement). Public sector bodies should, however, exercise their copyright in a way that facilitates re-use.

(23) Tools that help potential re-users to find documents available for re-use and the conditions for re-use can facilitate considerably the cross-border use of public sector documents. Member States should therefore ensure that practical arrangements are in place that help re-users in their search for documents available for re-use. Assets lists, accessible preferably online, of main documents (documents that are extensively re-used or that have the potential to be extensively re-used), and portal sites that are linked to decentralised assets lists are examples of such practical arrangements.

(24) This Directive is without prejudice to Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (10) and Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (11). It spells out the conditions within which public sector bodies can exercise their intellectual property rights in the internal information market when allowing re-use of documents.

(25) Since the objectives of the proposed action, namely to facilitate the creation of Community-wide information products and services based on public sector documents, to enhance an effective cross-border use of public sector documents by private companies for added-value information products and services and to limit distortions of competition on the Community market, cannot be sufficiently achieved by the Member States and can therefore, in view of the intrinsic

Community scope and impact of the said action, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives. This Directive should achieve minimum harmonisation, thereby avoiding further disparities between the Member States in dealing with the re-use of public sector documents,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive establishes a minimum set of rules governing the re-use and the practical means of facilitating re-use of existing documents held by public sector bodies of the Member States.

2. This Directive shall not apply to:

(a) documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or in the absence of such rules, as defined in line with common administrative practice in the Member State in question, provided that the scope of the public tasks is transparent and subject to review;

(b) documents for which third parties hold intellectual property rights;

(c) documents which are excluded from access by virtue of the access regimes in the Member States, including on the grounds of:

— the protection of national security (i.e. State security), defence, or public security,

— statistical confidentiality,

— commercial confidentiality (e.g. business, professional or company secrets);

(ca) documents access to which is restricted by virtue of the access regimes in the Member States, including cases whereby citizens or companies have to prove a particular interest to obtain access to documents;

(cb) parts of documents containing only logos, crests and insignia;

(cc) documents access to which is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data;

(d) documents held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit;

(e) documents held by educational and research establishments, including organisations established for the

transfer of research results, schools and universities, except university libraries and

(f) documents held by cultural establishments other than libraries, museums and archives.

3. This Directive builds on and is without prejudice to access regimes in the Member States.

4. This Directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law, and in particular does not alter the obligations and rights set out in Directive 95/46/EC.

5. The obligations imposed by this Directive shall apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention and the TRIPS Agreement.

Article 2

Definitions

For the purpose of this Directive the following definitions shall apply:

1. 'public sector body' means the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law;

2. 'body governed by public law' means any body:

(a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; and

(b) having legal personality; and

(c) financed, for the most part by the State, or regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law;

3. 'document' means:

(a) any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording);

(b) any part of such content;

4. 're-use' means the use by persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced. Exchange of documents between public sector bodies purely in pursuit of their public tasks does not constitute re-use;

5. 'personal data' means data as defined in Article 2(a) of Directive 95/46/EC.

6. 'machine-readable format' means a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure;

7. 'open format' means a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents;

8. 'formal open standard' means a standard which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability;

9. 'university' means any public sector body that provides post-secondary-school higher education leading to academic degrees.

Article 3

General principle

1. Subject to paragraph 2 Member States shall ensure that documents to which this Directive applies in accordance with Article 1 shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV.

2. For documents in which libraries, including university libraries, museums and archives hold intellectual property rights, Member States shall ensure that, where the re-use of such documents is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV.

CHAPTER II

REQUESTS FOR RE-USE

Article 4

Requirements applicable to the processing of requests for re-use

1. Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the time-frames laid down for the processing of requests for access to documents.

2. Where no time limits or other rules regulating the timely provision of documents have been established, public sector bodies shall process the request and shall deliver the documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a timeframe of not more than 20 working days after its receipt. This timeframe may be extended by another 20 working days for extensive or complex requests. In such cases the applicant shall be notified within three weeks after the initial request that more time is needed to process it.

3. In the event of a negative decision, the public sector bodies shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or of the national provisions adopted pursuant to this Directive, in particular points (a) to (cc) of Article 1(2) or Article 3. Where a negative decision is based on Article 1(2)(b), the public sector body shall include a reference to the natural or legal person who is the rightholder, where known, or alternatively to the licensor from which the public sector body has obtained the relevant material. Libraries, including university libraries, museums and archives shall not be required to include such a reference.

4. Any decision on re-use shall contain a reference to the means of redress in case the applicant wishes to appeal the decision. The means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the national access to documents authority or a national judicial authority, whose decisions are binding upon the public sector body concerned.

5. Public sector bodies covered under Article 1(2)(d), (e) and (f) shall not be required to comply with the requirements of this Article.

CHAPTER III

CONDITIONS FOR RE-USE

Article 5

Available formats

1. Public sector bodies shall make their documents available in any pre-existing format or language, and, where possible and appropriate, in open and machine-readable format together with their metadata. Both the format and the metadata should, in so far as possible, comply with formal open standards.

2. Paragraph 1 shall not imply an obligation for public sector bodies to create or adapt documents or provide extracts in order to comply with that paragraph where this would involve disproportionate effort, going beyond a simple operation.

3. On the basis of this Directive, public sector bodies cannot be required to continue the production and storage of a certain type of documents with a view to the re-use of such documents by a private or public sector organisation.

Article 6

Principles governing charging

1. Where charges are made for the re-use of documents, those charges shall be limited to the marginal costs incurred for their reproduction, provision and dissemination.

2. Paragraph 1 shall not apply to the following:

(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;

(b) by way of exception, documents for which the public sector body concerned is required to generate sufficient revenue to cover a substantial part of the costs relating to their collection, production, reproduction and dissemination. Those requirements shall be defined by law or by other binding rules in the Member State. In the absence of such rules, the requirements shall be defined in accordance with common administrative practice in the Member State;

(c) libraries, including university libraries, museums and archives.

3. In the cases referred to in points (a) and (b) of paragraph 2, the public sector bodies concerned shall calculate the total charges according to objective, transparent and verifiable criteria to be laid down by the Member States. The total income of those bodies from supplying and allowing re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment. Charges shall be calculated in line with the accounting principles applicable to the public sector bodies involved.

4. Where charges are made by the public sector bodies referred to in point (c) of paragraph 2, the total income from supplying and allowing re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, preservation and rights clearance, together with a reasonable return on investment. Charges shall be calculated in line with the

accounting principles applicable to the public sector bodies involved.

Article 7

Transparency

1. In the case of standard charges for the re-use of documents held by public sector bodies, any applicable conditions and the actual amount of those charges, including the calculation basis for such charges, shall be pre-established and published, through electronic means where possible and appropriate.

2. In the case of charges for the re-use other than those referred to in paragraph 1, the public sector body in question shall indicate at the outset which factors are taken into account in the calculation of those charges. Upon request, the public sector body in question shall also indicate the way in which such charges have been calculated in relation to the specific re-use request.

3. The requirements referred to in point (b) of Article 6(2) shall be pre-established. They shall be published by electronic means, where possible and appropriate.

4. Public sector bodies shall ensure that applicants for re-use of documents are informed of available means of redress relating to decisions or practices affecting them.

Article 8

Licences

1. Public sector bodies may allow re-use without conditions or may impose conditions, where appropriate through a licence. These conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.

2. In Member States where licences are used, Member States shall ensure that standard licences for the re-use of public sector documents, which can be adapted to meet particular licence applications, are available in digital format and can be processed electronically. Member States shall encourage all public sector bodies to use the standard licences.

Article 9

Practical arrangements

Member States shall make practical arrangements facilitating the search for documents available for re-use, such as asset lists of main documents with relevant metadata, accessible where possible and appropriate online and in machine-readable format, and portal sites that are linked to the asset lists. Where possible Member States shall facilitate the cross-linguistic search for documents.

CHAPTER IV

NON-DISCRIMINATION AND FAIR TRADING

Article 10

Non-discrimination

1. Any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use.

2. If documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the documents for those activities as apply to other users.

Article 11

Prohibition of exclusive arrangements

1. The re-use of documents shall be open to all potential actors in the market, even if one or more market players already exploit added-value products based on these documents. Contracts or other arrangements between the public sector bodies holding the documents and third parties shall not grant exclusive rights.

2. However, where an exclusive right is necessary for the provision of a service in the public interest, the validity of the reason for granting such an exclusive right shall be subject to regular review, and shall, in any event, be reviewed every three years. The exclusive arrangements established after the entry into force of this Directive shall be transparent and made public.

This paragraph shall not apply to digitisation of cultural resources.

2a. Notwithstanding paragraph 1, where an exclusive right relates to digitisation of cultural resources, the period of exclusivity shall in general not exceed 10 years. In case where that period exceeds 10 years, its duration shall be subject to review during the 11th year and, if applicable, every seven years thereafter.

The arrangements granting exclusive rights referred to in the first subparagraph shall be transparent and made public.

In the case of an exclusive right referred to in the first subparagraph, the public sector body concerned shall be provided free of charge with a copy of the digitised cultural resources as part of those arrangements. That copy shall be available for re-use at the end of the period of exclusivity.

3. Exclusive arrangements existing on 1 July 2005 that do not qualify for the exceptions under paragraph 2 shall be terminated at the end of the contract or in any event not later than 31 December 2008.

4. Without prejudice to paragraph 3, exclusive arrangements existing on 17 July 2013 that do not qualify for the exceptions under paragraphs 2 and 2a shall be terminated at the end of the contract or in any event not later than 18 July 2043.

CHAPTER V

FINAL PROVISIONS

Article 12

Implementation

Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive by 1 July 2005. They shall forthwith inform the Commission thereof.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

Article 13

Review

1. The Commission shall carry out a review of the application of this Directive before 18 July 2018 and shall communicate the results of that review, together with any proposals for

amendments to this Directive, to the European Parliament and the Council.

2. Member States shall submit a report every 3 years to the Commission on the availability of public sector information for re-use and the conditions under which it is made available and the redress practices. On the basis of that report, which shall be made public, Member States shall carry out a review of the implementation of Article 6, in particular as regards charging above marginal cost.

3. The review referred to in paragraph 1 shall in particular address the scope and impact of this Directive, including the extent of the increase in re-use of public sector documents, the effects of the principles applied to charging and the re-use of official texts of a legislative and administrative nature, the interaction between data protection rules and re-use possibilities, as well as further possibilities of improving the proper functioning of the internal market and the development of the European content industry.

Article 14

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Union.

Article 15

Addressees

This Directive is addressed to the Member States.

(1) OJ C 227 E, 24.9.2002, p. 382.

(2) OJ C 85, 8.4.2003, p. 25.

(3) OJ C 73, 26.3.2003, p. 38.

(4) Opinion of the European Parliament of 12 February 2003 (not yet published in the Official Journal), Council Common Position of 26 May 2003 (OJ C 159 E, 8.7.2003, p. 1) and Position of the European Parliament of 25 September 2003 (not yet published in the Official Journal). Council Decision of 27 October 2003.

(5) OJ L 209, 24.7.1992, p. 1. Directive as last amended by Commission Directive 2001/78/EC (OJ L 285, 29.10.2001, p. 1).

(6) OJ L 199, 9.8.1993, p. 1. Directive as last amended by Commission Directive 2001/78/EC.

(7) OJ L 199, 9.8.1993, p. 54. Directive as last amended by Commission Directive 2001/78/EC.

(8) OJ L 101, 1.4.1998, p. 1.

(9) OJ L 281, 23.11.1995, p. 31.

(10) OJ L 167, 22.6.2001, p. 10.

(11) OJ L 77, 27.3.1996, p. 20.

Relevant Case Law on Public Sector Information

C-343/95, Diego Cali & Figli Srl v. Servizi Ecologici Porto di Genova SpA (SEPG)

(...)

13 In the course of the proceedings contesting that order, the Tribunale di Genova stayed proceedings until the Court of Justice had given a preliminary ruling on the following questions:

1. Can a "dominant position within the common market or in a substantial part of it" be said to exist where a limited company, set up by a national port authority, is given responsibility for and does actually carry out, pursuant to an administrative concession from that authority, the task of providing, with exclusive rights within a harbour sector specializing in loading and unloading petroleum products, an "anti-pollution surveillance" service, and where that company collects the relevant fee, which is set unilaterally by the port authority on the basis of the vessel's tonnage and the quantity of the product loaded or unloaded, from users of that service, that is to say vessels which dock at the wharves to carry out those operations?

2. Having regard to the situation set out in Question 1 and if there is a dominant position within the common market or a substantial part of it, is there an abuse of the aforesaid "dominant position" within the meaning of Article 86 of the Treaty, in particular of subparagraphs (a), (c) and (d), and are there related practices, when an undertaking holding the exclusive concession for a service (even though on the basis of a decision of the authority granting the concession) charges fees:

- which are compulsory and independent of the provision of an efficient surveillance and/or intervention service, merely because a vessel berths in a mooring in the Porto Petroli and loads/unloads goods, whether petroleum products or chemicals and petrochemicals, according to the contractual terms imposed;

- the amount of which depends solely on the tonnage of the vessel, the amount of the product and also, in the event of any actual intervention, the duration thereof, but not on the product's nature, quality or capacity to pollute;

- which, since they are imposed exclusively on the vessel (which is merely passively loaded and unloaded), affect a subject other than those whose responsibility it is to carry out the necessary technical operations (in this case Porto Petroli di Genova SpA and the loaders/receivers of the product), resulting in an inevitable discrepancy between the responsibility for any pollution and the bearing of the cost of the anti-pollution service;

- which, given the nature of the product and/or its existence, represent an unnecessary service for vessels equipped with their own anti-pollution devices and systems adapted to the type of product to be loaded or unloaded;

- which impose on the vessel a charge, and an associated extra cost, in addition to those provided for by the landing contract between the carrier and the company operating the wharves, and have no practical connection with the subject-matter of the contract.

3. If, in the situations set out in Questions 1 and 2, there are one or more practices amounting to abuse of a dominant position by an undertaking for the purposes of Article 86 of the Treaty, does this lead to a potential adverse effect on trade between Member States of the Union?

(...)

Findings of the Court

135. Under the rules which govern procedure in cases before the Court of First Instance, parties are entitled to protection against the misuse of pleadings and evidence. Thus, in accordance with the third subparagraph of Article 5(3) of the Instructions to the Registrar of 3 March 1994 (O) 1994 L 78, p. 32), no third party, private or public, may have access to the case-file or to the procedural documents without the express authorisation of the President, after the parties have been heard. Moreover, in accordance with Article 116(2) of the Rules of Procedure, the President may exclude secret or confidential documents from those furnished to an intervener in a case.

136. These provisions reflect a general principle in the due administration of justice according to which parties have the right to defend their interests free from all external influences and particularly from influences on the part of members of the public.

137. It follows that a party who is granted access to the procedural documents of other parties is entitled to use those documents only for the purpose of pursuing his own case and for no other purpose, including that of inciting criticism on the part of the public in relation to arguments raised by other parties in the case.

138. In the present case, it is clear that the actions of the applicant in publishing an edited version of the defence on the Internet in conjunction with an invitation to the public to send their comments to the Agents of the Council and in providing the telephone and telefax numbers of those Agents, had as their purpose to bring pressure to bear upon the Council and to provoke public criticism of the Agents of the institution in the performance of their duties.

139. These actions on the part of the applicant involved an abuse of procedure which will be taken into account in awarding costs (see below, paragraph 140), having regard, in particular, to the fact that this incident led to a suspension of the proceedings and made it necessary for the parties in the case to lodge additional submissions in this respect.

(...)

On those grounds,

THE COURT OF FIRST INSTANCE (Fourth Chamber, Extended Composition) hereby:

1. Annuls the Council's decision of 6 July 1995 refusing the applicant access to certain documents relating to the European Police Office (Europol);
2. Orders the Council to pay two-thirds of the applicant's costs as well as its own costs;
3. Orders the Kingdom of Denmark, the French Republic, the Kingdom of the Netherlands, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland to bear their own costs.

Delivered in open court in Luxembourg on 17 June 1998.

C-7/13, Creditinfo Lánstraust hf. and Registers Iceland and the Icelandic State

(...)

13 The plaintiff is engaged in recording and communicating information on financial matters and creditworthiness, and related services. In the course of its business, it seeks information and data from public sector bodies, including the first defendant, Registers Iceland.

14 Between 2004 and 2007, the plaintiff entered into a series of contracts with the National Land Registry concerning access to information. In 2010, the National Land Registry merged with the National Registry to form Registers Iceland.

15 Registers Iceland has charged the plaintiff fees for the disclosure of information and data. The plaintiff has brought an action before the national court for the repayment of fees for the period between 11 January 2008 and 31 December 2011. Since the tariffs were approved by the Minister of Finance, the plaintiff also brings its action against the Icelandic State.

16 In its request, registered at the Court on 29 April 2013, Reykjavik District Court has referred the following questions:

1. Is it compatible with EEA law, and specifically with Article 6 of Council Directive 2003/98/EC, on the re-use of public sector information (cf. The Decision of the EEA Joint Committee, No 105/2005, amending Annex XI (Telecommunication services) to the EEA Agreement), to charge a fee on account of each mechanical enquiry for information from the register if no calculation of the 'total income' and the 'cost', in the sense of Article 6 of the Directive, is available at the time of the determination of the fee?

2. Is it compatible with Article 6 of the Directive if, when the 'cost' subject to Article 6 of the Directive is determined, no account is taken of:

a. income accruing to the State when documents are collected, in the form of fees paid by individuals and undertakings for the recording of contracts in the registers of legal deeds, and

b. income accruing to the State when documents are collected, in the form of taxes which are levied as stamp duties on recorded legal deeds at the time when individuals and undertakings apply to have them recorded in the registers of legal deeds?

3. Is it compatible with Article 6 of the Directive if, when the 'cost' pursuant to Article 6 of the Directive is determined, account is taken of costs incurred by a public sector body in connection with the collection of documents which it is legally obliged to collect, irrespective of whether or not individuals or undertakings request to re-use them?

4. Is it compatible with Article 6 of the Directive if, when the 'cost' pursuant to the article is determined, the legislature sets the amount of the fee in legislation without any particular amount being made subject to substantive examination?

5. Would it be compatible with Article 6 of the Directive if, when the 'cost' pursuant to the Directive is determined, appropriate account were taken of a general requirement in national legislation that public sector bodies be self-financing?

6. If the answer to Question No 5 is in the affirmative, what does this involve in further detail and what cost elements in public sector operations may be taken into account in this context?

(...)

33 Recital 5 of the preamble to the Directive states that public sector data are an important primary material for digital content products and services. European companies should be able to exploit their potential and contribute to economic growth and job creation.

34 Public sector information is a key resource for industry in the information society (see the Commission's Green Paper, COM(1998)585). A main goal of the European legislature was to put European firms on an equal footing with their American counterparts, which, since the enactment of the Freedom of Information Act in 1966, have benefited from a highly developed, efficient public information system at all levels of the administration. The Commission has highlighted that the US government's active policy of ensuring both access to and commercial exploitation of public sector information has greatly stimulated the development of the US information industry (see the Commission's Green Paper, cited above, p. 1).

35 According to its Article 1, the Directive establishes a minimum set of rules governing re-use and the practical means of facilitating the re-use of existing documents held by public sector bodies. In Article 2(4) of the Directive, re-use is defined as use for any commercial or non-commercial purpose other than the initial purpose within the public task for which the documents were produced.

36 It is clear from recital 9 of the preamble that, although the Directive does not contain any obligation to allow re-use, public sector bodies should be encouraged to make any documents held by them available for re-use.

37 Where re-use is authorised, and where charges are made for that purpose, it is an objective of the Directive, as set out in recital 14 of its preamble, to preclude excessive pricing. It must

be borne in mind in this context that the public bodies in question are normally monopolies.

38 Article 6 of the Directive therefore states that charges may not exceed the cost of collection, production, reproduction and dissemination of the documents in question, together with a reasonable return on investment.

39 Pricing is a crucial issue in relation to the exploitation of public sector information by the digital content industries. It largely determines whether they will find an interest in investing in value added products and services based on public sector information. American companies benefit from the fact that they can obtain US public sector information free of charge (the Commission's Green Paper, cited above, p. 14). If European companies are to be put on an equal footing with their competitors in other parts of the world, the cost elements and return on investment cannot be calculated in a way that would put them at a significant disadvantage. It is for the national court to assess the facts in that respect, in particular with regard to the relevant interest level. It must therefore take into account that Article 6 of the Directive does not aim to provide public sector bodies with a profit.

40 Moreover, pursuant to Article 7 of the Directive, standard charges for the re-use of documents shall be pre-established and published. The public sector body shall indicate the calculation basis for the published charge if requested to do so. This should be done in order to enable individuals and economic operators charged for re-use of public information to verify whether the charges in question are compatible with Article 6 of the Directive. The Directive does not require that the calculation basis be made available at the time when the charge is fixed. Nevertheless, the requirement that standard charges within the limit set by Article 6 shall be pre-established presupposes that a substantive examination has been undertaken at the time when the charge is fixed. This must apply irrespective of whether the charge is set in legislation, by the relevant public authority or by other means.

41 As pointed out by the Commission, if the factors relevant to performing a calculation are uncertain, the public body in question must at least make a reasonable estimate, for example in the form of the average cost of enabling re-use. If experience shows that the estimate was incorrect, and if that entails that set charges are incompatible with Article 6 of the Directive, the calculation must be adjusted accordingly.

It is for the national court to determine whether the methods used to calculate the charges relevant to the case before it, and the transparency of those methods, comply with the requirements of the Directive. However, the national court must keep in mind that the public sector body bears the burden of proof in this regard.

43 For the sake of completeness, the Court notes that individuals and economic operators are entitled to obtain repayment of charges levied in an EEA State in breach of EEA law provisions. That is a consequence of the rights conferred on them. The EEA State in question is therefore required, in principle, to repay charges levied in breach of EEA law (see, for comparison, most recently, C-191/12 Alakor, judgment of 16 May 2013, not yet reported, paragraphs 22 and 23, and case law cited).

44 An exception to the repayment obligation applies when repayment entails unjust enrichment. Repayment is not required if it is established that the person required to pay unlawful charges has actually passed them on to other persons (see, for comparison, Alakor, cited above, paragraph 25, and case law cited). Such an exception must however be interpreted restrictively (see, for comparison, most recently, C-398/09 Lady & Kid and Others [2011] ECR I-7375, paragraph 20).

45 It is for the domestic legal system of each EEA State to lay down the procedural rules governing such repayments. However, these rules must not be less favourable than those governing similar domestic actions (the principle of equivalence), and must not render practically impossible or excessively difficult the exercise of rights conferred by EEA law (the principle of effectiveness) (compare Alakor, cited above, paragraph 26, and case law cited). Consequently, the question

of whether a charge levied in violation of EEA law has or has not been passed on is a question of fact to be determined by the national court, taking all relevant circumstances into account.

46 Whether a charge levied in violation of EEA law is passed on, depends on the circumstances of the case, in particular the market structure. For example, a monopoly operator can be expected to pass on the entire charge. If there is competition, an operator may not be able to pass on any part of it (compare with regard to this conclusion the judgment by the Supreme Court of Norway of 28 May 2008 in case 2007/1738, Rt. 2008 p. 738, paragraph 52). Moreover, even where it is established that the charge has been passed on in whole or in part to customers, repayment does not necessarily entail unjust enrichment. The charged person may still suffer a loss, in particular as a result of a fall in the volume of his sales (see, for comparison, Lady & Kid and Others, cited above, paragraph 21, and case law cited).

47 As regards the specific situation where a charge for the re-use of public information set out in legislation has proven to be excessive, the court recalls that the national courts must apply the methods of interpretation recognised by national law as far as possible in order to achieve the result sought by the relevant EEA law rule (see, inter alia, Case E-7/11 Grund [2012] EFTA Ct. Rep. 191, paragraph 83, and case law cited).

48 The answer to the first and fourth questions must therefore be that Articles 6 and 7 of the Directive require that, when charges are made for the re-use of public sector information, a substantive examination must have been undertaken at the time when the charge was fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the charges need only be made available upon request. This applies irrespective of whether the charge is set in legislation, by the relevant public authority or by other means.

(...)

58 As mentioned above, Article 6 of the Directive provides that, where charges are made, they may not exceed the cost of collection, production, reproduction and dissemination of the documents in question, together with a reasonable return on investment.

59 It follows from the wording that cost within the meaning of this provision is not limited to the cost of facilitating re-use, that is, reproduction and dissemination. Account may be taken of the cost incurred by a public sector body in connection with the initial collection and production of the documents in question. This must apply irrespective of whether the public sector body was legally obliged to collect the documents, as the Directive makes no such distinction.

60 Recital 14 of the preamble emphasises that States should encourage public sector bodies to make documents available at charges that do not exceed the marginal cost of reproducing and disseminating them. It should also be kept in mind that the Directive has recently been amended by Directive 2013/37/EU. Once the amendment has entered into force, the main rule under the new Article 6 will be that the cost of collection and production cannot be taken into account.

61 However, under the Directive, if account is taken of cost incurred by a public sector body in connection with the initial collection and production of documents, any income accrued in that respect, for example fees or taxes such as stamp duties, which reduce or offset that cost, must also be taken into account. Consequently, the cost within the meaning of Article 6 must be construed as the net cost. If only the cost incurred as a result of collection were to be taken into account and not the income accrued in that connection, this would undermine the effectiveness of the Directive's objective of precluding excessive pricing.

62 It is for the national court to examine the facts of the case before it in order to determine the cost that may, on the basis of the above, be taken into consideration pursuant to Article 6.

63 The answer to the second and third questions must therefore be that, when the cost pursuant to Article 6 of the Directive is determined, account may be taken of the cost incurred by a public sector body in connection with the initial collection and production of the documents in question. In such case, any income accrued in that connection, for example fees or taxes such as stamp duties, which reduce or offset that cost, must also be taken into account.

(...)

70 Article 6 of the Directive provides that charges may not exceed the cost of collection, production, reproduction and dissemination of the documents in question, together with a reasonable return on investment, having due regard to any self-financing requirements of the public sector body concerned, as stated in recital 14 of the preamble to the Directive.

71 Accordingly, general or specific self-financing requirements for public sector bodies may be taken into account when determining the cost pursuant to Article 6 of the Directive. Nonetheless, as argued by both ESA and the Commission, the cost within the meaning of Article 6, together with a reasonable return on investment, must relate to the handling of documents, either their initial collection or production, or the actual facilitation of re-use through reproduction and dissemination. Consequently, when charges are made, cost elements and investments that are unrelated to the document processing necessary for re-use set out in Article 6 may not be taken into account. These principles governing charging in Article 6 must be the same irrespective of any self-financing requirement to which the public body in question is subject.

72 At the oral hearing, the defendants implied, in response to a question put to them, that the charges for re-use in dispute in the case before the national court are also used to cover the cost of services that the plaintiff itself has not received from Registers Iceland. If it is established that the charges are used to cover cost other than that related to the collection, production, reproduction and dissemination of the documents in question, together with a reasonable return on investment in the facilitation of re-use, those charges are contrary to Article 6. It is for the national court to make the assessment.

73 The answer to the fifth and sixth questions must therefore be that self-financing requirements for public sector bodies may be taken into account when determining the cost under Article 6 of the Directive. This applies insofar as only cost elements, together with a reasonable return on investment, that are related to the document processing necessary for re-use set out in Article 6 are taken into account.

(...)

On those grounds, THE COURT in answer to the questions referred to it by Héraðsdómur Reykjavíkur hereby gives the following Advisory Opinion:

1. Articles 6 and 7 of Directive 2003/98/EC require that, when charges are made for the re-use of public sector information, a substantive examination must have been undertaken at the time when the charge is fixed. The examination must show that the total income from such charges does not exceed the cost of collection, production, reproduction and dissemination of documents, plus a reasonable return on investment. If the factors relevant to performing a calculation are uncertain, an estimate must at least be made. However, the calculation basis for the charges need only be made available upon request. This applies irrespective of whether the charge is set in legislation, by the relevant public authority or by other means.

2. When the cost pursuant to Article 6 of the Directive is determined, account may be taken of the cost incurred by a public sector body in connection with the initial collection and production of the documents in question. In such case, any income accrued in that respect, for example fees or taxes such as stamp duties, which reduce or offset that cost, must also be taken into account.

3. Self-financing requirements for public sector bodies may be taken into account when determining the cost under Article 6 of the Directive. This applies insofar as only cost elements,

together with a reasonable return on investment, that are related to the document processing necessary for re-use set out in Article 6 are taken into account.

Delivered in open court in Luxembourg on 16 December 2013.

C-117/13, Technische Universität Darmstadt v Eugen Ulmer KG

10 TU Darmstadt operates a regional and academic library in which it installed electronic reading points that allow the public to consult works contained in the collection of that library.

11 Since January or February 2009, those works have included the textbook of Schulze W., *Einführung in die neuere Geschichte* ('the textbook at issue'), published by Ulmer, a scientific publishing house established in Stuttgart (Germany).

12 TU Darmstadt did not take up Ulmer's offer of 29 January 2009 of an opportunity to purchase and use the textbooks it publishes as electronic books ('e-books'), including the textbook at issue.

13 TU Darmstadt digitised that textbook so as to make it available to users on electronic reading points installed in its library. Those points did not allow for a greater number of copies of that work to be consulted at any one time than the number owned by the library. Users of the reading points could print out the work on paper or store it on a USB stick, in part or in full, and take it out of the library in that form.

14 In an action brought by Ulmer, the Landgericht (Regional Court) Frankfurt am Main held, by judgment of 6 March 2011, that the rightholder and establishment must have reached prior agreement on the digital use of the work concerned for Paragraph 52b of the UrhG not to apply. That court also rejected Ulmer's application seeking to prohibit TU Darmstadt from digitising the textbook at issue or having it digitised. However, it granted that company's request to prohibit users of the TU Darmstadt library from being able, at electronic reading points installed therein, to print out that work and/or store it on a USB stick and/or take such reproductions out of the library.

15 Hearing an appeal by TU Darmstadt on a point of law, the Bundesgerichtshof (Federal Court of Justice) considers, in the first place, that the question arises whether works and other protected objects are 'subject to purchase or licensing terms', within the meaning of Article 5(3)(n) of Directive 2001/29, where the rightholder offers to conclude with an establishment referred to in that provision appropriately worded licensing agreements in respect of those works or whether a different interpretation of that provision must be adopted, in terms of which only cases where the owner and the establishment have entered into an agreement on that matter are covered.

16 That court takes the view that, unlike the German language version of the provision, the English and French language versions are consistent with the first of the above interpretations. That interpretation could also be justified on the basis of the purpose and general scheme of Directive 2001/29. However, if only the entering into an agreement would allow for the application of that provision to be ruled out, it would be open to the establishment to refuse an appropriate offer from the rightholder so as to benefit from the limiting provision in question, which would also mean that the owner would not receive appropriate remuneration, which nevertheless is one of the objectives of that Directive.

17 In the second place, the referring court is uncertain whether Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it allows Member States to confer on the establishments referred to in that provision the right to digitise the works contained in their collections to the extent that the communication or making available of those works on their terminals requires such reproduction. The referring court takes the view that Member States should have an ancillary competence in order to provide for such an exception to the reproduction right referred to in Article 2 of that Directive or such a limitation of that right; otherwise the effectiveness of Article 5(3)(n) would not be guaranteed. That competence

could, in any event, be inferred from Article 5(2)(c) of the Directive.

18 In the third place, the referring court takes the view that the dispute in the main proceedings raises the question whether, pursuant to Article 5(3)(n) of Directive 2001/29, Member States may provide for a limiting provision permitting the users of an establishment referred to in that provision to print out on paper or store on a USB stick, in part or in full, the works reproduced or made available by the establishment on its terminals.

19 In that regard, that court considers, first of all, that while those printouts, stored copies or downloads, being related to the reproduction of a work, are not, in principle, covered by the limitation provided for in Article 5(3)(n) of Directive 2001/29, they could nevertheless be permitted, as an extension of the communication or of the making available of a work by the establishment in question, under another limitation, in particular, pursuant to the so-called 'private copying' exception provided for in Article 5(2)(b) of that Directive.

20 Next, the court finds that the objective referred to in Article 5(3)(n) of Directive 2001/29, which entails permitting the efficient use, for the purpose of research or private study, of texts communicated or made available on the terminals of an establishment such as a library, is consistent with an interpretation of that provision to the effect that the printing out on paper of a work from a terminal should be permitted, whereas storage on a USB stick should not be.

21 Lastly, the referring court considers that such an interpretation of Article 5(3)(n) of Directive 2001/29 would also ensure that the scope of the limitation provided for in that provision respects the threefold condition provided for in Article 5(5) of that Directive. In its view, storage of a work on a USB stick encroaches upon the rights of the author of that work more than printing it out on paper.

22 In those circumstances, the Bundesgerichtshof decided to stay the proceedings and refer the following questions to the Court for a preliminary ruling:

'(1) Is a work subject to purchase or licensing terms, within the meaning of Article 5(3)(n) of Directive 2001/29, where the rightholder offers to conclude with the establishments referred to therein licensing agreements for the use of that work on appropriate terms?

(2) Does Article 5(3)(n) of Directive 2001/29 entitle the Member States to confer on those establishments the right to digitise the works contained in their collections, if that is necessary in order to make those works available on terminals?

(3) May the rights which the Member States lay down pursuant to Article 5(3)(n) of Directive 2001/29 go so far as to enable users of the terminals to print out on paper or store on a USB stick the works made available there?

23 By its first question, the referring court is essentially asking whether a work is subject to 'purchase or licensing terms', within the meaning of Article 5(3)(n) of Directive 2001/29, where the rightholder has offered to conclude with an establishment referred to in that provision, such as a publicly accessible library, on appropriately worded terms a licensing agreement in respect of that work.

24 All of the interested parties that have presented written observations, with the exception of Ulmer, propose that the first question be answered in the negative and essentially support an interpretation to the effect that the concept of 'purchase or licensing terms', mentioned in Article 5(3)(n) of Directive 2001/29, must be understood to mean that the rightholder and establishment concerned must have concluded a licensing agreement in respect of the work in question that sets out the conditions in which that establishment may use the work.

25 Ulmer argues that the mere fact that the rightholder offers to conclude a licensing agreement with a publicly accessible library is sufficient for ruling out the application of Article 5(3)(n) of Directive 2001/29, provided always that such offer is 'appropriate'.

26 In that regard, first of all, a comparison of the language versions of Article 5(3)(n) of Directive 2001/29, particularly the English, French, German and Spanish versions — which use the words 'terms', 'conditions', 'Regelung' and 'condiciones', respectively — shows that, in that provision, the EU legislature used the concepts 'terms' or 'provisions', which refer to contractual terms actually agreed as opposed to mere contractual offers.

27 Next, it should be recalled that the limitation under Article 5(3)(n) of Directive 2001/29 aims to promote the public interest in promoting research and private study, through the dissemination of knowledge, which constitutes, moreover, the core mission of publicly accessible libraries.

28 The interpretation favoured by Ulmer implies that the rightholder could, by means of a unilateral and essentially discretionary action, deny the establishment concerned the right to benefit from that limitation and thereby prevent it from realising its core mission and promoting the public interest.

29 Moreover, recital 40 in the preamble to Directive 2001/29 states that specific contracts or licences should be promoted which, without creating imbalances, favour such establishments and the disseminative purposes they serve.

30 As noted by the Advocate General in points 21 and 22 of his Opinion, recitals 45 and 51 in the preamble to Directive 2001/29 confirm (including in their German version) that, in the context, *inter alia*, of the exceptions and limitations listed in Article 5(3) of Directive 2001/29, it is existing contractual relations and the conclusion and implementation of existing contractual agreements that are at issue, and not mere prospects of contracts or licences.

31 Furthermore, the interpretation proposed by Ulmer is difficult to reconcile with the aim pursued by Article 5(3)(n) of Directive 2001/29, which is to maintain a fair balance between the rights and interests of rightholders, on the one hand, and, on the other hand, users of protected works who wish to communicate them to the public for the purpose of research or private study undertaken by individual members of the public.

32 In addition, if the mere act of offering to conclude a licensing agreement were sufficient to rule out the application of Article 5(3)(n) of Directive 2001/29, such an interpretation would be liable to negate much of the substance of the limitation provided for in that provision, or indeed its effectiveness, since, were it to be accepted, the limitation would apply, as Ulmer has maintained, only to those increasingly rare works of which an electronic version, primarily in the form of an e-book, is not yet offered on the market.

33 Lastly, the interpretation to the effect that there must be contractual terms actually agreed also cannot be ruled out — contrary to what is maintained by Ulmer — by reason of the fact that it would conflict with the threefold condition provided for in Article 5(5) of Directive 2001/29.

34 In that regard, it is sufficient to state that the limitation provided for in Article 5(3)(n) of Directive 2001/29 is accompanied by a number of restrictions that guarantee — even though the application of that provision is ruled out only in the event that contractual terms have actually been concluded — the continuing applicability of such a limitation in special cases which do not conflict with a normal exploitation of the works and do not unreasonably prejudice the legitimate interests of the rightholder.

35 In the light of the foregoing considerations, the answer to the first question is that the concept of 'purchase or licensing terms' provided for in Article 5(3)(n) of Directive 2001/29 must be understood as requiring that the rightholder and an establishment, such as a publicly accessible library, referred to in that provision must have concluded a licensing agreement in respect of the work in question that sets out the conditions in which that establishment may use that work.

The second question

36 By its second question, the referring court is essentially asking whether Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it precludes Member States from granting to publicly accessible libraries covered by that

provision the right to digitise the works contained in their collections, if such act of reproduction is necessary for the purpose of making those works available to users, by means of dedicated terminals, within those establishments.

37 The first point to be noted is that the digitisation of a work, which essentially involves the conversion of the work from an analogue format into a digital one, constitutes an act of reproduction of the work.

38 The question therefore arises whether Article 5(3)(n) of Directive 2001/29 permits Member States to grant that reproduction right to publicly accessible libraries, since, under Article 2 of that Directive, it is the authors that have the exclusive right to authorise or prohibit the reproduction of their works.

39 In that regard, it should first be stated that, according to the first sentence of Article 5(3) of Directive 2001/29, the exceptions and limitations set out in that paragraph relate to the rights provided for in Articles 2 and 3 of that Directive and thus both the exclusive reproduction right enjoyed by the rightholder and the right of communication to the public of works.

40 However, Article 5(3)(n) of the Directive limits the use of works, within the meaning of that provision, to the 'communication or making available' of those works and thus to acts which fall under the sole exclusive right of communication to the public of works referred to in Article 3 of that Directive.

41 Next, it should be recalled that for there to be an 'act of communication' for the purposes of Article 3(1) of Directive 2001/29, it is sufficient, in particular, that those works are made available to a public in such a way that the persons forming that public may access them, irrespective of whether they avail themselves of that opportunity (judgment in *Svensson and Others*, C-466/12, EU:C:2014:76, paragraph 19).

42 It follows that, in circumstances such as those of the case in the main proceedings, where an establishment, such as a publicly accessible library, which falls within Article 5(3)(n) of Directive 2001/29, gives access to a work contained in its collection to a 'public', namely all of the individual members of the public using the dedicated terminals installed on its premises for the purpose of research or private study, that must be considered to be 'making [that work] available' and, therefore, an 'act of communication' for the purposes of Article 3(1) of that Directive (see, to that effect, judgment in *Svensson and Others*, EU:C:2014:76, paragraph 20).

43 Such a right of communication of works enjoyed by establishments such as publicly accessible libraries covered by Article 5(3)(n) of Directive 2001/29, within the limits of the conditions provided for by that provision, would risk being rendered largely meaningless, or indeed ineffective, if those establishments did not have an ancillary right to digitise the works in question.

44 Those establishments are recognised as having such a right pursuant to Article 5(2)(c) of Directive 2001/29, provided that 'specific acts of reproduction' are involved.

45 That condition of specificity must be understood as meaning that, as a general rule, the establishments in question may not digitise their entire collections.

46 However, that condition is, in principle, observed where the digitisation of some of the works of a collection is necessary for the purpose of the 'use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals', as provided in Article 5(3)(n) of Directive 2001/29.

47 Furthermore, the scope of that ancillary right of digitisation must be determined by interpreting Article 5(2)(c) of Directive 2001/29 in the light of Article 5(5) of that Directive, under which that limitation is applicable only in certain special cases which do not prejudice the normal exploitation of the work or other protected object or cause unjustified harm to the legitimate interests of the rightholder, the latter provision, however, not being intended to extend the scope of the exceptions and limitations provided for in Article 5(2) of the

Directive (see, to that effect, judgments in *Infopaq International*, C-5/08, EU:C:2009:465, paragraph 58, and *ACI Adam and Others*, C-435/12, EU:C:2014:254, paragraph 26).

48 In the present case, it must be stated that the applicable national legislation takes due account of the conditions provided for in Article 5(5) of the Directive, since it follows, first, from Article 52b of the *UrhG*, that the digitisation of works by publicly accessible libraries cannot have the result of the number of copies of each work made available to users by dedicated terminals being greater than that which those libraries have acquired in analogue format. Secondly, although, by virtue of that provision of national law, the digitisation of the work is not, as such, coupled with an obligation to provide compensation, the subsequent making available of that work in digital format, on dedicated terminals, gives rise to a duty to make payment of adequate remuneration.

49 Having regard to the foregoing considerations, the answer to the second question is that Article 5(3)(n) of Directive 2001/29, read in conjunction with Article 5(2)(c) of that Directive, must be interpreted to mean that it does not preclude Member States from granting to publicly accessible libraries covered by those provisions the right to digitise the works contained in their collections, if such act of reproduction is necessary for the purpose of making those works available to users, by means of dedicated terminals, within those establishments.

The third question

50 By its third question, the referring court is essentially asking whether Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it precludes Member States from granting to publicly accessible libraries covered by that provision the right to make works available to users by dedicated terminals which permit the printing out of those works on paper or their storage on a USB stick.

51 As is clear from paragraphs 40 and 42 of the present judgment, the limitation laid down in Article 5(3)(n) of Directive 2001/29 covers, in principle, only certain acts of communication normally falling under the exclusive right of the author provided for in Article 3 of that Directive, namely those by which the establishments in question make a work available to individual members of the public, for the purpose of research or private study, by dedicated terminals installed on their premises.

52 It is undisputed that acts such as the printing out of a work on paper or its storage on a USB stick, even if made possible by the specific features of the dedicated terminals on which that work can be consulted, are not acts of 'communication', within the meaning of Article 3 of that Directive 2001/29, but rather of 'reproduction', within the meaning of Article 2 of that Directive.

53 What is involved is the creation of a new analogue or digital copy of the work that an establishment makes available to users by means of dedicated terminals.

54 Such acts of reproduction, unlike some operations involving the digitisation of a work, also cannot be permitted under an ancillary right stemming from the combined provisions of Articles 5(2)(c) and 5(3)(n) of Directive 2001/29, since they are not necessary for the purpose of making the work available to the users of that work, by dedicated terminals, in accordance with the conditions laid down by those provisions. Moreover, since those acts are carried out not by the establishments referred to in Article 5(3)(n) of Directive 2001/29, but rather by the users of the dedicated terminals installed within those establishments, they cannot be authorised under that provision.

55 By contrast, such acts of reproduction on analogue or digital media may, if appropriate, be authorised under the national legislation transposing the exceptions or limitations provided for in Article 5(2)(a) or (b) of Directive 2001/29 since, in each individual case, the conditions laid down by those provisions, in particular as regards the fair compensation which the rightholder must receive, are met.

56 Furthermore, such acts of reproduction must observe the conditions set out in Article 5(5) of Directive 2001/29.

Consequently, the extent of the texts reproduced may not, in particular, unreasonably prejudice the legitimate interests of the rightholder.

57 Having regard to the foregoing considerations, the answer to the third question is that Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it does not extend to acts such as the printing out of works on paper or their storage on a USB stick, carried out by users from dedicated terminals installed in publicly accessible libraries covered by that provision. However, such acts may, if appropriate, be authorised under national legislation transposing the exceptions or limitations provided for in Article 5(2)(a) or (b) of that Directive provided that, in each individual case, the conditions laid down by those provisions are met.

(...)

On those grounds, the Court (Fourth Chamber) hereby rules:

1. The concept of 'purchase or licensing terms' provided for in Article 5(3)(n) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be understood as requiring that the rightholder and an establishment, such as a publicly

accessible library, referred to in that provision must have concluded a licensing agreement in respect of the work in question that sets out the conditions in which that establishment may use that work.

2. Article 5(3)(n) of Directive 2001/29, read in conjunction with Article 5(2)(c) of that Directive, must be interpreted to mean that it does not preclude Member States from granting to publicly accessible libraries covered by those provisions the right to digitise the works contained in their collections, if such act of reproduction is necessary for the purpose of making those works available to users, by means of dedicated terminals, within those establishments.

3. Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it does not extend to acts such as the printing out of works on paper or their storage on a USB stick, carried out by users from dedicated terminals installed in publicly accessible libraries covered by that provision. However, such acts may, if appropriate, be authorised under national legislation transposing the exceptions or limitations provided for in Article 5(2)(a) or (b) of that Directive provided that, in each individual case, the conditions laid down by those provisions are met.

V.ISP Liability

Convention on Information and Legal Co-operation concerning "Information Society Services"

Preamble

The Parties to this Convention, signatories hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Noting the continued development of information and communication technology and the numerous national initiatives and their impact at a European and international level;

Recognising the cross-border nature of interactive services that are diffused on-line by new means of electronic communication and their growing importance in facilitating the economic, social and cultural progress of the Council of Europe member States;

Recalling the system established by the legislation of the European Community for the exchange of the texts of draft domestic Regulations concerning "Information Society Services";

Noting the need for all Council of Europe member States to be kept regularly informed of legislative developments on "Information Society Services" at a Pan-European level and, where necessary, to have the possibility to discuss and exchange information and ideas regarding these developments;

Agreeing on the desirability to provide a legal framework to enable member States of the Council of Europe to exchange, where practicable by electronic means, texts of draft domestic Regulations aimed specifically at "Information Society Services";

Have agreed as follows:

Article 1 – Object and scope of application

1 In accordance with the provisions of this Convention, the Parties shall exchange texts, where practicable by electronic means, of draft domestic Regulations aimed specifically at "Information Society Services" and shall co-operate in the functioning of the information and legal co-operation system set up under the Convention.

2 This Convention shall not apply:

a to domestic Regulations which are exempted from prior notification by virtue of European Community legislation (hereinafter referred to as "Community law"), or
b where a notification has to be made to comply with other international agreements.

3 This Convention shall not apply :

a to radio broadcasting services;
b to television programme services covered by the European Convention on Transfrontier Television, opened for signature in Strasbourg on 5 May 1989 (ETS No. 132), as amended by the Protocol of 1 October 1998 (ETS No. 171);

c to domestic Regulations relating to matters which are covered by European Community legislation or international agreements in the fields of telecommunications services and financial services.

Article 2 – Definitions

For the purposes of this Convention :

a "Information Society Services" means any service, normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;

b "domestic Regulations" means legal texts concerning the compliance with requirements of a general nature relating to the taking up and pursuit of service activities within the meaning of paragraph a of this article, in particular provisions concerning the service provider, the services and the recipient of services, excluding any rules which are not specifically aimed at the Information Society Services.

Article 3 – Receiving and transmitting authorities

Each Party shall designate an authority that is in charge of transmitting and receiving, where practicable by electronic means, draft domestic Regulations aimed specifically at "Information Society Services" as well as any other documents pertaining to the functioning of the present Convention.

Article 4 – Procedure

1 Each Party shall transmit, where practicable by electronic means, to the Secretary General of the Council of Europe the texts of draft domestic Regulations which are aimed specifically at "Information Society Services" and which are at a stage of preparation in which it is still possible for them to be substantially amended, as well as a short summary of these texts in English or French. The Parties shall communicate the draft again under the above conditions if they make changes to the draft that have the effect of significantly altering its scope, shortening the timetable originally envisaged for implementation, adding specifications or requirements, or making the latter more restrictive.

2 Upon receipt of the texts of the draft domestic Regulations and summaries under paragraph 1 above or paragraph 6 below, the Secretary General of the Council of Europe shall transmit them, where practicable by electronic means, to the authority of each Party.

3 Upon receipt of the texts and summaries under paragraph 2 above, each Party may transmit, where practicable by electronic means, observations on the texts of the draft domestic Regulations in English or French to the Secretary General of the Council of Europe and to the Party concerned.

4 A Party receiving the observations under paragraph 3 above shall endeavour to take them into account as far as possible when preparing new domestic Regulations.

5 Paragraphs 1 to 4 above shall not apply :

a in cases where, for urgent reasons, occasioned by serious and unforeseeable circumstances relating to the protection of public health or safety, the protection of animals or the preservation of plants, and public policy, notably the protection of minors, a Party is obliged to prepare technical Regulations in a very short space of time in order to enact and introduce them immediately without any consultations being possible;

b in cases where for urgent reasons occasioned by serious circumstances relating to the protection of the security and the

integrity of the financial system, notably the protection of depositors, investors and insured persons, a Party is obliged to enact and to implement rules on financial services immediately;

in the cases mentioned in sub-paragraphs a and b, the Party shall give reasons to the Secretary General of the Council of Europe for the urgency of the measures in question;
c to domestic Regulations enacted by or for regulated markets or by or for other markets or bodies carrying out clearing or settlement functions for those markets.

6 Each Party which finalises any domestic Regulations aimed specifically at "Information Society Services" shall transmit the definitive text to the Secretary General of the Council of Europe without delay and where practicable by electronic means.

7 Upon receipt of the texts of the adopted domestic Regulations under paragraph 6 above, the Secretary General of the Council of Europe shall make them available, where practicable by electronic means, and shall keep this information in a single database within the Council of Europe.

Article 5 – Declarations

The authorities referred to in Article 3 shall be designated by means of a declaration addressed to the Secretary General of the Council of Europe when the State concerned or the European Community becomes a Party to the present Convention in accordance with the provisions of Articles 8 and 9. Any change shall likewise be declared to the Secretary General of the Council of Europe.

Article 6 – Relationship to other instruments and agreements

1 This Convention shall not affect any international instrument which is binding on the Parties and which contains provisions on matters governed by this Convention.

2 The European Community shall equally fulfil the obligation to notify the texts transmitted to it by its member States in pursuance of the provisions of paragraph 1 of Article 4, and shall transmit to them the observations received by the other Parties, in pursuance of the provisions of paragraph 3 of Article 4.

Article 7 – Amendments to Article 1 of the Convention concerning excluded matters

1 Any amendment to Article 1, paragraph 3 of this Convention proposed by a Party shall be communicated to the Secretary General of the Council of Europe who shall forward the communication to the European Committee on Legal Cooperation (CDCJ).

2 The proposed amendment shall be examined by the Parties, which may adopt it by a two-thirds majority of the votes cast. The text adopted shall be forwarded to the Parties. The European Community shall have the same number of votes as the number of its member States.

3 On the first day of the month following the expiration of a period of four months after its adoption by the Parties, unless the Parties have notified objections by one-third of the votes cast, any amendment shall enter into force for those Parties which have not notified objection.

4 A Party which has notified an objection in pursuance of the provisions of paragraph 3 of Article 7 may subsequently withdraw it in whole or in part. Such withdrawal shall be made by means of a notification addressed to the Secretary General of the Council of Europe and shall become effective as from the date of its receipt.

Article 8 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe, the non-member States which have participated in its elaboration and the European Community. Such States and the European Community may express their consent to be bound by:

- a signature without reservation as to ratification, acceptance or approval, or
- b signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2 Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five signatories, of which at least one is not a member State of the European Economic Area, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraph 1.

4 In respect of any signatory which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of their consent to be bound by the Convention in accordance with the provisions of paragraph 2.

Article 9 – Accession to the Convention

1 After the entry into force of the present Convention, the Committee of Ministers of the Council of Europe, after consulting the Parties to the Convention, may invite any non-member State of the Council which has not participated in its elaboration to accede to this Convention, by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Parties entitled to sit on the Committee.

2 In respect of any State acceding to it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 10 – Reservations

No reservation may be made in respect of any provision of this Convention.

Article 11 – Territorial application

1 Any State or the European Community may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any Party may, at any later date, by declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory or territories specified in the declaration and for whose international relations it is responsible or on whose behalf it is authorised to give undertakings. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3 Any declaration made in pursuance of the preceding paragraph may, in respect of any territory mentioned in such declaration, be withdrawn by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the first day of the month following the expiration of a period of three months after the date of receipt by the Secretary General of the Council of Europe of the notification.

Article 12 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 13 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council and any other signatories and Parties to this Convention of:

- a any signature;
- b the deposit of any instrument of ratification, acceptance, approval or accession;

c any declaration made in pursuance of the provisions of Article 5;
d any notification received in pursuance of the provisions of Article 7;
e any date of entry into force of this Convention, in accordance with Articles 8, 9 and 11;

f any declaration received in pursuance of the provisions of paragraphs 2 and 3 of Article 11;
g any notification received in pursuance of the provision of paragraph 1 of Article 12;
h any other act, notification or communication relating to this Convention.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

CHAPTER I GENERAL PROVISIONS

Article 1 Objective and scope

1. This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.
2. This Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.
3. This Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.
4. This Directive does not establish additional rules on private international law nor does it deal with the jurisdiction of Courts.
5. This Directive shall not apply to:
(a) the field of taxation;
(b) questions relating to information society services covered by Directives 95/46/EC and 97/66/EC;
(c) questions relating to agreements or practices governed by cartel law;
(d) the following activities of information society services:
- the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority,
- the representation of a client and defence of his interests before the courts,
- gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.
6. This Directive does not affect measures taken at Community or national level, in the respect of Community law, in order to promote cultural and linguistic diversity and to ensure the defence of pluralism.

Article 2 Definitions

For the purpose of this Directive, the following terms shall bear the following meanings:

(a) "information society services": services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC;
(b) "service provider": any natural or legal person providing an information society service;
(c) "established service provider": a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide

the service do not, in themselves, constitute an establishment of the provider;

(d) "recipient of the service": any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible;

(e) "consumer": any natural person who is acting for purposes which are outside his or her trade, business or profession;

(f) "commercial communication": any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession. The following do not in themselves constitute commercial communications:

- information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address,

- communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration;

(g) "regulated profession": any profession within the meaning of either Article 1(d) of Council Directive 89/48/EEC of 21 December 1988 on a general system for the recognition of higher-education diplomas awarded on completion of professional education and training of at least three-years' duration(26) or of Article 1(f) of Council Directive 92/51/EEC of 18 June 1992 on a second general system for the recognition of professional education and training to supplement Directive 89/48/EEC(27);

(h) "coordinated field": requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.

(i) The coordinated field concerns requirements with which the service provider has to comply in respect of:

- the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification,

- the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider;

(ii) The coordinated field does not cover requirements such as:
- requirements applicable to goods as such,
- requirements applicable to the delivery of goods,
- requirements applicable to services not provided by electronic means.

Section 4: Liability of intermediary service providers

Article 12 "Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access

to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

- (a) does not initiate the transmission;
- (b) does not select the receiver of the transmission; and
- (c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13 "Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

- (a) the provider does not modify the information;
- (b) the provider complies with conditions on access to the information;
- (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
- (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an

administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14 Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

- (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Relevant Case law concerning Directive 2000/31/EC

C-324/09, L'Oréal SA and others v. eBay International AG and others

26 L'Oréal is a manufacturer and supplier of perfumes, cosmetics and hair-care products. In the United Kingdom it is the proprietor of a number of national trade marks. It is also the proprietor of Community trade marks.

27 L'Oréal operates a closed selective distribution network, in which authorised distributors are restrained from supplying products to other distributors.

28 eBay operates an electronic marketplace on which are displayed listings of goods offered for sale by persons who have registered for that purpose with eBay and have created a seller's account with it. eBay charges a percentage fee on completed transactions.

29 eBay enables prospective buyers to bid for items offered by sellers. It also allows items to be sold without an auction, and thus for a fixed price, by means of a system known as 'Buy It Now'. Sellers can also set up online shops on eBay sites. An online shop lists all the items offered for sale by one seller at a given time.

30 Sellers and buyers must accept eBay's online-market user agreement. One of the terms of that agreement is a prohibition on selling counterfeit items and on infringing trade marks.

31 In some cases eBay assists sellers in order to enhance their offers for sale, to set up online shops, to promote and increase their sales. It also advertises some of the products sold on its marketplace using search engine operators such as Google to trigger the display of advertisements.

32 On 22 May 2007, L'Oréal sent eBay a letter expressing its concerns about the widespread incidence of transactions infringing its intellectual property rights on eBay's European websites.

33 L'Oréal was not satisfied with the response it received and brought actions against eBay in various Member States, including an action before the High Court of Justice (England & Wales), Chancery Division.

34 L'Oréal's action before the High Court of Justice sought a ruling, first, that eBay and the individual defendants are liable for sales of 17 items made by those individuals through the website www.ebay.co.uk, L'Oréal claiming that those sales infringed the rights conferred on it by, inter alia, the figurative

Community trade mark including the words 'Amor Amor' and the national word mark 'Lancôme'.

35 It is common ground between L'Oréal and eBay that two of those 17 items are counterfeits of goods bearing L'Oréal trade marks.

36 Although L'Oréal does not claim that the other 15 items are counterfeits, it none the less considers that the sale of the items infringing its trade mark rights, since those items were either goods that were not intended for sale (such as tester or dramming products) or goods bearing L'Oréal trade marks intended for sale in North America and not in the European Economic Area ('EEA'). Furthermore, some of the items were sold without packaging.

37 Whilst refraining from ruling at this stage on the question as to the extent to which L'Oréal's trade mark rights have been infringed, the High Court of Justice has confirmed that the individual defendants made the sales described by L'Oréal on the website www.ebay.co.uk.

38 Second, L'Oréal submits that eBay is liable for the use of L'Oréal trade marks where those marks are displayed on eBay's website and where sponsored links triggered by the use of keywords corresponding to the trade marks are displayed on the websites of search engine operators, such as Google.

39 Concerning the last point, it is not disputed that eBay, by choosing keywords corresponding to L'Oréal trade marks in Google's 'Ad Words' referencing service, caused to be displayed, each time that there was a match between a keyword and the word entered in Google's search engine by an internet user, a sponsored link to the site www.ebay.co.uk. That link would appear in the 'sponsored links' section displayed on either the right-hand side, or on the upper part, of the screen displayed by Google.

40 Thus, on 27 March 2007, when an internet user entered the words 'shu uemura' – which in essence coincide with L'Oréal's national word mark 'Shu Uemura' – as a search string in the Google search engine, the following eBay advertisement was displayed in the 'sponsored links' section:

'Shu Uemura Great deals on Shu uemura Shop on eBay and Save! www.ebay.co.uk'.

41 Clicking on that sponsored link led to a page on the www.ebay.co.uk website which showed '96 items found for shu uemura'. Most of those items were expressly stated to be from Hong Kong.

42 Similarly, taking one of the other examples, when, on 27 March 2007, an internet user entered the words 'matrix hair', which correspond in part to L'Oréal's national word mark 'Matrix', as a search string in the Google search engine, the following eBay listing was displayed as a 'sponsored link':

'Matrix hair Fantastic low prices here Feed your passion on eBay.co.uk! www.ebay.co.uk'.

43 Third, L'Oréal has claimed that, even if eBay was not liable for the infringements of its trade mark rights, it should be granted an injunction against eBay by virtue of Article 11 of Directive 2004/48.

44 L'Oréal reached a settlement with some of the individual defendants (Mr Potts, Ms Ratchford, Ms Ormsby, Mr Clarke and Ms Clarke) and obtained judgment in default against the others (Mr Fox and Ms Bi). Subsequently, in March 2009, a hearing dealing with the action against eBay was held before the High Court of Justice.

45 By judgment of 22 May 2009, the High Court of Justice made a number of findings of fact and concluded that the state of the proceedings did not permit final judgment in the case, as a number of questions of law first required an interpretation from the Court of Justice of the European Union.

46 In its judgment, the High Court of Justice notes that eBay has installed filters in order to detect listings which might contravene the conditions of use of the site. That court also notes that eBay has developed, using a programme called 'VeRO' (Verified Rights Owner), a notice and take-down system that is intended to provide intellectual property owners with assistance in removing infringing listings from the marketplace. L'Oréal has declined to participate in the VeRO programme, contending that the programme is unsatisfactory.

47 The High Court of Justice has also stated that eBay applies sanctions, such as the temporary – or even permanent – suspension of sellers who have contravened the conditions of use of the online marketplace.

48 Despite the findings set out above, the High Court of Justice took the view that eBay could do more to reduce the number of sales on its online marketplace which infringe intellectual property rights. According to that court, eBay could use additional filters. It could also include in its rules a prohibition on selling, without the consent of the trade mark proprietors, trade-marked goods originating from outside the EEA. It could also impose additional restrictions on the volumes of products that can be listed at any one time and apply sanctions more rigorously.

49 The High Court of Justice states, however, that the fact that it would be possible for eBay to do more does not necessarily mean that it is legally obliged to do so.

50 By decision of 16 July 2009, which follows on from the judgment of 22 May 2009, the High Court of Justice decided to stay the proceedings and refer the following questions to the Court for a preliminary ruling:

(1) Where perfume and cosmetic testers (i.e. samples for use in demonstrating products to consumers in retail outlets) and dramming bottles (i.e. containers from which small aliquots can be taken for supply to consumers as free samples) which are not intended for sale to consumers (and are often marked "not for sale" or "not for individual sale") are supplied without charge to the trade mark proprietor's authorised distributors, are such goods "put on the market" within the meaning of Article 7(1) of [Directive 89/104] and Article 13(1) of [Regulation No 40/94]?

(2) Where the boxes (or other outer packaging) have been removed from perfumes and cosmetics without the consent of the trade mark proprietor, does this constitute a "legitimate reason" for the trade mark proprietor to oppose further commercialisation of the unboxed products within the meaning of Article 7(2) of [Directive 89/104] and Article 13(2) of [Regulation No 40/94]?

(3) Does it make a difference to the answer to question 2 above if:

(a) as a result of the removal of the boxes (or other outer packaging), the unboxed products do not bear the information required by Article 6(1) of [Directive 76/768], and in particular do not bear a list of ingredients or a "best before date"?

(b) as a result of the absence of such information, the offer for sale or sale of the unboxed products constitutes a criminal offence according to the law of the Member State of the Community in which they are offered for sale or sold by third parties?

(4) Does it make a difference to the answer to question 2 above if the further commercialisation damages, or is likely to damage, the image of the goods and hence the reputation of the trade mark? If so, is that effect to be presumed, or is it required to be proved by the trade mark proprietor?

(5) Where a trader which operates an online marketplace purchases the use of a sign which is identical to a registered trade mark as a keyword from a search engine operator so that the sign is displayed to a user by the search engine in a sponsored link to the website of the operator of the online marketplace, does the display of the sign in the sponsored link constitute "use" of the sign within the meaning of Article 5(1)(a) of [Directive 89/104] and Article 9(1)(a) of [Regulation No 40/94]?

(6) Where clicking on the sponsored link referred to in question 5 above leads the user directly to advertisements or offers for sale of goods identical to those for which the trade mark is registered under the sign placed on the website by other parties, some of which infringe the trade mark and some [of] which do not infringe the trade mark by virtue of the differing statuses of the respective goods, does that constitute use of the sign by the operator of the online marketplace "in relation to" the infringing goods within the meaning of 5(1)(a) of [Directive 89/104] and Article 9(1)(a) of [Regulation No 40/94]?

(7) Where the goods advertised and offered for sale on the website referred to in question 6 above include goods which have not been put on the market within the EEA by or with the consent of the trade mark proprietor, is it sufficient for such use to fall within the scope of Article 5(1)(a) of [Directive 89/104] and Article 9(1)(a) of [Regulation No 40/94] and outside Article 7(1) of [Directive 89/104] and Article 13(1) of [Regulation No 40/94] that the advertisement or offer for sale is targeted at consumers in the territory covered by the trade mark or must the trade mark proprietor show that the advertisement or offer for sale necessarily entails putting the goods in question on the market within the territory covered by the trade mark?

(8) Does it make any difference to the answers to questions 5 to 7 above if the use complained of by the trade mark proprietor consists of the display of the sign on the web site of the operator of the online marketplace itself rather than in a sponsored link?

(9) If it is sufficient for such use to fall within the scope of Article 5(1)(a) of [Directive 89/104] and Article 9(1)(a) of [Regulation No 40/94] and outside Article 7 ... of [Directive 89/104] and Article 13 ... of [Regulation No 40/94] that the advertisement or offer for sale is targeted at consumers in the territory covered by the trade mark:

(a) does such use consist of or include "the storage of information provided by a recipient of the service" within the meaning of Article 14(1) of [Directive 2000/31]?

(b) if the use does not consist exclusively of activities falling within the scope of Article 14(1) of [Directive 2000/31], but includes such activities, is the operator of the online marketplace exempted from liability to the extent that the use consists of such activities and if so may damages or other financial remedies be granted in respect of such use to the extent that it is not exempted from liability?

(c) in circumstances where the operator of the online marketplace has knowledge that goods have been advertised, offered for sale and sold on its website in infringement of registered trade marks, and that infringements of such registered trade marks are likely to continue to occur through the advertisement, offer for sale and sale of the same or similar goods by the same or different users of the website, does this constitute "actual knowledge" or "awareness" within the meaning of Article 14(1) of [Directive 2000/31]?

(10) Where the services of an intermediary such as an operator of a website have been used by a third party to infringe a registered trade mark, does Article 11 of [Directive 2004/48] require Member States to ensure that the trade mark proprietor can obtain an injunction against the intermediary to prevent further infringements of the said trade mark, as opposed to continuation of that specific act of infringement, and if so what is the scope of the injunction that shall be made available?

(...)

On those grounds, the Court (Grand Chamber) hereby rules:

1. Where goods located in a third State, which bear a trade mark registered in a Member State of the European Union or a Community trade mark and have not previously been put on the market in the European Economic Area or, in the case of a Community trade mark, in the European Union, (i) are sold by an economic operator on an online marketplace without the consent of the trade mark proprietor to a consumer located in the territory covered by the trade mark or (ii) are offered for sale or advertised on such a marketplace targeted at consumers located in that territory, the trade mark proprietor may prevent that sale, offer for sale or advertising by virtue of the rules set out in Article 5 of First Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks, as amended by the Agreement on the European Economic Area of 2 May 1992, or in Article 9 of Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark. It is the task of the national courts to assess on a case-by-case basis whether relevant factors exist, on the basis of which it may be concluded that an offer for sale or an advertisement displayed on an online marketplace

accessible from the territory covered by the trade mark is targeted at consumers in that territory.

2. Where the proprietor of a trade mark supplies to its authorised distributors items bearing that mark, intended for demonstration to consumers in authorised retail outlets, and bottles bearing the mark from which small quantities can be taken for supply to consumers as free samples, those goods, in the absence of any evidence to the contrary, are not put on the market within the meaning of Directive 89/104 and Regulation No 40/94.

3. Article 5 of Directive 89/104 and Article 9 of Regulation No 40/94 must be interpreted as meaning that the proprietor of a trade mark may, by virtue of the exclusive right conferred by the mark, oppose the resale of goods such as those at issue in the main proceedings, on the ground that the person reselling the goods has removed their packaging, where the consequence of that removal is that essential information, such as information relating to the identity of the manufacturer or the person responsible for marketing the cosmetic product, is missing. Where the removal of the packaging has not resulted in the absence of that information, the trade mark proprietor may nevertheless oppose the resale of an unboxed perfume or cosmetic product bearing his trade mark, if he establishes that the removal of the packaging has damaged the image of the product and, hence, the reputation of the trade mark.

4. On a proper construction of Article 5(1)(a) of Directive 89/104 and Article 9(1)(a) of Regulation No 40/94, the proprietor of a trade mark is entitled to prevent an online marketplace operator from advertising – on the basis of a keyword which is identical to his trade mark and which has been selected in an internet referencing service by that operator – goods bearing that trade mark which are offered for sale on the marketplace, where the advertising does not enable reasonably well-informed and reasonably observant internet users, or enables them only with difficulty, to ascertain whether the goods concerned originate from the proprietor of the trade mark or from an undertaking economically linked to that proprietor or, on the contrary, originate from a third party.

5. The operator of an online marketplace does not 'use' – for the purposes of Article 5 of Directive 89/104 or Article 9 of Regulation No 40/94 – signs identical with or similar to trade marks which appear in offers for sale displayed on its site.

6. Article 14(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') must be interpreted as applying to the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored. The operator plays such a role when it provides assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them. Where the operator of the online marketplace has not played an active role within the meaning of the preceding paragraph and the service provided falls, as a consequence, within the scope of Article 14(1) of Directive 2000/31, the operator none the less cannot, in a case which may result in an order to pay damages, rely on the exemption from liability provided for in that provision if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of Directive 2000/31.

7. The third sentence of Article 11 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights must be interpreted as requiring the Member States to ensure that the national courts with jurisdiction in relation to the protection of intellectual property rights are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements

of that kind. Those injunctions must be effective, proportionate, and dissuasive and must not create barriers to legitimate trade. Joined Cases C-236/08 to C-238/08: Google France SARL, Google Inc. vs. Louis Vuitton Malletier SA (C-236/08), Google France SARL vs. Viaticum SA, Luteciel SARL (C-237/08), and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08)

1. An internet referencing service provider that stores, as a keyword, a sign identical to a trade mark and organises the display of advertisements on the basis of that keyword does not use that sign within the meaning of Article 5(1) and (2) of Directive 89/104 relating to trade marks or of Article 9(1) of Regulation No 40/94 on the Community trade mark.

It is common ground that the referencing service provider carries on a commercial activity with a view to economic advantage when it stores as keywords, for certain of its clients, signs which are identical with trade marks and arranges for the display of 'ads' on the basis of those keywords.

It is also common ground that that service is not supplied only to the proprietors of those trade marks or to operators entitled to market their goods or services, but is provided without the consent of the proprietors and is supplied to their competitors or to imitators.

Although it is clear from those factors that the referencing service provider operates 'in the course of trade' when it permits advertisers to select, as keywords, signs identical to trade marks, stores those signs and displays its clients' 'ads' on the basis thereof, it does not follow, however, from those factors that that service provider itself 'uses' those signs within the terms of Article 5 of Directive 89/104 and Article 9 of Regulation No 40/94.

The use, by a third party, of a sign identical or similar to the proprietor's trade mark implies, at the very least, that that third party uses the sign in its own commercial communication. A referencing service provider allows its clients to use signs identical or similar to trade marks, without itself using those signs.

That conclusion cannot be called into question by the fact that the service provider is paid by its clients for the use of those signs. The fact of creating the technical conditions necessary for the use of a sign and being paid for that service does not mean that the party offering the service itself uses the sign.

2. The use as a keyword by the advertiser of a sign identical to the trade mark of a competitor in an internet referencing service in order that internet users may become aware, not only of the goods or services offered by that competitor, but also of those of the advertiser, constitutes a use in relation to the goods or services of that advertiser.

In addition, even in cases in which the advertiser does not seek, by its use, as a keyword, of a sign identical to the trade mark, to present its goods or services to internet users as an alternative to the goods or services of the proprietor of the trade mark but, on the contrary, seeks to mislead internet users as to the origin of its goods or services by making them believe that they originate from the proprietor of the trade mark or from an undertaking economically connected to it, there is use 'in relation to goods or services'. Such use exists in any event when the third party uses the sign identical to the trade mark in such a way that a link is established between that sign and the goods marketed or the services provided by the third party.

It follows that use by an advertiser of a sign identical with a trade mark as a keyword in the context of an internet referencing service falls within the concept of use 'in relation to goods or services' within the meaning of Article 5(1)(a) of Directive 89/104 relating to trade marks.

3. Article 5(1)(a) of Directive 89/104 relating to trade marks and Article 9(1)(a) of Regulation No 40/94 on the Community trade mark must be interpreted as meaning that the proprietor of a trade mark is entitled to prohibit an advertiser from advertising, on the basis of a keyword identical to that trade mark which that advertiser has, without the consent of the

proprietor, selected in connection with an internet referencing service, goods or services identical to those for which that mark is registered, when that advertisement does not enable an average internet user, or enables that user only with difficulty, to ascertain whether the goods or services referred to therein originate from the proprietor of the trade mark or an undertaking economically connected to it or, on the contrary, originate from a third party.

In such a situation, which is, moreover, characterised by the fact that the 'ad' in question appears immediately after entry of the trade mark as a search term by the internet user concerned and is displayed at a point when the trade mark is, in its capacity as a search term, also displayed on the screen, the internet user may err as to the origin of the goods or services in question. In those circumstances, the use by the third party of the sign identical to the mark as a keyword triggering the display of that 'ad' is liable to create the impression that there is a material link in the course of trade between the goods or services in question and the proprietor of the trade mark.

Having regard to the essential function of a trade mark, which, in the area of electronic commerce, consists in particular in enabling internet users browsing the 'ads' displayed in response to a search relating to a specific trade mark to distinguish the goods or services of the proprietor of that mark from those that have a different origin, that proprietor must be entitled to prohibit the display of third-party 'ads' that internet users may erroneously perceive as emanating from that proprietor.

It is for the national court to assess, on a case-by-case basis, whether the facts of the dispute before it indicate adverse effects, or a risk thereof, on the function of indicating origin.

When a third party's 'ad' suggests that there is an economic link between that third party and the proprietor of the trade mark, the conclusion must be that there is an adverse effect on the function of indicating origin.

When the 'ad', while not suggesting the existence of an economic link, is to such an extent vague as to the origin of the goods or services at issue that normally informed and reasonably attentive internet users are unable to determine, on the basis of the advertising link and the commercial message attached thereto, whether the advertiser is a third party vis-à-vis the proprietor of the trade mark or, on the contrary, economically linked to that proprietor, the conclusion must also be that there is an adverse effect on that function of the trade mark.

4. Since the course of trade provides a varied offer of goods and services, the proprietor of a trade mark may have not only the objective of indicating, by means of that mark, the origin of its goods or services, but also that of using its mark for advertising purposes designed to inform and persuade consumers.

Accordingly, the proprietor of a trade mark is entitled to prohibit a third party from using, without the proprietor's consent, a sign identical with its trade mark in relation to goods or services which are identical to those for which that trade mark is registered, when that use adversely affects the proprietor's use of its mark as a factor in sales promotion or as an instrument of commercial strategy.

With regard to the use by internet advertisers of a sign identical to another person's trade mark as a keyword for the purposes of displaying advertising messages, it is clear that that use is liable to have certain repercussions on the advertising use of that mark by its proprietor and on the latter's commercial strategy.

Having regard to the important position which internet advertising occupies in trade and commerce, it is plausible that the proprietor of a trade mark may register its own trade mark as a keyword with a referencing service provider in order to have an 'ad' appear under the heading 'sponsored links'. Where that is the case, the proprietor of the mark must, as necessary, agree to pay a higher price per click than certain other economic operators if it wishes to ensure that its 'ad' appears before those of those operators which have also selected its mark as a keyword. Furthermore, even if the proprietor of the mark is prepared to pay a higher price per click than that

offered by third parties that have also selected that trade mark, the proprietor cannot be certain that its 'ad' will appear before those of those third parties, given that other factors are also taken into account in determining the order in which the ads are displayed.

Nevertheless, those repercussions of use by third parties of a sign identical with the trade mark do not of themselves constitute an adverse effect on the advertising function of the trade mark.

5. Article 14 of Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') must be interpreted as meaning that the rule laid down therein applies to an internet referencing service provider when that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned.

It is for the national court to examine whether the role played by an internet referencing service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores.

C-314/12 UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH.

11 Having established that a website was offering, without their agreement, either a download or 'streaming' of some of the films which they had produced, Constantin Film and Wega, two film production companies, referred the matter to the court responsible for hearing applications for interim measures with a view to obtaining, on the basis of Article 81(1a) of the UrhG, an order enjoining UPC Telekabel, an internet service provider, to block the access of its customers to the website at issue, inasmuch as that site makes available to the public, without their consent, cinematographic works over which they hold a right related to copyright.

12 By order of 13 May 2011, the Handelsgericht Wien (Commercial Court, Vienna) (Austria) prohibited UPC Telekabel from providing its customers with access to the website at issue; that prohibition was to be carried out in particular by blocking that site's domain name and current IP ('Internet Protocol') address and any other IP address of that site of which UPC Telekabel might be aware.

13 In June 2011, the website at issue ceased its activity following an action of the German police forces against its operators.

14 By order of 27 October 2011, the Oberlandesgericht Wien (Higher Regional Court, Vienna) (Austria), as an appeal court, partially reversed the order of the court of first instance in so far as it had wrongly specified the means that UPC Telekabel had to introduce in order to block the website at issue and thus execute the injunction. In order to reach that conclusion, the Oberlandesgericht Wien first of all held that Article 81(1a) of the UrhG must be interpreted in the light of Article 8(3) of Directive 2001/29. It then held that, by giving its customers access to content illegally placed online, UPC Telekabel had to be regarded as an intermediary whose services were used to infringe a right related to copyright, with the result that Constantin Film and Wega were entitled to request that an injunction be issued against UPC Telekabel. However, as regards the protection of copyright, the Oberlandesgericht Wien held that UPC Telekabel could only be required, in the form of an obligation to achieve a particular result, to forbid its customers access to the website at issue, but that it had to remain free to decide the means to be used.

15 UPC Telekabel appealed on a point of law to the Oberster Gerichtshof (Supreme Court) (Austria).

16 In support of its appeal, UPC Telekabel submits inter alia that its services could not be considered to be used to infringe a copyright or related right within the meaning of Article 8(3) of Directive 2001/29 because it did not have any business relationship with the operators of the website at issue and it was not established that its own customers acted unlawfully. In any event, UPC Telekabel claims that the various blocking measures which may be introduced can all be technically circumvented and that some of them are excessively costly.

17 In those circumstances, the Oberster Gerichtshof decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'1. Is Article 8(3) of Directive 2001/29 ... to be interpreted as meaning that a person who makes protected subject-matter available on the internet without the rightholder's consent [for the purpose of Article 3(2) of Directive 2001/29] is using the services of the [internet] access providers of persons seeking access to that protected subject-matter?

If the answer to the first question is in the negative:

2. Are reproduction for private use [within the meaning of Article 5(2)(b) of Directive 2001/29] and transient and incidental reproduction [within the meaning of Article 5(1) of Directive 2001/29] permissible only if the original of the reproduction was lawfully reproduced, distributed or made available to the public?

If the answer to the first question or the second question is in the affirmative and an injunction is therefore to be issued against the user's [internet] access provider in accordance with Article 8(3) of [Directive 2001/29]:

3. Is it compatible with Union law, in particular with the necessary balance between the parties' fundamental rights, to prohibit in general terms an [internet] access provider from allowing its customers access to a certain website (thus without ordering specific measures) as long as the material available on that website is provided exclusively or predominantly without the rightholder's consent, if the access provider can avoid incurring coercive penalties for breach of the prohibition by showing that it had nevertheless taken all reasonable measures?

If the answer to the third question is in the negative:

4. Is it compatible with Union law, in particular with the necessary balance between the parties' fundamental rights, to require an [internet] access provider to take specific measures to make it more difficult for its customers to access a website containing material that is made available unlawfully if those measures require not inconsiderable costs and can easily be circumvented without any special technical knowledge?' (...)

66 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Fourth Chamber) hereby rules:

1. Article 8(3) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that a person who makes protected subject-matter available to the public on a website without the agreement of the rightholder, for the purpose of Article 3(2) of that Directive, is using the services of the internet service provider of the persons accessing that subject-matter, which must be regarded as an intermediary within the meaning of Article 8(3) of Directive 2001/29.

2. The fundamental rights recognised by EU law must be interpreted as not precluding a court injunction prohibiting an internet service provider from allowing its customers access to a website placing protected subject-matter online without the

agreement of the rightholders when that injunction does not specify the measures which that access provider must take and when that access provider can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures, provided that (i) the measures taken do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that those measures have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right, that being a matter for the national authorities and courts to establish.

Case of Delfi AS v. Estonia (ECHR Application No. 64569/09, Grand Chamber)

11. The applicant company is the owner of Delfi, an Internet news portal that published up to 330 news articles a day at the time of the lodging of the application. Delfi is one of the largest news portals on the Internet in Estonia. It publishes news in Estonian and Russian in Estonia and also operates in Latvia and Lithuania.

12. At the material time, at the end of the body of the news articles there were the words “add your comment” and fields for comments, the commenter’s name and his or her e-mail address (optional). Below these fields there were buttons labelled “publish the comment” and “read comments”. The part for reading comments left by others was a separate area which could be accessed by clicking on the “read comments” button. The comments were uploaded automatically and were, as such, not edited or moderated by the applicant company. The articles received about 10,000 readers’ comments daily, the majority posted under pseudonyms.

13. Nevertheless, there was a system of notice-and-take-down in place: any reader could mark a comment as leim (an Estonian word for an insulting or mocking message or a message inciting hatred on the Internet) and the comment was removed expeditiously. Furthermore, there was a system of automatic deletion of comments that included certain stems of obscene words. In addition, a victim of a defamatory comment could directly notify the applicant company, in which case the comment was removed immediately.

14. The applicant company had made efforts to advise users that the comments did not reflect its own opinion and that the authors of comments were responsible for their content. On Delfi’s Internet site there were “Rules of comment” which included the following:

“The Delfi message board is a technical medium allowing users to publish comments. Delfi does not edit comments. An author of a comment is liable for his or her comment. It is worth noting that there have been cases in the Estonian courts where authors have been punished for the contents of a comment ... Delfi prohibits comments whose content does not comply with good practice.

These are comments that:

- contain threats;
- contain insults;
- incite hostility and violence;
- incite illegal activities ...
- contain off-topic links, spam or advertisements;
- are without substance and/or off-topic;
- contain obscene expressions and vulgarities ...

Delfi has the right to remove such comments and restrict their authors’ access to the writing of comments ...”

The functioning of the notice-and-take-down system was also explained in the “Rules of comment”.

15. The Government submitted that in Estonia Delfi had a notorious history of publishing defamatory and degrading comments. Thus, on 22 September 2005 the weekly newspaper Eesti Ekspress had published an open letter from its editorial board to the Minister of Justice, the Chief Public Prosecutor and

the Chancellor of Justice in which concern was expressed about incessant taunting of people on public websites in Estonia. Delfi was named as a source of brutal and arrogant mockery. The addressees of the public letter responded to it in the 29 September 2005 edition of Eesti Ekspress. The Minister of Justice emphasised that the insulted persons had the right to defend their honour and reputation in court by bringing a suit against Delfi and claiming damages. The Chief Public Prosecutor referred to the legal grounds which made threats, incitement to social hatred, and sexual abuse of minors punishable under criminal law, and noted that liability for defamation and insults was dealt with under civil procedure. The Chancellor of Justice referred to the legal provisions designed to ensure the freedom of expression as well as the protection of everyone’s honour and good name, including sections 1043 and 1046 of the Obligations Act (Võlaõigusseadus).

16. On 24 January 2006 the applicant company published an article on the Delfi portal under the heading “SLK Destroyed Planned Ice Road”. Ice roads are public roads over the frozen sea which are open between the Estonian mainland and some islands in winter. The abbreviation “SLK” stands for AS Saaremaa Laevakompanii (Saaremaa Shipping Company, a public limited liability company). SLK provides a public ferry transport service between the mainland and certain islands. L. was a member of the supervisory board of SLK and the company’s sole or majority shareholder at the material time.

17. On 24 and 25 January 2006 the article attracted 185 comments. About twenty of them contained personal threats and offensive language directed against L.

18. On 9 March 2006 L.’s lawyers requested the applicant company to remove the offensive comments and claimed 500,000 Estonian kroons (EEK) (approximately 32,000 euros (EUR)) in compensation for non-pecuniary damage. The request concerned the following twenty comments:

“1. (1) there are currents in [V]äinameri

(2) open water is closer to the places you referred to, and the ice is thinner.

Proposal – let’s do as in 1905, let’s go to [K]uressaare with sticks and put [L.] and [Le.] in a bag

2. bloody shitheads...

they bathe in money anyway thanks to that monopoly and State subsidies and have now started to fear that cars may drive to the islands for a couple of days without anything filling their purses. burn in your own ship, sick Jew!

3. good that [La.’s] initiative has not broken down the lines of the web flammers. go ahead, guys, [L.] into the oven!

4. [little L.] go and drown yourself

5. aha... [I] hardly believe that that happened by accident... assholes fck

6. rascal!!! [in Russian]

7. What are you whining for, knock this bastard down once and for all [.] In future the other ones ... will know what they risk, even they will only have one little life.

8. ... is goddamn right. Lynching, to warn the other [islanders] and would-be men. Then nothing like that will be done again! In any event, [L.] very much deserves that, doesn’t he.

9. “a good man lives a long time, a shitty man a day or two”

10. If there was an iceroad, [one] could easily save 500 for a full car, fckng [L.] pay for that economy, why does it take 3 [hours] for your ferries if they are such good icebreakers, go and break ice in Pärnu port ... instead, fcking monkey, I will cross [the strait] anyway and if I drown, it’s your fault

11. and can’t anyone defy these shits?

12. inhabitants of Saaremaa and Hiiumaa islands, do 1:0 to this dope.

13. wonder whether [L.] won’t be knocked down in Saaremaa? screwing one’s own folk like that.

14. The people will chatter for a couple of days on the Internet, but the crooks (and also those who are backed and whom we ourselves have elected to represent us) pocket the money and pay no attention to this flaming – no one gives a shit about this. Once [M.] and other big crooks also used to boss around, but their greed struck back (RIP). Will also strike back for these

crooks sooner or later. As they sow, so shall they reap, but they should nevertheless be contained (by lynching as the state is powerless towards them – it is really them who govern the state), because they only live for today. Tomorrow, the flood.

15. this [V.] will one day get hit with a cake by me.

damn, as soon as you put a cauldron on the fire and there is smoke rising from the chimney of the sauna, the crows from Saaremaa are there – thinking that ... a pig is going to be slaughtered. no way

16. bastards!!!! Ofelia also has an ice class, so this is no excuse why Ola was required!!!

17. Estonian state, led by scum [and] financed by scum, of course does not prevent or punish antisocial acts by scum. But well, every [L.] has his Michaelmas ... and this cannot at all be compared to a ram's Michaelmas. Actually sorry for [L.] – a human, after all... :D :D :D

18. ... if after such acts [L.] should all of a sudden happen to be on sick leave and also next time the ice road is destroyed ... will he [then] dare to act like a pig for the third time? :)

19. fucking bastard, that [L.]... could have gone home with my baby soon ... anyway his company cannot guarantee a normal ferry service and the prices are such that ... real creep ... a question arises whose pockets and mouths he has filled up with money so that he's acting like a pig from year to year

20. you can't make bread from shit; and paper and internet can stand everything; and just for my own fun (really the state and [L.] do not care about the people's opinion) ... just for fun, with no greed for money – I pee into [L.'s] ear and then I also shit onto his head. :)"

19. On the same day, that is about six weeks after their publication, the offensive comments were removed by the applicant company.

20. On 23 March 2006 the applicant company responded to the request from L.'s lawyers. It informed L. that the comments had been removed under the notice-and-take-down obligation, and refused the claim for damages.

(...)

43. Following the Supreme Court's judgment of 10 June 2009 in the case giving rise to the present case before the Court (case no. 3-2-1-43-09), several lower courts have resolved the issue of liability in respect of comments relating to online news articles in a similar manner. Thus, in a judgment of 21 February 2012 the Tallinn Court of Appeal (case no. 2 08 76058) upheld a lower court's judgment concerning a defamed person's claim against a publisher of a newspaper. The publisher was found liable for defamatory online comments posted by readers in the newspaper's online commenting environment. The courts found that the publisher was a content service provider. They rejected the publisher's request for a preliminary ruling from the Court of Justice of the European Union (CJEU), finding that it was evident that the defendant did not satisfy the criteria for a passive service provider as previously interpreted by the CJEU and the Supreme Court and that the relevant rules were sufficiently clear. Therefore, no new directions from the CJEU were needed. The courts also noted that pursuant to the judgment of 23 March 2010 of the CJEU (Joined Cases C 236/08 to C 238/08 Google France and Google [2010] ECR I 2417) it was for the national courts to assess whether the role played by a service provider was neutral, in the sense that its conduct was merely technical, automatic and passive, pointing to a lack of knowledge of or control over the data which it stored. The courts considered that this was not the case in the matter before them. As the publisher had already deleted the defamatory comments by the time of the delivery of the judgment, no ruling was made on that issue; the plaintiff's claim in respect of non-pecuniary damage was dismissed. A similar judgment was handed down by the Tallinn Court of Appeal on 27 June 2013 (case no. 2-10-46710). In that case as well, an Internet news portal was held liable for defamatory comments posted by readers and the plaintiff's claim in respect of non-pecuniary damage was dismissed.

(...)

61. In its judgment of 10 October 2013 the Chamber noted at the outset that the parties' views diverged as to the applicant company's role in the present case. According to the Government, the applicant company was to be considered the discloser of the defamatory comments, whereas the applicant company was of the opinion that its freedom to impart information created and published by third parties was at stake, and that the applicant company itself was not a publisher of the third-party comments. The Chamber did not proceed to determine the exact role to be attributed to the applicant company's activities and noted that it was not, in substance, in dispute between the parties that the domestic courts' decisions in respect of the applicant company constituted an interference with its freedom of expression guaranteed under Article 10 of the Convention.

62. As regards the lawfulness of the interference, the Chamber rejected the applicant company's argument that the interference with its freedom of expression was not "prescribed by law". The Chamber observed that the domestic courts had found that the applicant company's activities did not fall within the scope of the Directive on Electronic Commerce and the Information Society Services Act. It considered that it was not its task to take the place of the domestic courts and that it was primarily for the national authorities, notably the courts, to resolve problems of interpretation of domestic legislation. The Chamber was furthermore satisfied that the relevant provisions of the civil law – although they were quite general and lacked detail in comparison with, for example, the Information Society Services Act – along with the relevant case-law, made it clear that a media publisher was liable for any defamatory statements made in its publication. The Chamber had regard to the fact that the applicant company was a professional publisher which operated one of the largest news portals in Estonia, and also that a degree of notoriety had been attributable to comments posted in its commenting area. Against that background, the Chamber considered that the applicant company had been in a position to assess the risks related to its activities and that it must have been able to foresee, to a reasonable degree, the consequences which these could entail.

63. The Chamber further found that the restriction of the applicant company's freedom of expression had pursued the legitimate aim of protecting the reputation and rights of others. In the Chamber's view, the fact that the actual authors of the comments were also in principle liable did not remove the legitimate aim of holding the applicant company liable for any damage to the reputation and rights of others.

64. As regards the proportionality of the interference, the Chamber noted that there was no dispute that the comments in question had been of a defamatory nature. In assessing the proportionality of the interference with the applicant company's freedom of expression, the Chamber had regard to the following elements. Firstly, it examined the context of the comments, secondly, the measures applied by the applicant company in order to prevent or remove defamatory comments, thirdly, the liability of the actual authors of the comments as an alternative to the applicant company's liability, and fourthly, the consequences of the domestic proceedings for the applicant company.

65. In particular, the Chamber considered that the news article published by the applicant company that had given rise to the defamatory comments had concerned a matter of public interest and the applicant company could have foreseen the negative reactions and exercised a degree of caution in order to avoid being held liable for damaging the reputation of others. However, the prior automatic filtering and notice-and-take-down system used by the applicant company had not ensured sufficient protection for the rights of third parties. Moreover, publishing news articles and making readers' comments on them public had been part of the applicant company's professional activities and its advertising revenue depended on the number of readers and comments. The applicant company

had been able to exercise a substantial degree of control over readers' comments and it had been in a position to predict the nature of the comments a particular article was liable to prompt and to take technical or manual measures to prevent defamatory statements from being made public. Furthermore, there had been no realistic opportunity of bringing a civil claim against the actual authors of the comments as their identity could not be easily established. In any event, the Chamber was not convinced that measures allowing an injured party to bring a claim only against the authors of defamatory comments would have guaranteed effective protection of the injured parties' right to respect for their private life. It had been the applicant company's choice to allow comments by non-registered users, and by doing so it had to be considered to have assumed a certain responsibility for such comments. For all the above reasons, and considering the moderate amount of damages the applicant company had been ordered to pay, the restriction on its freedom of expression was considered to have been justified and proportionate. There had accordingly been no violation of Article 10 of the Convention.

(...)

152. The Court notes that the applicant company highlighted the number of comments on each article on its website, and therefore the places of the most lively exchanges must have been easily identifiable for the editors of the news portal. The article in issue in the present case attracted 185 comments, apparently well above average. The comments in question were removed by the applicant company some six weeks after they were uploaded on the website, upon notification by the injured person's lawyers to the applicant company (see paragraphs 17 to 19 above).

153. The Court observes that the Supreme Court stated in its judgment that "[o]n account of the obligation arising from law to avoid causing harm, the [applicant company] should have prevented the publication of comments with clearly unlawful contents". However, it also held that "[a]fter the disclosure, the [applicant company had] failed to remove the comments – the unlawful content of which it should have been aware of – from the portal on its own initiative" (see § 16 of the judgment as set out in paragraph 31 above). Therefore, the Supreme Court did not explicitly determine whether the applicant company was under an obligation to prevent the uploading of the comments on the website or whether it would have sufficed under domestic law for the applicant company to have removed the offending comments without delay after publication, to escape liability under the Obligations Act. The Court considers that when assessing the grounds upon which the Supreme Court relied in its judgment entailing an interference with the applicant's Convention rights, there is nothing to suggest that the national court intended to restrict the applicant's rights to a greater extent than that required to achieve the aim pursued. On this basis, and having regard to the freedom to impart information as enshrined in Article 10, the Court will thus proceed on the assumption that the Supreme Court's judgment must be understood to mean that the subsequent removal of the comments by the applicant company, without delay after publication, would have sufficed for it to escape liability under domestic law. Consequently, and taking account of the above findings (see paragraph 145) to the effect that the applicant company must be considered to have exercised a substantial degree of control over the comments published on its portal, the Court does not consider that the imposition on the applicant company of an obligation to remove from its website, without delay after publication, comments that amounted to hate speech and incitements to violence, and were thus clearly unlawful on their face, amounted, in principle, to a disproportionate interference with its freedom of expression.

154. The pertinent issue in the present case is whether the national court's findings that liability was justified, as the applicant company had not removed the comments without delay after publication, were based on relevant and sufficient grounds. With this in mind, account must, firstly, be taken of

whether the applicant company had instituted mechanisms that were capable of filtering comments amounting to hate speech or speech entailing an incitement to violence.

155. The Court notes that the applicant company took certain measures in this regard. There was a disclaimer on the Delfi news portal stating that the writers of the comments – and not the applicant company – were accountable for them, and that the posting of comments that were contrary to good practice or contained threats, insults, obscene expressions or vulgarities, or incited hostility, violence or illegal activities, was prohibited. Furthermore, the portal had an automatic system of deletion of comments based on stems of certain vulgar words and it had a notice-and-take-down system in place, whereby anyone could notify it of an inappropriate comment by simply clicking on a button designated for that purpose, to bring it to the attention of the portal administrators. In addition, on some occasions the administrators removed inappropriate comments on their own initiative.

156. Thus, the Court notes that the applicant company cannot be said to have wholly neglected its duty to avoid causing harm to third parties. Nevertheless, and more importantly, the automatic word-based filter used by the applicant company failed to filter out odious hate speech and speech inciting violence posted by readers and thus limited its ability to expeditiously remove the offending comments. The Court reiterates that the majority of the words and expressions in question did not include sophisticated metaphors or contain hidden meanings or subtle threats. They were manifest expressions of hatred and blatant threats to the physical integrity of L. Thus, even if the automatic word-based filter may have been useful in some instances, the facts of the present case demonstrate that it was insufficient for detecting comments whose content did not constitute protected speech under Article 10 of the Convention (see paragraph 136 above). The Court notes that as a consequence of this failure of the filtering mechanism, such clearly unlawful comments remained online for six weeks (see paragraph 18 above).

157. The Court observes in this connection that on some occasions the portal administrators did remove inappropriate comments on their own initiative and that, apparently some time after the events of the present case, the applicant company set up a dedicated team of moderators. Having regard to the fact that there are ample possibilities for anyone to make his or her voice heard on the Internet, the Court considers that a large news portal's obligation to take effective measures to limit the dissemination of hate speech and speech inciting violence – the issue in the present case – can by no means be equated to "private censorship". While acknowledging the "important role" played by the Internet "in enhancing the public's access to news and facilitating the dissemination of information in general" (see Ahmet Yıldırım, cited above, § 48, and Times Newspapers Ltd, cited above, § 27), the Court reiterates that it is also mindful of the risk of harm posed by content and communications on the Internet (see Editorial Board of Pravoye Delo and Shtekel, cited above, § 63; see also Mosley, cited above, § 130).

158. Moreover, depending on the circumstances, there may be no identifiable individual victim, for example in some cases of hate speech directed against a group of persons or speech directly inciting violence of the type manifested in several of the comments in the present case. In cases where an individual victim exists, he or she may be prevented from notifying an Internet service provider of the alleged violation of his or her rights. The Court attaches weight to the consideration that the ability of a potential victim of hate speech to continuously monitor the Internet is more limited than the ability of a large commercial Internet news portal to prevent or rapidly remove such comments.

159. Lastly, the Court observes that the applicant company has argued (see paragraph 78 above) that the Court should have due regard to the notice-and-take-down system that it had introduced. If accompanied by effective procedures allowing for rapid response, this system can in the Court's view function in many cases as an appropriate tool for balancing the rights

and interests of all those involved. However, in cases such as the present one, where third-party user comments are in the form of hate speech and direct threats to the physical integrity of individuals, as understood in the Court's case-law (see paragraph 136 above), the Court considers, as stated above (see paragraph 153), that the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals, without contravening Article 10 of the Convention, if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties.

162. Based on the concrete assessment of the above aspects, taking into account the reasoning of the Supreme Court in the present case, in particular the extreme nature of the comments in question, the fact that the comments were posted in reaction to an article published by the applicant company on its professionally managed news portal run on a commercial basis, the insufficiency of the measures taken by the applicant company to remove without delay after publication comments amounting to hate speech and speech inciting violence and to ensure a realistic prospect of the authors of such comments

being held liable, and the moderate sanction imposed on the applicant company, the Court finds that the domestic courts' imposition of liability on the applicant company was based on relevant and sufficient grounds, having regard to the margin of appreciation afforded to the respondent State. Therefore, the measure did not constitute a disproportionate restriction on the applicant company's right to freedom of expression. Accordingly, there has been no violation of Article 10 of the Convention.

FOR THESE REASONS, THE COURT

Holds, by fifteen votes to two, that there has been no violation of Article 10 of the Convention.

***C-291/13 Sotiris Papasavvas v O Fileleftheros Dimosia
Etairia Ltd, Takis Kounnafi, Giorgos Sertis***

*Text contained in relevant case law to Directive 2000/31/EC on Electronic commerce

VI. Cybercrime and Cybersecurity

Convention on Cybercrime

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system

by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

- a producing child pornography for the purpose of its distribution through a computer system;
- b offering or making available child pornography through a computer system;
- c distributing or transmitting child pornography through a computer system;
- d procuring child pornography through a computer system for oneself or for another person;
- e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

- a a minor engaged in sexually explicit conduct;
- b a person appearing to be a minor engaged in sexually explicit conduct;
- c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

- a a power of representation of the legal person;
- b an authority to take decisions on behalf of the legal person;
- c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service

provider, relating to subscribers of its services other than traffic or content data and by which can be established:

- a the type of communication service used, the technical provisions taken thereto and the period of service;
- b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
- c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

- a a computer system or part of it and computer data stored therein; and
- b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

- a seize or similarly secure a computer system or part of it or a computer-data storage medium;
- b make and retain a copy of those computer data;
- c maintain the integrity of the relevant stored computer data;
- d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

- a in its territory; or
- b on board a ship flying the flag of that Party; or
- c on board an aircraft registered under the laws of that Party; or
- d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions

provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a

notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, signatory hereto; Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that all human beings are born free and equal in dignity and rights;

Stressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments;

Convinced that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;

Considering that national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems;

Aware of the fact that propaganda to such acts is often subject to criminalisation in national legislation;

Having regard to the Convention on Cybercrime, which provides for modern and flexible means of international co-operation and convinced of the need to harmonise substantive law provisions concerning the fight against racist and xenophobic propaganda;

Aware that computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;

Recognising that freedom of expression constitutes one of the essential foundations of a democratic society, and is one of the basic conditions for its progress and for the development of every human being;

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Concerned, however, by the risk of misuse or abuse of such computer systems to disseminate racist and xenophobic propaganda;

Mindful of the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;

Recognising that this Protocol is not intended to affect established principles relating to freedom of expression in national legal systems;

Taking into account the relevant international legal instruments in this field, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination, the existing Council of Europe conventions on co-operation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia;

Welcoming the recent developments which further advance international understanding and co-operation in combating cybercrime and racism and xenophobia;

Having regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10-11 October 1997) to seek common responses to the developments of the new technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as “the Convention”), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Article 2 – Definition

1 For the purposes of this Protocol:

“racist and xenophobic material” means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

2 The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

Chapter II – Measures to be taken at national level

Article 3 – Dissemination of racist and xenophobic material through computer systems

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2 A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3 Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 – Racist and xenophobic motivated threat

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2 A Party may either:

a require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or

b reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

1 Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2 A Party may either

a require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

b reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 7 – Aiding and abetting

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Chapter III – Relations between the Convention and this Protocol

Article 8 – Relations between the Convention and this Protocol
1 Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, *mutatis mutandis*, to this Protocol.

2 The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol.

Chapter IV – Final provisions

Article 9 – Expression of consent to be bound

1 This Protocol shall be open for signature by the States which have signed the Convention, which may express their consent to be bound by either:

a signature without reservation as to ratification, acceptance or approval; or

b subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2 A State may not sign this Protocol without reservation as to ratification, acceptance or approval, or deposit an instrument of ratification, acceptance or approval, unless it has already deposited or simultaneously deposits an instrument of ratification, acceptance or approval of the Convention.

3 The instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

Article 10 – Entry into force

1 This Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States have expressed their consent to be bound by the Protocol, in accordance with the provisions of Article 9.

2 In respect of any State which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of its signature without reservation as to ratification, acceptance or approval or deposit of its instrument of ratification, acceptance or approval.

Article 11 – Accession

1 After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

2 Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession which shall take effect on the first day of the month following the expiration of a period of three months after the date of its deposit.

Article 12 – Reservations and declarations

1 Reservations and declarations made by a Party to a provision of the Convention shall be applicable also to this Protocol, unless that Party declares otherwise at the time of signature or

when depositing its instrument of ratification, acceptance, approval or accession.

2 By a written notification addressed to the Secretary General of the Council of Europe, any Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Articles 3, 5 and 6 of this Protocol. At the same time, a Party may avail itself, with respect to the provisions of this Protocol, of the reservation(s) provided for in Article 22, paragraph 2, and Article 41, paragraph 1, of the Convention, irrespective of the implementation made by that Party under the Convention. No other reservations may be made.

3 By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for in Article 5, paragraph 2.a, and Article 6, paragraph 2.a, of this Protocol.

Article 13 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 12 above shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations in accordance with Article 12 as to the prospects for withdrawing such reservation(s).

Article 14 – Territorial application

1 Any Party may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Protocol shall apply.

2 Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Protocol to any other territory specified in

the declaration. In respect of such territory, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 15 – Denunciation

1 Any Party may, at any time, denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 16 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Protocol as well as any State which has acceded to, or has been invited to accede to, this Protocol of:

- a any signature;
- b the deposit of any instrument of ratification, acceptance, approval or accession;
- c any date of entry into force of this Protocol in accordance with its Articles 9, 10 and 11;
- d any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

Done at Strasbourg, this 28th day of January 2003, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Protocol, and to any State invited to accede to it.

For further interpretation see - Convention on Cybercrime – Explanatory report

At www.coe.in

98/560/EC: Council Recommendation on the development of the competitiveness of the European audiovisual and information services industry

COUNCIL RECOMMENDATION of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (98/560/EC)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 130 thereof,

Having regard to the Commission's proposal,

Having regard to the opinion of the European Parliament (1),
Having regard to the opinion of the Economic and Social Committee (2),

(1) Whereas the Commission adopted the Green Paper on the protection of minors and human dignity in audiovisual and information services on 16 October 1996 and the Council received it favourably at its meeting on 16 December 1996;

(2) Whereas the European Parliament (3), the Economic and Social Committee (4) and the Committee of the Regions (5) have all adopted opinions on the Green Paper;

(3) Whereas the conclusions of the consultation process were submitted by the Commission to the Council at its meeting of 30 June 1997 and unanimously welcomed;

(4) Whereas on 16 October 1996, the Commission adopted the communication on illegal and harmful content on the Internet; whereas on 17 February 1997 the Council and the representatives of the Governments of the Member States, meeting within the Council, adopted the resolution on illegal and harmful content on the Internet (6); whereas on 24 April 1997 the European Parliament adopted an opinion on the Commission communication on illegal and harmful content on the Internet; whereas this work is continuing in a manner complementary to the present recommendation since it deals with all forms of illegal and harmful content specifically on the Internet;

(5) Whereas the present recommendation addresses, in particular, issues of protection of minors and of human dignity in relation to audiovisual and information services made available to the public, whatever the means of conveyance (such as broadcasting, proprietary on-line services or services on the Internet);

(6) Whereas, in order to promote the competitiveness of the audiovisual and information services industry and its adaptation to technological development and structural changes, the provision of information, the raising of awareness and the education of users are essential; whereas this is also a condition of the European citizen's full participation in the information society; whereas, therefore, in addition to measures to protect minors and to combat illegal content offensive to human dignity, legal and responsible use of information and communication services should be encouraged, through the exercise, inter alia, of parental control measures;

(7) Whereas Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, Regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (7), and in particular Articles 22, 22a and 22b of Directive 89/552/EEC, lays down a full range of measures aimed at the protection of minors with regard to television broadcasting for the purposes of ensuring the free movement of television broadcasts;

(8) Whereas the development of audiovisual and information services is of vital importance for Europe in view of their significant potential in the fields of education, access to information and culture, economic development and job creation;

(9) Whereas full achievement of this potential requires the existence of a successful and innovative industry in the Community; whereas it is in the first instance incumbent on businesses to ensure and improve their competitiveness with the support of public authorities where appropriate;

(10) Whereas the establishment of the climate of confidence needed to achieve the potential of the audiovisual and information services industry by removing obstacles to the development and full competitiveness of the said industry is promoted by the protection of certain important general interests, in particular the protection of minors and of human dignity;

(11) Whereas the general competitiveness of the European audiovisual and information services industry will improve through the development of an environment that favours cooperation between the enterprises in the sector on matters concerning the protection of minors and human dignity;

(12) Whereas the existence of certain technological conditions enables a high level of protection of the abovementioned important general interests, in particular the protection of minors and human dignity, and, consequently, the acceptance by all users of these services;

(13) Whereas it is important therefore to encourage enterprises to develop a national self-regulatory framework through cooperation between them and the other parties concerned; whereas self-Regulation could provide enterprises with the means to adapt themselves rapidly to the quickening technical progress and to market globalisation;

(14) Whereas the protection of general interests sought in this manner must be seen in the context of the fundamental principles of respect for privacy and freedom of expression, as enshrined in Articles 8 and 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and as recognised by Article F(2) of the Treaty on European Union and by the case-law of the Court of Justice as general principles of Community law;

(15) Whereas any restriction of these rights and freedoms must be non-discriminatory, necessary to achieving the desired objective and strictly proportional with regard to the limitations it imposes;

(16) Whereas the global nature of communications networks necessitates an international approach to the question of the protection of minors and human dignity in audiovisual and information services; whereas, in this context, the development of a common indicative framework at European level makes it possible both to promote European values and make a decisive contribution to the international debate;

(17) Whereas it is vital to distinguish between questions relating to illegal content which is offensive to human dignity and those relating to content that is legal, but liable to harm minors by impairing their physical, mental or moral development; whereas these two types of problem may require a different approach and different solutions;

(18) Whereas the national laws in which Member States have laid down rules and principles on the protection of minors and human dignity reflect cultural diversity and national and local sensitivities; whereas, in this regard, particular attention must be paid to the application of the principle of subsidiarity;

(19) Whereas, in view of the transnational nature of communications networks, the effectiveness of national measures would be strengthened, at Community level, by coordination of national initiatives, and of the bodies responsible for their implementation, in accordance with the respective responsibilities and functions of the parties concerned and by the development of cooperation and the sharing of good practices in relevant areas;

(20) Whereas, as a supplementary measure, and with full respect for the relevant regulatory frameworks at national and Community level, greater self-Regulation by operators should contribute to the rapid implementation of concrete solutions to the problems of the protection of minors and human dignity, while maintaining the flexibility needed to take account of the rapid development of audiovisual and information services;

(21) Whereas the contribution of the Community, the aim of which will be to supplement Member States' measures to protect minors and human dignity in audiovisual and information services, should be based on the maximum use of existing instruments;

(22) Whereas there should be close coordination of the various relevant initiatives conducted in parallel with the follow-up to the Green Paper, particularly the work on the follow-up to the communication on 'Illegal and Harmful Content on the Internet', including the resolution adopted by the Council and the representatives of the Governments of the Member States meeting within the Council on 17 February 1997, the 1997 European Parliament resolution and the two working party reports submitted to the Council on 28 November 1996 and 27 June 1997, work carried out according to the provisions of Article 22b of Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, Regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (8) and the work on cooperation on justice and home affairs;

(23) Whereas the implementation of this recommendation will be closely coordinated with that of any possible new measure

resulting from the work on the follow-up to the Commission communication on illegal and harmful content on the Internet, I. HEREBY RECOMMENDS that the Member States foster a climate of confidence which will promote the development of the audiovisual and information services industry by:

(1) promoting, as a supplement to the regulatory framework, the establishment on a voluntary basis of national frameworks for the protection of minors and human dignity in audiovisual and information services through:

- the encouragement, in accordance with national traditions and practices, of the participation of relevant parties (such as users, consumers, businesses and public authorities) in the definition, implementation and evaluation of national measures in the fields covered by this recommendation,

- the establishment of a national framework for self-Regulation by operators of on-line services, taking into account the indicative principles and methodology described in the Annex,

- cooperation at Community level in developing comparable assessment methodologies;

(2) encouraging broadcasters in their jurisdiction to carry out research and to experiment, on a voluntary basis, with new means of protecting minors and informing viewers, as a supplement to the national and Community regulatory frameworks governing broadcasting;

(3) taking effective measures, where appropriate and feasible, to reduce potential obstacles to the development of the on-line services industry while sustaining the fight against illegal content offensive to human dignity, through:

- the handling of complaints and the transmission of the necessary information about alleged illegal content to the relevant authorities at national level,

- transnational cooperation between the complaints-handling structures, in order to strengthen the effectiveness of national measures;

(4) promoting, in order to encourage the take-up of technological developments and in addition to and consistent with existing legal and other measures regarding broadcasting services, and in close cooperation with the parties concerned:

- action to enable minors to make responsible use of on-line audiovisual and information services, notably by improving the level of awareness among parents, educators and teachers of the potential of the new services and of the means whereby they may be made safe for minors,

- action to facilitate, where appropriate and necessary, identification of, and access to, quality content and services for minors, including through the provision of means of access in educational establishments and public places.

II. RECOMMENDS that the industries and parties concerned:

(1) cooperate, in accordance with national traditions and practices, with the relevant authorities in setting up structures representing all the parties concerned at national level, in order inter alia to facilitate participation in coordination at European and international level in the fields covered by this recommendation;

(2) cooperate in the drawing up of codes of conduct for the protection of minors and human dignity applying to the provision of on-line services, inter alia to create an environment favourable to the development of new services, taking into account the principles and the methodology described in the Annex;

(3) develop and experiment, as regards broadcasting services, on a voluntary basis, with new means of protecting minors and informing viewers in order to encourage innovation while improving such protection;

(4) develop positive measures for the benefit of minors, including initiatives to facilitate their wider access to audiovisual and information services, while avoiding potentially harmful content;

(5) collaborate in the regular follow-up and evaluation of initiatives carried out at national level in application of this recommendation.

III. INVITES the Commission to:

(1) facilitate, where appropriate through existing Community financial instruments, the networking of the bodies responsible

for the definition and implementation of national self-Regulation frameworks and the sharing of experience and good practices, in particular in relation to innovative approaches, at Community level, between the Member States and parties concerned in the various fields covered by this recommendation;

(2) encourage cooperation and the sharing of experience and good practices between the self-Regulation structures and complaints-handling structures, with a view to fostering a climate of confidence by combating the circulation of illegal content offensive to human dignity in on-line audiovisual and information services;

(3) promote, with the Member States, international cooperation in the various fields covered by this recommendation, particularly through the sharing of experience and good practices between operators and other concerned parties in the Community and their partners in other regions of the world;

(4) develop, in cooperation with the competent national authorities, a methodology for evaluating the measures taken in pursuance of this recommendation, with particular attention to the evaluation of the added value of the cooperation process at Community level, and present, two years after the adoption of this recommendation, an evaluation report on its effect to the European Parliament and the Council.

Done at Brussels, 24 September 1998.

For the Council

The President

J. FARNLEITNER

(1) Opinion delivered on 13 May 1998 (not yet published in the Official Journal).

(2) OJ C 214, 10. 7. 1998, p. 25.

(3) OJ C 339, 10. 11. 1997, p. 420.

(4) OJ C 287, 22. 9. 1997, p. 11.

(5) OJ C 215, 16. 7. 1997, p. 37.

(6) OJ C 70, 6. 3. 1997, p. 1.

(7) OJ L 202, 30. 7. 1997, p. 60.

(8) OJ L 298, 17. 10. 1989, p. 23. Directive as amended by Directive 97/36/EC of the European Parliament and of the Council (OJ L 202, 30. 7. 1997, p. 60).

ANNEX

INDICATIVE GUIDELINES FOR THE IMPLEMENTATION, AT NATIONAL LEVEL, OF A SELF-REGULATION FRAMEWORK FOR THE PROTECTION OF MINORS AND HUMAN DIGNITY IN ON-LINE AUDIOVISUAL AND INFORMATION SERVICES

Objective

The purpose of these guidelines is to foster a climate of confidence in the on-line audiovisual and information services industry by ensuring broad consistency, at Community level, in the development, by the businesses and other parties concerned, of national self-Regulation frameworks for the protection of minors and human dignity. The services covered by these guidelines are those provided at a distance, by electronic means. They do not include broadcasting services covered by Council Directive 89/552/EEC or radio broadcasting. The contents concerned are those which are made available to the public, rather than private correspondence.

This consistency will enhance the effectiveness of the self-Regulation process and provide a basis for the necessary transnational cooperation between the parties concerned.

While taking into account the voluntary nature of the self-Regulation process (the primary purpose of which is to supplement existing legislation) and respecting the differences in approach and varying sensitivities in the Member States of the Community, these guidelines relate to four key components of a national self-Regulation framework:

- consultation and representativeness of the parties concerned,

- code(s) of conduct,

- national bodies facilitating cooperation at Community level,

- national evaluation of self-Regulation frameworks.

1. CONSULTATION AND REPRESENTATIVENESS OF THE PARTIES CONCERNED

The objective is to ensure that the definition, implementation and evaluation of a national self-Regulation framework benefits from the full participation of the parties concerned, such as the public authorities, the users, consumers and the businesses which are directly or indirectly involved in the audiovisual and on-line information services industries. The respective responsibilities and functions of the parties concerned, both public and private, should be set out clearly.

The voluntary nature of self-Regulation means that the acceptance and effectiveness of a national self-Regulation framework depends on the extent to which the parties concerned actively cooperate in its definition, application and evaluation.

All the parties concerned should also help with longer-term tasks such as the development of common tools or concepts (for example, on labelling of content) or the planning of ancillary measures (for example, on information, awareness and education).

2. CODE(S) OF CONDUCT

2.1. General

The objective is the production, within the national self-Regulation framework, of basic rules which are strictly proportionate to the aims pursued; these rules should be incorporated into a code (or codes) of conduct covering at least the categories set out at 2.2, to be adopted and implemented voluntarily by the operators (i.e. primarily the businesses) concerned.

In drawing up these rules, the following should be taken into account:

- the diversity of services and functions performed by the various categories of operator (providers of network, access, service, content, etc.) and their respective responsibilities,
- the diversity of environments and applications in on-line services (open and closed networks, applications of varying levels of interactivity).

In view of the above, operators may need one or more codes of conduct.

Given such diversity, the proportionality of the rules drawn up should be assessed in the light of:

- the principles of freedom of expression, protection of privacy and free movement of services,
- the principle of technical and economic feasibility, given that the overall objective is to develop the information society in Europe.

2.2. The content of the code(s) of conduct

The code (or codes) of conduct should cover the following:

2.2.1. Protection of minors

Objective: to enable minors to make responsible use of on-line services and to avoid them gaining access, without the consent of their parents or teachers, to legal content which may impair their physical, mental or moral development. Besides coordinated measures to educate minors and to improve their awareness, this should cover the establishment of certain standards in the following fields:

(a) Information to users

Objective: within the framework of encouraging responsible use of networks, on-line service providers should inform users, where possible, of any risks from the content of certain on-line services and of such appropriate means of protection as are available.

The codes of conduct should address, for example, the issue of basic rules on the nature of the information to be made available to users, its timing and the form in which it is communicated. The most appropriate occasions should be chosen to communicate the information (sale of technical equipment, conclusion of contracts with user, web sites, etc.).

(b) Presentation of legal contents which may harm minors

Objective: where possible, legal content which may harm minors or affect their physical, mental or moral development should be presented in such a way as to provide users with basic information on its potentially harmful effect on minors.

The codes of conduct should therefore address, for example, the issue of basic rules for the businesses providing on-line services concerned and for users and suppliers of content; the rules

should set out the conditions under which the supply and distribution of content likely to harm minors should be subject, where possible, to protection measures such as:

- a warning page, visual signal or sound signal,
- descriptive labelling and/or classification of contents,
- systems to check the age of users.

Priority should be given, in this regard, to protection systems applied at the presentation stage to legal content which is clearly likely to be harmful to minors, such as pornography or violence.

(c) Support for parental control

Objective: where possible, parents, teachers and others exercising control in this area should be assisted by easy-to-use and flexible tools in order to enable, without the former's educational choices being compromised, minors under their charge to have access to services, even when unsupervised.

The codes of conduct should address, for example, the issue of basic rules on the conditions under which, wherever possible, additional tools or services are supplied to users to facilitate parental control, including:

- filter software installed and activated by the user,
- filter options activated, at the end-user's request, by service operators at a higher level (for example, limiting access to predefined sites or offering general access to services).

(d) Handling of complaints ('hotlines')

Objective: to promote the effective management of complaints about content which does not comply with the rules on the protection of minors and/or violates the code of conduct.

The codes of conduct should address, for example, the issue of basic rules on the management of complaints and encourage operators to provide the management tools and structures needed so that complaints can be sent and received without difficulties (telephone, e-mail, fax) and to introduce procedures for dealing with complaints (informing content providers, exchanging information between operators, responding to complaints, etc.).

2.2.2. Protection of human dignity

Objective: to support effective measures in the fight against illegal content offensive to human dignity.

(a) Information for users

Objective: where possible, users should be clearly informed of the risks inherent in the use of on-line services as content providers so as to encourage legal and responsible use of networks.

Codes of conduct should address, for example, the issue of basic rules on the nature of information to be made available, its timing and the form in which it is to be communicated.

(b) Handling of complaints ('hotlines')

Objective: to promote the effective handling of complaints about illegal content offensive to human dignity circulating in audiovisual and on-line services, in accordance with the respective responsibilities and functions of the parties concerned, so as to reduce illegal content and misuse of the networks.

The codes of conduct should address, for example, the issue of basic rules on the management of complaints and encourage operators to provide the management tools and structures needed so that complaints can be sent and received without difficulties (telephone, e-mail, fax) and to introduce procedures for dealing with complaints (informing content providers, exchanging information between operators, responding to complaints, etc.).

(c) Cooperation of operators with judicial and police authorities

Objective: to ensure, in accordance with the responsibilities and functions of the parties concerned effective cooperation between operators and the judicial and police authorities within Member States in combating the production and circulation of illegal content offensive to human dignity in audiovisual and on-line information services.

The codes of conduct should address, for example, the issue of basic rules on cooperation procedures between operators and the competent public authorities, while respecting the principles of proportionality and freedom of expression as well as relevant national legal provisions.

2.2.3. Violations of the codes of conduct

Objective: to strengthen the credibility of the code (or codes) of conduct, taking account of its voluntary nature, by providing for dissuasive measures which are proportionate to the nature of the violations. In this connection, provision should be made, where appropriate, for appeal and mediation procedures.

Appropriate rules to govern this area should be included in the code of conduct.

3. NATIONAL BODIES FACILITATING COOPERATION AT COMMUNITY LEVEL

Objective: to facilitate cooperation at Community level (sharing of experience and good practices; working together) through the networking of the appropriate structures within Member States, consistent with their national functions and responsibilities. Such structures could also allow international cooperation to be extended.

Cooperation at European level means:

- cooperation between the parties concerned:

all the parties involved in the drawing up of the national self-Regulation framework are asked to set up a representative body at national level to facilitate the sharing of experience and

good practices and to work together at Community and international level,

- cooperation between national complaints-handling structures:

to facilitate and develop cooperation at European and international level, the parties involved in an effective complaint management system are asked to set up a national contact point to strengthen cooperation in the fight against illegal content, facilitate the sharing of experience and good practices, and improve legal and responsible use of the networks.

4. EVALUATION OF SELF-REGULATION FRAMEWORKS

The objective is to provide for regular evaluations of the self-Regulation framework at national level, to assess its effectiveness in protecting the general interests in question, to measure its success in achieving its objectives and to adapt it gradually to changes in the market, technology and types of use. The parties concerned are asked to set up an evaluation system at national level so that they can monitor the progress made in implementing the self-Regulation framework. This should take into account appropriate European-level cooperation, inter alia on the development of comparable assessment methodologies.

Regulation (EC) No 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency

Regulation (EC) No 460/2004 of the European Parliament and of the Council
of 10 March 2004

establishing the European Network and Information Security Agency

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee(1),

After consulting the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty(2),

Whereas:

(1) Communication networks and information systems have become an essential factor in economic and societal development. Computing and networking are now becoming ubiquitous utilities in the same way as electricity or water supply already are. The security of communication networks and information systems, in particular their availability, is therefore of increasing concern to society not least because of the possibility of problems in key information systems, due to system complexity, accidents, mistakes and attacks, that may have consequences for the physical infrastructures which deliver services critical to the well-being of EU citizens.

(2) The growing number of security breaches has already generated substantial financial damage, has undermined user confidence and has been detrimental to the development of e-commerce. Individuals, public administrations and businesses have reacted by deploying security technologies and security management procedures. Member States have taken several supporting measures, such as information campaigns and research projects, to enhance network and information security throughout society.

(3) The technical complexity of networks and information systems, the variety of products and services that are interconnected, and the huge number of private and public actors that bear their own responsibility risk undermining the smooth functioning of the Internal Market.

(4) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (the Framework Directive)(3) lays down the tasks of national regulatory authorities, which include cooperating with each other and the Commission in a transparent manner to ensure the development of consistent regulatory practice, contributing to ensuring a high level of protection of personal data and privacy, and ensuring that the integrity and security of public communications networks are ensured.

(5) Present Community legislation also includes Directive 2002/20/EC(4), Directive 2002/22/EC(5), Directive 2002/19/EC(6), Directive 2002/58/EC(7), Directive 1999/93/EC(8), Directive 2000/31/EC(9), as well as the Council Resolution of 18 February 2003 on the implementation of the eEurope 2005 Action Plan(10).

(6) Directive 2002/20/EC entitles Member States to attach to the general authorisation, conditions regarding the security of public networks against unauthorised access in accordance with Directive 97/66/EC(11).

(7) Directive 2002/22/EC requires that Member States take necessary steps to ensure the integrity and availability of the public telephone networks at fixed locations and that undertakings providing publicly available telephone services at fixed locations take all reasonable steps to ensure uninterrupted access to emergency services.

(8) Directive 2002/58/EC requires a provider of a publicly available electronic communications service to take appropriate technical and organisational measures to safeguard security of its services and also requires the confidentiality of the communications and related traffic data. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(12), requires Member States to provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing.

(9) Directive 2002/21/EC and Directive 1999/93/EC contain provisions on standards that are to be published in the Official Journal of the European Union. Member States also use standards from international bodies as well as de facto standards developed by the global industry. It is necessary for the Commission and the Member States to be able to track those standards which meet the requirements of Community legislation.

(10) These internal market measures require different forms of technical and organisational applications by the Member States and the Commission. These are technically complex tasks with no single, self-evident solutions. The heterogeneous application of these requirements can lead to inefficient solutions and create obstacles to the internal market. This calls for the creation of a centre of expertise at European level providing guidance, advice, and when called upon, with assistance within its objectives, which may be relied upon by the European Parliament, the Commission or competent bodies appointed by the Member States. National Regulatory Authorities, designated under Directive 2002/21/EC, can be appointed by a Member State as a competent body.

(11) The establishment of a European agency, the European Network and Information Security Agency, hereinafter referred to as "the Agency", operating as a point of reference and establishing confidence by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in performing the tasks assigned to it, would respond to these needs. The Agency should build on national and Community efforts and therefore perform its tasks in full cooperation with the Member States and be open to contacts with industry and other relevant stakeholders. As electronic networks, to a large extent, are privately owned, the Agency should build on the input from and cooperation with the private sector.

(12) The exercise of the Agency's tasks should not interfere with the competencies and should not pre-empt, impede or overlap with the relevant powers and tasks conferred on:

- the national regulatory authorities as set out in the Directives relating to the electronic communications networks and services, as well as on the European Regulators Group for Electronic Communications Networks and Services established by Commission Decision 2002/627/EC(13) and the Communications Committee referred to in Directive 2002/21/EC,

- the European standardisation bodies, the national standardisation bodies and the Standing Committee as set out in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and Regulations and of rules on Information Society Services(14),

- the supervisory authorities of the Member States relating to the protection of individuals with the regard to the processing of personal data and on the free movement of such data.

(13) To understand better the challenges in the network and information security field, there is a need for the Agency to analyse current and emerging risks and for that purpose the Agency may collect appropriate information, in particular through questionnaires, without imposing new obligations on the private sector or the Member States to generate data. Emerging risks should be understood as issues already visible as possible future risks to network and information security.

(14) Ensuring confidence in networks and information systems requires that individuals, businesses and public administrations are sufficiently informed, educated and trained in the field of network and information security. Public authorities have a role in increasing awareness by informing the general public, small and medium-sized enterprises, corporate companies, public administrations, schools and universities. These measures need to be further developed. An increased information exchange between Member States will facilitate such awareness raising actions. The Agency should provide advice on best practices in awareness-raising, training and courses.

(15) The Agency should have the task of contributing to a high level of network and information security within the Community and of developing a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organisations in the European Union, thus contributing to the smooth functioning of the internal market.

(16) Efficient security policies should be based on well-developed risk assessment methods, both in the public and private sector. Risk assessment methods and procedures are used at different levels with no common practice on their efficient application. The promotion and development of best practices for risk assessment and for interoperable risk management solutions within public and private sector organisations will increase the security level of networks and information systems in Europe.

(17) The work of the Agency should utilise ongoing research, development and technological assessment activities, in particular those carried out by the different Community research initiatives.

(18) Where appropriate and useful for fulfilling its scope, objectives and tasks, the Agency could share experience and general information with bodies and agencies created under European Union law and dealing with network and information security.

(19) Network and information security problems are global issues. There is a need for closer cooperation at global level to improve security standards, improve information, and promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security. Efficient cooperation with third countries and the global community has become a task also at European level. To this end, the Agency should contribute to Community efforts to cooperate with third countries and, where appropriate, with international organisations.

(20) In its activities the Agency should pay attention to small and medium-sized enterprises.

(21) In order effectively to ensure the accomplishment of the tasks of the Agency, the Member States and the Commission should be represented on a Management Board entrusted with the necessary powers to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Agency, approve the Agency's work programme, adopt its own rules of procedure and the Agency's internal rules of operation, appoint and remove the Executive Director. The Management Board should ensure that the Agency carries out its tasks under conditions which enable it to serve in accordance with this Regulation.

(22) A Permanent Stakeholders' Group would be helpful, in order to maintain a regular dialogue with the private sector, consumers organisations and other relevant stakeholders. The Permanent Stakeholders' Group, established and chaired by the Executive Director, should focus on issues relevant to all stakeholders and bring them to the attention of the Executive Director. The Executive Director may, where appropriate and according to the agenda of the meetings, invite representatives of the European Parliament and from other relevant bodies to take part in the meetings of the Group.

(23) The smooth functioning of the Agency requires that its Executive Director is appointed on the grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for network and information security and that he/she performs his/her duties with complete independence and flexibility as to the organisation of the internal functioning of the Agency. To this end, the Executive Director should prepare a proposal for the Agency's work programme, after prior consultation of the Commission and of the Permanent Stakeholders' Group, and take all necessary steps to ensure the proper accomplishment of the working programme of the Agency, should prepare each year a draft general report to be submitted to the Management Board, should draw up a draft statement of estimates of

revenue and expenditure of the Agency and should implement the budget.

(24) The Executive Director should have the possibility to set up ad hoc Working Groups to address in particular scientific and technical matters. In establishing the ad hoc Working Groups the Executive Director should seek input from and mobilise the relevant expertise of private sector. The ad hoc Working Groups should enable the Agency to have access to the most updated information available in order to be able to respond to the security challenges posed by the developing information society. The Agency should ensure that its ad hoc Working Groups are competent and representative and that they include, as appropriate according to the specific issues, representation of the public administrations of the Member States, of the private sector including industry, of the users and of academic experts in network and information security. The Agency may, if necessary, add to the Working Groups independent experts recognised as competent in the field concerned. The experts who participate in the ad hoc Working Groups organised by the Agency should not belong to the Agency's staff. Their expenses should be met by the Agency in accordance with its internal rules and in conformity with the existing Financial Regulations.

(25) The Agency should apply the relevant Community legislation concerning public access to documents as set out in Regulation (EC) No 1049/2001(15) of the European Parliament and of the Council and the protection of individuals with regard to the processing of personal data as set out in Regulation (EC) No 45/2001(16) of the European Parliament and of the Council.

(26) Within its scope, its objectives and in the performance of its tasks, the Agency should comply in particular with the provisions applicable to the Community institutions, as well as the national legislation regarding the treatment of sensitive documents.

(27) In order to guarantee the full autonomy and independence of the Agency, it is considered necessary to grant it an autonomous budget whose revenue comes essentially from a contribution from the Community. The Community budgetary procedure remains applicable as far as any subsidies chargeable to the general budget of the European Union are concerned. Moreover, the Court of Auditors should undertake the auditing of accounts.

(28) Where necessary and on the basis of arrangements to be concluded, the Agency may have access to the interpretation services provided by the Directorate General for Interpretation (DGI) of the Commission, or by Interpretation Services of other Community institutions.

(29) The Agency should be initially established for a limited period and its operations evaluated in order to determine whether the duration of its operations should be extended,

HAVE ADOPTED THIS REGULATION:

SECTION 1 SCOPE, OBJECTIVES AND TASKS

Article 1

Scope

1. For the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market, a European Network and Information Security Agency is hereby established, hereinafter referred to as "the Agency".

2. The Agency shall assist the Commission and the Member States, and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security, thereby ensuring the smooth functioning of the internal market, including those set out in present and future Community legislation, such as in the Directive 2002/21/EC.

3. The objectives and the tasks of the Agency shall be without prejudice to the competencies of the Member States regarding network and information security which fall outside the scope of the EC Treaty, such as those covered by Titles V and VI of the

Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the issues relate to State security matters) and the activities of the State in areas of criminal law.

Article 2

Objectives

1. The Agency shall enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems.

2. The Agency shall provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security falling within its competencies as set out in this Regulation.

3. Building on national and Community efforts, the Agency shall develop a high level of expertise. The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors.

4. The Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

Article 3

Tasks

In order to ensure that the scope and objectives set out in Articles 1 and 2 are complied with and met, the Agency shall perform the following tasks:

(a) collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission;

(b) provide the European Parliament, the Commission, European bodies or competent national bodies appointed by the Member States with advice, and when called upon, with assistance within its objectives;

(c) enhance cooperation between different actors operating in the field of network and information security, inter alia, by organising, on a regular basis, consultation with industry, universities, as well as other sectors concerned and by establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies;

(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues;

(e) contribute to awareness raising and the availability of timely, objective and comprehensive information on network and information security issues for all users by, inter alia, promoting exchanges of current best practices, including on methods of alerting users, and seeking synergy between public and private sector initiatives;

(f) assist the Commission and the Member States in their dialogue with industry to address security-related problems in the hardware and software products;

(g) track the development of standards for products and services on network and information security;

(h) advise the Commission on research in the area of network and information security as well as on the effective use of risk prevention technologies;

(i) promote risk assessment activities, interoperable risk management solutions and studies on prevention management solutions within public and private sector organisations;

(j) contribute to Community efforts to cooperate with third countries and, where appropriate, with international organisations to promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security;

(k) express independently its own conclusions, orientations and give advice on matters within its scope and objectives.

Article 4

Definitions

For the purposes of this Regulation the following definitions shall apply:

(a) "network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable TV networks, irrespective of the type of information conveyed;

(b) "information system" means computers and electronic communication networks, as well as electronic data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

(c) "network and information security" means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems;

(d) "availability" means that data is accessible and services are operational;

(e) "authentication" means the confirmation of an asserted identity of entities or users;

(f) "data integrity" means the confirmation that data which has been sent, received, or stored are complete and unchanged;

(g) "data confidentiality" means the protection of communications or stored data against interception and reading by unauthorised persons;

(h) "risk" means a function of the probability that a vulnerability in the system affects authentication or the availability, authenticity, integrity or confidentiality of the data processed or transferred and the severity of that effect, consequential to the intentional or non-intentional use of such a vulnerability;

(i) "risk assessment" means a scientific and technologically based process consisting of four steps, threats identification, threat characterisation, exposure assessment and risk characterisation;

(j) "risk management" means the process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and, if need be, selecting appropriate prevention and control options;

(k) "culture of network and information security" has the same meaning as that set out in the OECD Guidelines for the security of Information Systems and Networks of 25 July 2002 and the Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security⁽¹⁷⁾.

SECTION 2 ORGANISATION

Article 5

Bodies of the Agency

The Agency shall comprise:

- (a) a Management Board;
- (b) an Executive Director, and
- (c) a Permanent Stakeholders' Group.

Article 6

Management Board

1. The Management Board shall be composed of one representative of each Member State, three representatives appointed by the Commission, as well as three representatives, proposed by the Commission and appointed by the Council, without the right to vote, each of whom represents one of the following groups:

- (a) information and communication technologies industry;
- (b) consumer groups;

(c) academic experts in network and information security.

2. Board members shall be appointed on the basis of their degree of relevant experience and expertise in the field of network and information security. Representatives may be replaced by alternates, appointed at the same time.

3. The Management Board shall elect its Chairperson and a Deputy Chairperson from among its members for a two-and-a-half-year period, which shall be renewable. The Deputy Chairperson shall ex-officio replace the Chairperson in the event of the Chairperson being unable to attend to his/her duties.

4. The Management Board shall adopt its rules of procedure, on the basis of a proposal by the Commission. Unless otherwise provided, the Management Board shall take its decisions by a majority of its members with the right to vote.

A two-thirds majority of all members with the right to vote is required for the adoption of its rules of procedure, the Agency's internal rules of operation, the budget, the annual work programme, as well as the appointment and the removal of the Executive Director.

5. Meetings of the Management Board shall be convened by its Chairperson. The Management Board shall hold an ordinary meeting twice a year. It shall also hold extraordinary meetings at the instance of the Chairperson or at the request of at least a third of its members with the right to vote. The Executive Director shall take part in the meetings of the Management Board, without voting rights, and shall provide the Secretariat.

6. The Management Board shall adopt the Agency's internal rules of operation on the basis of a proposal by the Commission. These rules shall be made public.

7. The Management Board shall define the general orientations for the operation of the Agency. The Management Board shall ensure that the Agency works in accordance with the principles laid down in Articles 12 to 14 and 23. It shall also ensure consistency of the Agency's work with activities conducted by Member States as well as at Community level.

8. Before 30 November each year, the Management Board, having received the Commission's opinion shall adopt the Agency's work programme for the following year. The Management Board shall ensure that the work programme is consistent with the Agency's scope, objectives and tasks as well as with the Community's legislative and policy priorities in the area of network and information security.

9. Before 31 March each year, the Management Board shall adopt the general report on the Agency's activities for the previous year.

10. The financial rules applicable to the Agency shall be adopted by the Management Board after the Commission has been consulted. They may not depart from Commission Regulation (EC, Euratom) No 2343/2002 of 19 November 2002 on the framework Financial Regulation for the bodies referred to in Article 185 of the Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities⁽¹⁸⁾, unless such departure is specifically required for the Agency's operation and the Commission has given its prior consent.

Article 7

Executive Director

1. The Agency shall be managed by its Executive Director, who shall be independent in the performance of his/her duties.

2. The Executive Director shall be appointed by the Management Board on the basis of a list of candidates proposed by the Commission after an open competition following publication in the Official Journal of the European Union and elsewhere of a call for expressions of interest. The Executive Director shall be appointed on the grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for network and information security. Before appointment the candidate nominated by the Management Board shall be invited without delay to make a statement before the European Parliament and to answer questions put by members of that institution. The European Parliament or the Council may also ask at any time for a hearing with the Executive Director on any subject related

to the Agency's activities. The Executive Director may be removed from office by the Management Board.

3. The term of office of the Executive Director shall be up to five years.

4. The Executive Director shall be responsible for:

- (a) the day-to-day administration of the Agency;
- (b) drawing up a proposal for the Agency's work programmes after prior consultation of the Commission and of the Permanent Stakeholders Group;
- (c) implementing the work programmes and the decisions adopted by the Management Board;
- (d) ensuring that the Agency carries out its tasks in accordance with the requirements of those using its services, in particular with regard to the adequacy of the services provided;
- (e) the preparation of the Agency's draft statement of estimates of revenue and expenditure and the execution of its budget;
- (f) all staff matters;
- (g) developing and maintaining contact with the European Parliament and for ensuring a regular dialogue with its relevant committees;
- (h) developing and maintaining contact with the business community and consumers organisations for ensuring a regular dialogue with relevant stakeholders;
- (i) chairing the Permanent Stakeholders' Group.

5. Each year, the Executive Director shall submit to the Management Board for approval:

- (a) a draft general report covering all the activities of the Agency in the previous year;
- (b) a draft work programme.

6. The Executive Director shall, following adoption by the Management Board, forward the work programme to the European Parliament, the Council, the Commission and the Member States and shall have it published.

7. The Executive Director shall, following adoption by the Management Board, transmit the Agency's general report to the European Parliament, the Council, the Commission, the Court of Auditors, the European Economic and Social Committee and the Committee of the Regions and shall have it published.

8. Where necessary and within the Agency's scope, objectives and tasks, the Executive Director may establish, in consultation with the Permanent Stakeholders' Group, ad hoc Working Groups composed of experts. The Management Board shall be duly informed. The procedures regarding in particular the composition, the appointment of the experts by the Executive Director and the operation of the ad hoc Working Groups shall be specified in the Agency's internal rules of operation.

Where established, the ad hoc Working Groups shall address in particular technical and scientific matters.

Members of the Management Board may not be members of the ad hoc Working Groups. Representatives of the Commission shall be entitled to be present in their meetings.

Article 8

Permanent Stakeholders' Group

1. The Executive Director shall establish a Permanent Stakeholders' Group composed of experts representing the relevant stakeholders, such as information and communication technologies industry, consumer groups and academic experts in network and information security.

2. The procedures regarding in particular the number, the composition, the appointment of the members by the Executive Director and the operation of the Group shall be specified in the Agency's internal rules of operation and shall be made public.

3. The Group shall be chaired by the Executive Director. The term of office of its members shall be two-and-a-half years. Members of the Group may not be members of the Management Board.

4. Representatives of the Commission shall be entitled to be present in the meetings and participate in the work of the Group.

5. The Group may advise the Executive Director in the performance of his/her duties under this Regulation, in drawing up a proposal for the Agency's work programme, as well as in ensuring communication with the relevant stakeholders on all issues related to the work programme.

SECTION 3 OPERATION

Article 9

Work programme

The Agency shall base its operations on carrying out the work programme adopted in accordance with Article 6(8). The work programme shall not prevent the Agency from taking up unforeseen activities that fall within its scope and objectives and within the given budget limitations.

Article 10

Requests to the Agency

1. Requests for advice and assistance falling within the Agency's scope, objectives and tasks shall be addressed to the Executive Director and accompanied by background information explaining the issue to be addressed. The Executive Director shall inform the Commission of the received requests. If the Agency refuses a request, justification shall be given.

2. Requests referred to in paragraph 1 may be made by:

- (a) the European Parliament;
- (b) the Commission;
- (c) any competent body appointed by a Member State, such as a national regulatory authority as defined in Article 2 of Directive 2002/21/EC.

3. The practical arrangements for the application of paragraphs 1 and 2, regarding in particular the submission, the prioritisation, the follow up as well as the information of the Management Board on the requests to the Agency shall be laid down by the Management Board in the Agency's internal rules of operation.

Article 11

Declaration of interests

1. The Executive Director, as well as officials seconded by Member States on a temporary basis shall make a declaration of commitments and a declaration of interests indicating the absence of any direct or indirect interests, which might be considered prejudicial to their independence. Such declarations shall be made in writing.

2. External experts participating in ad hoc Working Groups, shall declare at each meeting any interests, which might be considered prejudicial to their independence in relation to the items on the agenda.

Article 12

Transparency

1. The Agency shall ensure that it carries out its activities with a high level of transparency and in accordance with Article 13 and 14.

2. The Agency shall ensure that the public and any interested parties are given objective, reliable and easily accessible information, in particular with regard to the results of its work, where appropriate. It shall also make public the declarations of interest made by the Executive Director and by officials seconded by Member States on a temporary basis, as well as the declarations of interest made by experts in relation to items on the agendas of meetings of the ad hoc Working Groups.

3. The Management Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of the Agency's activities.

4. The Agency shall lay down in its internal rules of operation the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.

Article 13

Confidentiality

1. Without prejudice to Article 14, the Agency shall not divulge to third parties information that it processes or receives for which confidential treatment has been requested.

2. Members of the Management Board, the Executive Director, the members of the Permanent Stakeholders Group, external experts participating in ad hoc Working Groups, and members of the staff of the Agency including officials seconded by Member States on a temporary basis, even after their duties have ceased, are subject to the requirements of confidentiality pursuant to Article 287 of the Treaty.

3. The Agency shall lay down in its internal rules of operation the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.

Article 14

Access to documents

1. Regulation (EC) No 1049/2001 shall apply to documents held by the Agency.

2. The Management Board shall adopt arrangements for implementing the Regulation (EC) No 1049/2001 within six months of the establishment of the Agency.

3. Decisions taken by the Agency pursuant to Article 8 of Regulation (EC) No 1049/2001 may form the subject of a complaint to the Ombudsman or of an action before the Court of Justice of the European Communities, under Articles 195 and 230 of the Treaty respectively.

SECTION 4 FINANCIAL PROVISIONS

Article 15

Adoption of the budget

1. The revenues of the Agency shall consist of a contribution from the Community and any contribution from third countries participating in the work of the Agency as provided for by Article 24.

2. The expenditure of the Agency shall include the staff, administrative and technical support, infrastructure and operational expenses, and expenses resulting from contracts entered into with third parties.

3. By 1 March each year at the latest, the Executive Director shall draw up a draft statement of estimates of the Agency's revenue and expenditure for the following financial year, and shall forward it to the Management Board, together with a draft establishment plan.

4. Revenue and expenditure shall be in balance.

5. Each year, the Management Board, on the basis of a draft statement of estimates of revenue and expenditure drawn up by the Executive Director, shall produce a statement of estimates of revenue and expenditure for the Agency for the following financial year.

6. This statement of estimates, which shall include a draft establishment plan together with the provisional work programme, shall by 31 March at the latest, be transmitted by the Management Board to the Commission and the States with which the Community has concluded agreements in accordance with Article 24.

7. This statement of estimates shall be forwarded by the Commission to the European Parliament and the Council (both hereinafter referred to as the "budgetary authority") together with the preliminary draft general budget of the European Union.

8. On the basis of this statement of estimates, the Commission shall enter in the preliminary draft general budget of the European Union the estimates it deems necessary for the establishment plan and the amount of the subsidy to be charged to the general budget, which it shall submit to the budgetary authority in accordance with Article 272 of the Treaty.

9. The budgetary authority shall authorise the appropriations for the subsidy to the Agency.

The budgetary authority shall adopt the establishment plan for the Agency.

10. The Management Board shall adopt the Agency's budget. It shall become final following final adoption of the general budget of the European Union. Where appropriate, the Agency's budget shall be adjusted accordingly. The Management Board shall forward it without delay to the Commission and the budgetary authority.

11. The Management Board shall, as soon as possible, notify the budgetary authority of its intention to implement any project which may have significant financial implications for the funding of the budget, in particular any projects relating to property such as the rental or purchase of buildings. It shall inform the Commission thereof.

Where a branch of the budgetary authority has notified its intention to deliver an opinion, it shall forward its opinion to the Management Board within a period of six weeks from the date of notification of the project.

Article 16

Combating fraud

1. In order to combat fraud, corruption and other unlawful activities the provisions of Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-fraud Office (OLAF)(19) shall apply without restriction.

2. The Agency shall accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament and the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-fraud Office (OLAF)(20) and shall issue, without delay, the appropriate provisions applicable to all the employees of the Agency.

Article 17

Implementation of the budget

1. The Executive Director shall implement the Agency's budget.

2. The Commission's internal auditor shall exercise the same powers over the Agency as over Commission departments.

3. By 1 March at the latest following each financial year, the Agency's accounting officer shall communicate the provisional accounts to the Commission's accounting officer together with a report on the budgetary and financial management for that financial year. The Commission's accounting officer shall consolidate the provisional accounts of the institutions and decentralised bodies in accordance with Article 128 of Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities(21) (hereinafter referred to as the general Financial Regulation).

4. By 31 March at the latest following each financial year, the Commission's accounting officer shall transmit the Agency's provisional accounts to the Court of Auditors, together with a report on the budgetary and financial management for that financial year. The report on the budgetary and financial management for the financial year shall also be transmitted to the budgetary authority.

5. On receipt of the Court of Auditor's observations on the Agency's provisional accounts, pursuant to Article 129 of the general Financial Regulation, the Executive Director shall draw up the Agency's final accounts under his/her own responsibility and transmit them to the Management Board for an opinion.

6. The Management Board shall deliver an opinion on the Agency's final accounts.

7. The Executive Director shall, by 1 July at the latest following each financial year, transmit the final accounts to the European Parliament, the Council, the Commission and the Court of Auditors, together with the Management Board's opinion.

8. The final accounts shall be published.

9. The Executive Director shall send the Court of Auditors a reply to its observations by 30 September at the latest. He/she shall also send this reply to the Management Board.

10. The Executive Director shall submit to the European Parliament, at the latter's request, all information necessary for the smooth application of the discharge procedure for the financial year in question, as laid down in Article 146(3) of the general Financial Regulation.

11. The European Parliament, on a recommendation from the Council acting by a qualified majority, shall, before 30 April of year N+2 give a discharge to the Executive Director in respect of the implementation of the budget for the year N.

SECTION 5 GENERAL PROVISIONS

Article 18

Legal status

1. The Agency shall be a body of the Community. It shall have legal personality.

2. In each of the Member States the Agency shall enjoy the most extensive legal capacity accorded to legal persons under their laws. It may in particular, acquire and dispose of movable and immovable property and be a party to legal proceedings.

3. The Agency shall be represented by its Executive Director.

Article 19

Staff

1. The staff of the Agency, including its Executive Director, shall be subject to the rules and Regulations applicable to officials and other staff of the European Communities.

2. Without prejudice to Article 6, the powers conferred on the appointing authority by the Staff Regulations and on the authority authorised to conclude contracts by the Conditions of employment of other servants, shall be exercised by the Agency in respect of its own staff.

The Agency may also employ officials seconded by Member States on a temporary basis and for a maximum of five years.

Article 20

Privileges and immunities

The Protocol on the Privileges and Immunities of the European Communities shall apply to the Agency and its staff.

Article 21

Liability

1. The contractual liability of the Agency shall be governed by the law applicable to the contract in question.

The Court of Justice of the European Communities shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by the Agency.

2. In the case of non-contractual liability, the Agency shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by it or its servants in the performance of their duties.

The Court of Justice shall have jurisdiction in any dispute relating to compensation for such damage.

3. The personal liability of its servants towards the Agency shall be governed by the relevant conditions applying to the staff of the Agency.

Article 22

Languages

1. The provisions laid down in Regulation No 1 of 15 April 1958 determining the languages to be used in the European Economic Community(22) shall apply to the Agency. The Member States and the other bodies appointed by them may address the Agency and receive a reply in the Community language of their choice.

2. The translation services required for the functioning of the Agency shall be provided by the Translation Centre for the Bodies of the European Union(23).

Article 23

Protection of personal data

When processing data relating to individuals, the Agency shall be subject to the provisions of Regulation (EC) No 45/2001.

Article 24

Participation of third countries

1. The Agency shall be open to the participation of countries, which have concluded agreements with the European Community by virtue of which they have adopted and applied Community legislation in the field covered by this Regulation.

2. Arrangements shall be made under the relevant provisions of those agreements, specifying in particular the nature, extent and manner in which these countries will participate in the Agency's work, including provisions relating to participation in the initiatives undertaken by the Agency, financial contributions and staff.

SECTION 6 FINAL PROVISIONS

Article 25

Review clause

1. By 17 March 2007, the Commission, taking into account the views of all relevant stakeholders, shall carry out an evaluation on the basis of the terms of reference agreed with the Management Board. The Commission shall undertake the evaluation, notably with the aim to determine whether the duration of the Agency should be extended beyond the period specified in Article 27.

2. The evaluation shall assess the impact of the Agency on achieving its objectives and tasks, as well as its working practices and envisage, if necessary, the appropriate proposals.

3. The Management Board shall receive a report on the evaluation and issue recommendations regarding eventual appropriate changes to this Regulation to the Commission. Both the evaluation findings and recommendations shall be

forwarded by the Commission to the European Parliament and the Council and shall be made public.

Article 26

Administrative control

The operations of the Agency are subject to the supervision of the Ombudsman in accordance with the provisions of Article 195 of the Treaty.

Article 27

Duration

The Agency shall be established from 14 March 2004 for a period of five years.

Article 28

Entry into force

This Regulation shall enter into force on the day following that of its publication in the Official Journal of the European Union. This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg, 10 March 2004.

For the European Parliament

The President

P. Cox

For the Council

The President

D. Roche

(1) OJ C 220, 16.9.2003, p. 33.

(2) Opinion of the European Parliament of 19 November 2003 (not yet published in the Official Journal) and Council Decision of 19 February 2004.

(3) OJ L 108, 24.4.2002, p. 33.

(4) Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108, 24.4.2002, p. 21).

(5) Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108, 24.4.2002, p. 51).

(6) Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) (OJ L 108, 24.4.2002, p. 7).

(7) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

(8) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

(9) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1).

(10) OJ C 48, 28.2.2003, p. 2.

(11) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30.1.1998, p. 1). Directive repealed and replaced by Directive 2002/58/EC.

(12) OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

(13) OJ L 200, 30.7.2002, p. 38.

(14) OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

(15) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

(16) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by

the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(17) OJ C 48, 28.2.2003, p. 1.

(18) OJ L 357, 31.12.2002, p. 72.

(19) OJ L 136, 31.5.1999, p. 1.

(20) OJ L 136, 31.5.1999, p. 15.

(21) OJ L 248, 16.9.2002, p. 1.

(22) OJ L 17, 6.10.1958, p. 385/58. Regulation as last amended by the 1994 Act of Accession.

(23) Council Regulation (EC) No 2965/94 of 28 November 1994 setting up a Translation Centre for bodies of the European Union (OJ L 314, 7.12.1994, p. 1). Regulation as last amended by Regulation (EC) No 1645/2003 (OJ L 245, 29.9.2003, p. 13).

Directive 2013/40/EU of 12 August 2013 on attacks against information systems

DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 12 August 2013

on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 83(1) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1)

The objectives of this Directive are to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA).

(2)

Information systems are a key element of political, social and economic interaction in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of those systems in the Union is vital for the development of the internal market and of a competitive and innovative economy. Ensuring an appropriate level of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to cybercrime.

(3)

Attacks against information systems, and, in particular, attacks linked to organised crime, are a growing menace in the Union and globally, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and of the Union. This constitutes a threat to the achievement of a safer information society and of an area of freedom, security, and justice, and therefore requires a response at Union level and improved cooperation and coordination at international level.

(4)

There are a number of critical infrastructures in the Union, the disruption or destruction of which would have a significant cross-border impact. It has become apparent from the need to

increase the critical infrastructure protection capability in the Union that the measures against cyber attacks should be complemented by stringent criminal penalties reflecting the gravity of such attacks. Critical infrastructure could be understood to be an asset, system or part thereof located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, such as power plants, transport networks or government networks, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

(5)

There is evidence of a tendency towards increasingly dangerous and recurrent large-scale attacks conducted against information systems which can often be critical to Member States or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated methods, such as the creation and use of so-called 'botnets', which involves several stages of a criminal act, where each stage alone could pose a serious risk to public interests. This Directive aims, inter alia, to introduce criminal penalties for the creation of botnets, namely, the act of establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyber attacks. Once created, the infected network of computers that constitute the botnet can be activated without the computer users' knowledge in order to launch a large-scale cyber attack, which usually has the capacity to cause serious damage, as referred to in this Directive. Member States may determine what constitutes serious damage according to their national law and practice, such as disrupting system services of significant public importance, or causing major financial cost or loss of personal data or sensitive information.

(6)

Large-scale cyber attacks can cause substantial economic damage both through the interruption of information systems and communication and through the loss or alteration of commercially important confidential information or other data. Particular attention should be paid to raising the awareness of innovative small and medium-sized enterprises to threats relating to such attacks and their vulnerability to such attacks, due to their increased dependence on the proper functioning and availability of information systems and often limited resources for information security.

(7)

Common definitions in this area are important in order to ensure a consistent approach in the Member States to the application of this Directive.

(8)

There is a need to achieve a common approach to the constituent elements of criminal offences by introducing common offences of illegal access to an information system, illegal system interference, illegal data interference, and illegal interception.

(9)

Interception includes, but is not necessarily limited to, the listening to, monitoring or surveillance of the content of

communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means.

(10)

Member States should provide for penalties in respect of attacks against information systems. Those penalties should be effective, proportionate and dissuasive and should include imprisonment and/or fines.

(11)

This Directive provides for criminal penalties at least for cases which are not minor. Member States may determine what constitutes a minor case according to their national law and practice. A case may be considered minor, for example, where the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.

(12)

The identification and reporting of threats and risks posed by cyber attacks and the related vulnerability of information systems is a pertinent element of effective prevention of, and response to, cyber attacks and to improving the security of information systems. Providing incentives to report security gaps could add to that effect. Member States should endeavour to provide possibilities for the legal detection and reporting of security gaps.

(13)

It is appropriate to provide for more severe penalties where an attack against an information system is committed by a criminal organisation, as defined in Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime (3), where a cyber attack is conducted on a large scale, thus affecting a significant number of information systems, including where it is intended to create a botnet, or where a cyber attack causes serious damage, including where it is carried out through a botnet. It is also appropriate to provide for more severe penalties where an attack is conducted against a critical infrastructure of the Member States or of the Union.

(14)

Setting up effective measures against identity theft and other identity-related offences constitutes another important element of an integrated approach against cybercrime. Any need for Union action against this type of criminal behaviour could also be considered in the context of evaluating the need for a comprehensive horizontal Union instrument.

(15)

The Council Conclusions of 27 to 28 November 2008 indicated that a new strategy should be developed with the Member States and the Commission, taking into account the content of the 2001 Council of Europe Convention on Cybercrime. That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive builds on that Convention. Completing the process of ratification of that Convention by all Member States as soon as possible should be considered to be a priority.

(16)

Given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, this Directive refers to tools that can be used in order to commit the offences laid down in this Directive. Such tools could include malicious software, including those able to create botnets, used to commit cyber attacks. Even where such a tool is suitable or particularly suitable for carrying out one of the offences laid down in this Directive, it is possible that it was produced for a legitimate purpose. Motivated by the need to avoid criminalisation where such tools are produced and put on the market for legitimate purposes, such as to test the reliability of information technology products or the security of information systems, apart from the general intent requirement, a direct intent requirement that those tools be

used to commit one or more of the offences laid down in this Directive must be also fulfilled.

(17)

This Directive does not impose criminal liability where the objective criteria of the offences laid down in this Directive are met but the acts are committed without criminal intent, for instance where a person does not know that access was unauthorised or in the case of mandated testing or protection of information systems, such as where a person is assigned by a company or vendor to test the strength of its security system. In the context of this Directive, contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceedings. This Directive is without prejudice to the right of access to information as laid down in national and Union law, while at the same time it may not serve as a justification for unlawful or arbitrary access to information.

(18)

Cyber attacks could be facilitated by various circumstances, such as where the offender has access to security systems inherent in the affected information systems within the scope of his or her employment. In the context of national law, such circumstances should be taken into account in the course of criminal proceedings as appropriate.

(19)

Member States should provide for aggravating circumstances in their national law in accordance with the applicable rules established by their legal systems on aggravating circumstances. They should ensure that those aggravating circumstances are available for judges to consider when sentencing offenders. It remains within the discretion of the judge to assess those circumstances together with the other facts of the particular case.

(20)

This Directive does not govern conditions for exercising jurisdiction over any of the offences referred to herein, such as a report by the victim in the place where the offence was committed, a denunciation from the State of the place where the offence was committed, or the non-prosecution of the offender in the place where the offence was committed.

(21)

In the context of this Directive, States and public bodies remain fully bound to guarantee respect for human rights and fundamental freedoms, in accordance with existing international obligations.

(22)

This Directive strengthens the importance of networks, such as the G8 or the Council of Europe's network of points of contact available on a 24 hour, seven-day-a-week basis. Those points of contact should be able to deliver effective assistance thus, for example, facilitating the exchange of relevant information available and the provision of technical advice or legal information for the purpose of investigations or proceedings concerning criminal offences relating to information systems and associated data involving the requesting Member State. In order to ensure the smooth operation of the networks, each contact point should have the capacity to communicate with the point of contact of another Member State on an expedited basis with the support, inter alia, of trained and equipped personnel. Given the speed with which large-scale cyber attacks can be carried out, Member States should be able to respond promptly to urgent requests from this network of contact points. In such cases, it may be expedient that the request for information be accompanied by telephone contact in order to ensure that the request is processed swiftly by the requested Member State and that feedback is provided within eight hours.

(23)

Cooperation between public authorities on the one hand, and the private sector and civil society on the other, is of great importance in preventing and combating attacks against information systems. It is necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law. Such cooperation could include support by service providers in helping to preserve potential evidence, in providing elements helping to identify offenders and, as a last resort, in shutting down, completely or partially, in accordance with national law and practice, information systems or functions that have been compromised or used for illegal purposes. Member States should also consider setting up cooperation and partnership networks with service providers and producers for the exchange of information in relation to the offences within the scope of this Directive.

(24)

There is a need to collect comparable data on the offences laid down in this Directive. Relevant data should be made available to the competent specialised Union agencies and bodies, such as Europol and ENISA, in line with their tasks and information needs, in order to gain a more complete picture of the problem of cybercrime and network and information security at Union level and thereby to contribute to formulating a more effective response. Member States should submit information on the *modus operandi* of the offenders to Europol and its European Cybercrime Centre for the purpose of conducting threat assessments and strategic analyses of cybercrime in accordance with Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (4). Providing information can facilitate a better understanding of present and future threats and thus contribute to more appropriate and targeted decision-making on combating and preventing attacks against information systems.

(25)

The Commission should submit a report on the application of this Directive and make necessary legislative proposals which could lead to broadening its scope, taking into account developments in the field of cybercrime. Such developments could include technological developments, for example those enabling more effective enforcement in the area of attacks against information systems or facilitating prevention or minimising the impact of such attacks. For that purpose, the Commission should take into account the available analyses and reports produced by relevant actors and, in particular, Europol and ENISA.

(26)

In order to fight cybercrime effectively, it is necessary to increase the resilience of information systems by taking appropriate measures to protect them more effectively against cyber attacks. Member States should take the necessary measures to protect their critical infrastructure from cyber attacks, as part of which they should consider the protection of their information systems and associated data. Ensuring an adequate level of protection and security of information systems by legal persons, for example in connection with the provision of publicly available electronic communications services in accordance with existing Union legislation on privacy and electronic communication and data protection, forms an essential part of a comprehensive approach to effectively counteracting cybercrime. Appropriate levels of protection should be provided against reasonably identifiable threats and vulnerabilities in accordance with the state of the art for specific sectors and the specific data processing situations. The cost and burden of such protection should be proportionate to the likely damage a cyber attack would cause to those affected. Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks.

(27)

Significant gaps and differences in Member States' laws and criminal procedures in the area of attacks against information systems may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in this area. The transnational and borderless nature of modern information systems means that attacks against such systems have a cross-border dimension, thus underlining the urgent need for further action to approximate criminal law in this area. In addition, the coordination of prosecution of cases of attacks against information systems should be facilitated by the adequate implementation and application of Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflict of jurisdiction in criminal proceedings (5). Member States, in cooperation with the Union, should also seek to improve international cooperation relating to the security of information systems, computer networks and computer data. Proper consideration of the security of data transfer and storage should be given in any international agreement involving data exchange.

(28)

Improved cooperation between the competent law enforcement bodies and judicial authorities across the Union is essential in an effective fight against cybercrime. In this context, stepping up the efforts to provide adequate training to the relevant authorities in order to raise the understanding of cybercrime and its impact, and to foster cooperation and the exchange of best practices, for example via the competent specialised Union agencies and bodies, should be encouraged. Such training should, *inter alia*, aim at raising awareness about the different national legal systems, the possible legal and technical challenges of criminal investigations, and the distribution of competences between the relevant national authorities.

(29)

This Directive respects human rights and fundamental freedoms and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, including the protection of personal data, the right to privacy, freedom of expression and information, the right to a fair trial, the presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties. In particular, this Directive seeks to ensure full respect for those rights and principles and must be implemented accordingly.

(30)

The protection of personal data is a fundamental right in accordance with Article 16(1) TFEU and Article 8 of the Charter on Fundamental Rights of the European Union. Therefore, any processing of personal data in the context of the implementation of this Directive should fully comply with the relevant Union law on data protection.

(31)

In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, those Member States have notified their wish to take part in the adoption and application of this Directive.

(32)

In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

(33)

Since the objectives of this Directive, namely to subject attacks against information systems in all Member States to effective, proportionate and dissuasive criminal penalties and to improve and encourage cooperation between judicial and other competent authorities, cannot be sufficiently achieved

by the Member States, and can therefore, by reason of their scale or effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(34)

This Directive aims to amend and expand the provisions of Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (6). Since the amendments to be made are of substantial number and nature, Framework Decision 2005/222/JHA should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter

This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.

Article 2

Definitions

For the purposes of this Directive, the following definitions shall apply:

(a)

'information system' means a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;

(b)

'computer data' means a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function;

(c)

'legal person' means an entity having the status of legal person under the applicable law, but does not include States or public bodies acting in the exercise of State authority, or public international organisations;

(d)

'without right' means conduct referred to in this Directive, including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law.

Article 3

Illegal access to information systems

Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.

Article 4

Illegal system interference

Member States shall take the necessary measures to ensure that seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible,

intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 5

Illegal data interference

Member States shall take the necessary measures to ensure that deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 6

Illegal interception

Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 7

Tools used for committing offences

Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:

(a)

a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b)

a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Article 8

Incitement, aiding and abetting and attempt

1. Member States shall ensure that the incitement, or aiding and abetting, to commit an offence referred to in Articles 3 to 7 is punishable as a criminal offence.

2. Member States shall ensure that the attempt to commit an offence referred to in Articles 4 and 5 is punishable as a criminal offence.

Article 9

Penalties

1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by effective, proportionate and dissuasive criminal penalties.

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by a maximum term of imprisonment of at least two years, at least for cases which are not minor.

3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 and 5, when committed intentionally, are punishable by a maximum term of imprisonment of at least three years where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose.

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 4 and 5 are punishable by a maximum term of imprisonment of at least five years where:

(a)

they are committed within the framework of a criminal organisation, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for therein;

(b)
they cause serious damage; or

(c)
they are committed against a critical infrastructure information system.

5. Member States shall take the necessary measures to ensure that when the offences referred to in Articles 4 and 5 are committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with national law, be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law.

Article 10

Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 8, committed for their benefit by any person, acting either individually or as part of a body of the legal person, and having a leading position within the legal person, based on one of the following:

(a)
a power of representation of the legal person;

(b)
an authority to take decisions on behalf of the legal person;

(c)
an authority to exercise control within the legal person.

2. Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has allowed the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8 for the benefit of that legal person.

3. The liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators or inciters of, or accessories to, any of the offences referred to in Articles 3 to 8.

Article 11

Sanctions against legal persons

1. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 10(1) is punishable by effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and which may include other sanctions, such as:

(a)
exclusion from entitlement to public benefits or aid;

(b)
temporary or permanent disqualification from the practice of commercial activities;

(c)
placing under judicial supervision;

(d)
judicial winding-up;

(e)
temporary or permanent closure of establishments which have been used for committing the offence.

2. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 10(2) is punishable by effective, proportionate and dissuasive sanctions or other measures.

Article 12

Jurisdiction

1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8 where the offence has been committed:

(a)
in whole or in part within their territory; or

(b)
by one of their nationals, at least in cases where the act is an offence where it was committed.

2. When establishing jurisdiction in accordance with point (a) of paragraph 1, a Member State shall ensure that it has jurisdiction where:

(a)
the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or

(b)
the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.

3. A Member State shall inform the Commission where it decides to establish jurisdiction over an offence referred to in Articles 3 to 8 committed outside its territory, including where:

(a)
the offender has his or her habitual residence in its territory; or

(b)
the offence is committed for the benefit of a legal person established in its territory.

Article 13

Exchange of information

1. For the purpose of exchanging information relating to the offences referred to in Articles 3 to 8, Member States shall ensure that they have an operational national point of contact and that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that for urgent requests for assistance, the competent authority can indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer.

2. Member States shall inform the Commission of their appointed point of contact referred to in paragraph 1. The Commission shall forward that information to the other Member States and competent specialised Union agencies and bodies.

3. Member States shall take the necessary measures to ensure that appropriate reporting channels are made available in order to facilitate the reporting of the offences referred to in Article 3 to 6 to the competent national authorities without undue delay.

Article 14

Monitoring and statistics

1. Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 to 7.

2. The statistical data referred to in paragraph 1 shall, as a minimum, cover existing data on the number of offences referred to in Articles 3 to 7 registered by the Member States, and the number of persons prosecuted for and convicted of the offences referred to in Articles 3 to 7.

3. Member States shall transmit the data collected pursuant to this Article to the Commission. The Commission shall ensure that a consolidated review of the statistical reports is published and submitted to the competent specialised Union agencies and bodies.

Article 15

Replacement of Framework Decision 2005/222/JHA

Framework Decision 2005/222/JHA is hereby replaced in relation to Member States participating in the adoption of this Directive, without prejudice to the obligations of the Member States relating to the time limit for transposition of the Framework Decision into national law.

In relation to Member States participating in the adoption of this Directive, references to the Framework Decision 2005/222/JHA shall be construed as references to this Directive.

Article 16

Transposition

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive by 4 September 2015.

2. Member States shall transmit to the Commission the text of the measures transposing into their national law the obligations imposed on them under this Directive.

3. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such a reference shall be laid down by the Member States.

Article 17

Reporting

The Commission shall, by 4 September 2017, submit a report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by legislative proposals. The

Commission shall also take into account the technical and legal developments in the field of cybercrime, particularly with regard to the scope of this Directive.

Article 18

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 19

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels, 12 August 2013.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

L. LINKEVIČIUS

(1) OJ C 218, 23.7.2011, p. 130.

(2) Position of the European Parliament of 4 July 2013 (not yet published in the Official Journal) and decision of the Council of 22 July 2013.

(3) OJ L 300, 11.11.2008, p. 42.

(4) OJ L 121, 15.5.2009, p. 37.

(5) OJ L 328, 15.12.2009, p. 42.

(6) OJ L 69, 16.3.2005, p. 67.

See also:

2013/0027 (COD) Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union

Explanatory Memorandum - Directive concerning measures to ensure a high common level of network and information security across the Union

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

1. INTRODUCTION

1.1. Context

Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies - most strikingly during the Arab Spring.

For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role.

Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems.

By completing the Digital Single Market, Europe could boost its GDP by almost €500 billion a year; an average of €1000 per person. For new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication, citizens will need trust and confidence. Unfortunately, a 2012 Eurobarometer survey showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases. An overwhelming majority also said they avoid disclosing personal information online because of security concerns. Across the EU, more than one in ten Internet users has already become victim of online fraud.

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes. The EU economy is already affected by cybercrime activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and

state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.

In countries outside the EU, governments may also misuse cyberspace for surveillance and control over their own citizens. The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online.

All these factors explain why governments across the world have started to develop cyber- security strategies and to consider cyberspace as an increasingly important international issue. The time has come for the EU to step up its actions in this area. This proposal for a Cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.

1.2. Principles for cybersecurity

The borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or Regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent. This strategy clarifies the principles that should guide cybersecurity policy in the EU and internationally.

The EU's core values apply as much in the digital as in the physical world

The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain. Protecting fundamental rights, freedom of expression, personal data and privacy

Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field.

Access for all

Limited or no access to the Internet and digital illiteracy constitute a disadvantage to citizens, given how much the digital world pervades activity within society. Everyone should be able to access the Internet and to an unhindered flow of information. The Internet's integrity and security must be guaranteed to allow safe access for all.

Democratic and efficient multi-stakeholder governance

The digital world is not controlled by a single entity. There are currently several stakeholders, of which many are commercial and non-governmental entities, involved in the day-to-day management of Internet resources, protocols and standards and in the future development of the Internet. The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach.

A shared responsibility to ensure security

The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities which need to be properly defined, thoroughly analysed, remedied or reduced. All relevant actors, whether

public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity.

2. STRATEGIC PRIORITIES AND ACTIONS

The EU should safeguard an online environment providing the highest possible freedom and security for the benefit of everyone. While acknowledging that it is predominantly the task of Member States to deal with security challenges in cyberspace, this strategy proposes specific actions that can enhance the EU's overall performance. These actions are both short and long term, they include a variety of policy tools and involve different types of actors, be it the EU institutions, Member States or industry.

The EU vision presented in this strategy is articulated in five strategic priorities, which address the challenges highlighted above:

Achieving cyber resilience

Drastically reducing cybercrime

Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)

Develop the industrial and technological resources for cybersecurity

Establish a coherent international cyberspace policy for the European Union and promote core EU values

2.1. Achieving cyber resilience

To promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and cooperate effectively. Building on the positive results achieved via the activities carried out to date further EU action can help in particular to counter cyber risks and threats having a cross-border dimension, and contribute to a coordinated response in emergency situations. This will strongly support the good functioning of the internal market and boost the internal security of the EU.

Europe will remain vulnerable without a substantial effort to enhance public and private capacities, resources and processes to prevent, detect and handle cyber security incidents. This is why the Commission has developed a policy on Network and Information Security (NIS). The European Network and Information Security Agency ENISA was established in 2004 and a new Regulation to strengthen ENISA and modernise its mandate is being negotiated by Council and Parliament. In addition, the Framework Directive for electronic communications requires providers of electronic communications to appropriately manage the risks to their networks and to report significant security breaches. Also, the EU data protection legislation requires data controllers to ensure data protection requirements and safeguards, including measures related to security, and in the field of publicly available e-communication services, data controllers have to notify incidents involving a breach of personal data to the competent national authorities.

Despite progress based on voluntary commitments, there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders, and in terms of private sector involvement and preparedness. This strategy is accompanied by a proposal for legislation to notably:

- establish common minimum requirements for NIS at national level which would oblige Member States to: designate national competent authorities for NIS; set up a well-functioning CERT; and adopt a national NIS strategy and a national NIS cooperation plan. Capacity building and coordination also concern the EU institutions: a Computer Emergency Response Team responsible for the security of the IT systems of the EU institutions, agencies and bodies ("CERT-EU") was permanently established in 2012.

- set up coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national NIS competent authorities. National NIS competent authorities will be asked to ensure appropriate EU-wide cooperation, notably on the basis of a Union NIS cooperation plan, designed to respond to cyber incidents with cross-border dimension. This cooperation will

also build upon the progress made in the context of the "European Forum for Member States (EFMS)", which has held productive discussions and exchanges on NIS public policy and can be integrated in the cooperation mechanism once in place.

- improve preparedness and engagement of the private sector. Since the large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cybersecurity is crucial. The private sector should develop, at technical level, its own cyber resilience capacities and share best practices across sectors. The tools developed by industry to respond to incidents, identify causes and conduct forensic investigations should also benefit the public sector. However, private actors still lack effective incentives to provide reliable data on the existence or impact of NIS incidents, to embrace a risk management culture or to invest in security solutions. The proposed legislation therefore aims at making sure that players in a number of key areas (namely energy, transport, banking, stock exchanges, and enablers of key Internet services, as well as public administrations) assess the cybersecurity risks they face, ensure networks and information systems are reliable and resilient via appropriate risk management, and share the identified information with the national NIS competent authorities. The take up of a cybersecurity culture could enhance business opportunities and competitiveness in the private sector, which could make cybersecurity a selling point. Those entities would have to report, to the national NIS competent authorities, incidents with a significant impact on the continuity of core services and supply of goods relying on network and information systems. National NIS competent authorities should collaborate and exchange information with other regulatory bodies, and in particular personal data protection authorities. NIS competent authorities should in turn report incidents of a suspected serious criminal nature to law enforcement authorities. The national competent authorities should also regularly publish on a dedicated website unclassified information about on-going early warnings on incidents and risks and on coordinated responses. Legal obligations should neither substitute, nor prevent, developing informal and voluntary cooperation, including between public and private sectors, to boost security levels and exchange information and best practices. In particular, the European Public-Private Partnership for Resilience (EP3R15) is a sound and valid platform at EU level and should be further developed.

The Connecting Europe Facility (CEF)¹⁶ would provide financial support for key infrastructure, linking up Member States' NIS capabilities and so making it easier to cooperate across the EU.

Finally, cyber incident exercises at EU level are essential to simulate cooperation among the Member States and the private sector. The first exercise involving the Member States was carried out in 2010 ("Cyber Europe 2010") and a second exercise, involving also the private sector, took place in October 2012 ("Cyber Europe 2012"). An EU-US table top exercise was carried out in November 2011 ("Cyber Atlantic 2011"). Further exercises are planned for the coming years, including with international partners.

The Commission will:

- Continue its activities, carried out by the Joint Research Centre in close coordination with Member States authorities and critical infrastructure owners and operators, on identifying NIS vulnerabilities of European critical infrastructure and encouraging the development of resilient systems.

- Launch an EU-funded pilot project early in 2013 on fighting botnets and malware, to provide a framework for coordination and cooperation between EU Member States, private sector organisations such as Internet Service Providers, and international partners.

The Commission asks ENISA to:

- Assist the Member States in developing strong national cyber resilience capabilities, notably by building expertise on security

and resilience of industrial control systems, transport and energy infrastructure

☒ Examine in 2013 the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs) for the EU.

☒ Continue supporting the Member States and the EU institutions in carrying out regular pan-European cyber incident exercises which will also constitute the operational basis for the EU participation in international cyber incident exercises.

The Commission invites the European Parliament and the Council to:

☒ Swiftly adopt the proposal for a Directive on a common high level of Network and Information Security (NIS) across the Union, addressing national capabilities and preparedness, EU-level cooperation, take up of risk management practices and information sharing on NIS.

The Commission asks industry to:

☒ Take leadership in investing in a high level of cybersecurity and develop best practices and information sharing at sector level and with public authorities with the view of ensuring a strong and effective protection of assets and individuals, in particular through public-private partnerships like EP3R and Trust in Digital Life (TDL).

Raising awareness

Ensuring cybersecurity is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them.

Several initiatives have been developed in recent years and should be continued. In particular, ENISA has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships. Europol, Eurojust and national data protection authorities are also active in raising awareness. In October 2012, ENISA, with some Member States, piloted the "European Cybersecurity Month". Raising awareness is one of the areas the EU-US Working Group on Cybersecurity and Cybercrime is taking forward, and is also essential in the context of the Safer Internet Programme (focused on the safety of children online).

The Commission asks ENISA to:

☒ Propose in 2013 a roadmap for a "Network and Information Security driving licence" as a voluntary certification programme to promote enhanced skills and competence of IT professionals (e.g. website administrators).

The Commission will:☒

☒ Organise, with the support of ENISA, a cybersecurity championship in 2014, where university students will compete in proposing NIS solutions.

The Commission invites the Member States to:

Organise a yearly cybersecurity month with the support of ENISA and the involvement of the private sector from 2013 onwards, with the goal to raise awareness among end users. A synchronised EU-US cybersecurity month will be organised starting in 2014.

Step up national efforts on NIS education and training, by introducing: training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations. ☒The Commission invites industry to:

☒ Promote cybersecurity awareness at all levels, both in business practices and in the interface with customers. In particular, industry should reflect on ways to make CEOs and Boards more accountable for ensuring cybersecurity.

2.2. Drastically reducing cybercrime

The more we live in a digital world, the more opportunities for cyber criminals to exploit. Cybercrime is one of the fastest growing forms of crime, with more than one million people worldwide becoming victims each day. Cybercriminals and cybercrime networks are becoming increasingly sophisticated and we need to have the right operational tools and capabilities to tackle them. Cybercrimes are high-profit and low-risk, and

criminals often exploit the anonymity of website domains. Cybercrime knows no borders - the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative cross-border approach to respond to this growing threat.

Strong and effective legislation

The EU and the Member States need strong and effective legislation to tackle cybercrime. The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, is a binding international treaty that provides an effective framework for the adoption of national legislation.

The EU has already adopted legislation on cybercrime including a Directive on combating the sexual exploitation of children online and child pornography. The EU is also about to agree on a Directive on attacks against information systems, especially through the use of botnets.

The Commission will:

Ensure swift transposition and implementation of the cybercrime related Directives.

Urge those Member States that have not yet ratified the Council of Europe's Budapest Convention on Cybercrime to ratify and implement its provisions as early as possible.

Enhanced operational capability to combat cybercrime

The evolution of cybercrime techniques has accelerated rapidly: law enforcement agencies cannot combat cybercrime with outdated operational tools. Currently, not all EU Member States have the operational capability they need to effectively respond to cybercrime. All Member States need effective national cybercrime units.

The Commission will:

☒ Through its funding programmes, support the Member States to identify gaps and strengthen their capability to investigate and combat cybercrime. The Commission will furthermore support bodies that make the link between research/academia, law enforcement practitioners and the private sector, similar to the on-going work carried out by the Commission-funded Cybercrime Centres of Excellence already set up in some Member States.

Together with the Member States, coordinate efforts to identify best practices and best available techniques including with the support of JRC to fight cybercrime (e.g. with respect to the development and use of forensic tools or to threat analysis)

Work closely with the recently launched European Cybercrime Centre (EC3), within Europol and with Eurojust to align such policy approaches with best practices on the operational side.

Improved coordination at EU level

The EU can complement the work of Member States by facilitating a coordinated and collaborative approach, bringing together law enforcement and judicial authorities and public and private stakeholders from the EU and beyond.

The Commission will:

Support the recently launched European Cybercrime Centre (EC3) as the European focal point in the fight against cybercrime. The EC3 will provide analysis and intelligence, support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders, and gradually serve as a voice for the law enforcement community.

Support efforts to increase accountability of registrars of domain names and ensure accuracy of information on website ownership notably on the basis of the Law Enforcement Recommendations for the Internet Corporation for Assigned Names and Numbers (ICANN), in compliance with Union law, including the rules on data protection.

Build on recent legislation to continue strengthening the EU's efforts to tackle child sexual abuse online. The Commission has adopted a European Strategy for a Better Internet for Children and has, together with EU and non-EU countries, launched a Global Alliance against Child Sexual Abuse Online. The Alliance is a vehicle for further actions from the Member States

supported by the Commission and the EC3. The Commission asks Europol (EC3) to:

Initially focus its analytical and operational support to Member States' cybercrime investigations, to help dismantle and disrupt cybercrime networks primarily in the areas of child sexual abuse, payment fraud, botnets and intrusion.

On a regular basis produce strategic and operational reports on trends and emerging threats to identify priorities and target investigative action by cybercrime teams in the Member States. The Commission asks the European Police College (CEPOL) in cooperation with Europol to:

Coordinate the design and planning of training courses to equip law enforcement with the knowledge and expertise to effectively tackle cybercrime.

The Commission asks Eurojust to:

Identify the main obstacles to judicial cooperation on cybercrime investigations and to coordination between Member States and with third countries and support the investigation and prosecution of cybercrime both at the operational and strategic level as well as training activities in the field.

The Commission asks Eurojust and Europol (EC3) to:

Cooperate closely, inter alia through the exchange of information, in order to increase their effectiveness in combating cybercrime, in accordance with their respective mandates and competence.

2.3. Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)

Cybersecurity efforts in the EU also involve the cyber defence dimension. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyberdefence capability development should concentrate on detection, response and recovery from sophisticated cyber threats

Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, private sector and academia in the EU. To avoid duplications, the EU will explore possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures on which the members of both organisations depend.

The High Representative will focus on the following key activities and invite the Member States and the European Defence Agency to collaborate:

Assess operational EU cyberdefence requirements and promote the development of EU cyberdefence capabilities and technologies to address all aspects of capability development - including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability;

Develop the EU cyberdefence policy framework to protect networks within CSDP missions and operations, including dynamic risk management, improved threat analysis and information sharing. Improve Cyber Defence Training & Exercise Opportunities for the military in the European and multinational context including the integration of Cyber Defence elements in existing exercise catalogues;

Promote dialogue and coordination between civilian and military actors in the EU - with particular emphasis on the exchange of good practices, information exchange and early warning, incident response, risk assessment, awareness raising and establishing cybersecurity as a priority

Ensure dialogue with international partners, including NATO, other international organisations and multinational Centres of Excellence, to ensure effective defence capabilities, identify areas for cooperation and avoid duplication of efforts.

2.4. Develop industrial and technological resources for cybersecurity

Europe has excellent research and development capacities, but many of the global leaders providing innovative ICT products

and services are located outside the EU. There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers. It is key to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data.

Promoting a Single Market for cybersecurity products

A high level of security can only be ensured if all in the value chain (e.g. equipment manufacturers, software developers, information society services providers) make security a priority. It seems however that many players still regard security as little more than an additional burden and there is limited demand for security solutions. There need to be appropriate cybersecurity performance requirements implemented across the whole value chain for ICT products used in Europe. The private sector needs incentives to ensure a high level of cybersecurity; for example, labels indicating adequate cybersecurity performance will enable companies with a good cybersecurity performance and track record to make it a selling point and get a competitive edge. Also, the obligations set out in the proposed NIS Directive would significantly contribute to step up business competitiveness in the sectors covered.

A Europe-wide market demand for highly secure products should also be stimulated. First, this strategy aims to increase cooperation and transparency about security in ICT products. It calls for the establishment of a platform, bringing together relevant European public and private stakeholders, to identify good cybersecurity practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions. A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally. The Commission will promote the adoption of coherent approaches among the Member States to avoid disparities causing locational disadvantages for businesses.

Second, the Commission will support the development of security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing, while taking in due account the need to ensure data protection. Work should focus on the security of the supply chain, in particular in critical economic sectors (Industrial Control Systems, energy and transport infrastructure). Such work should build on the on-going standardisation work of the European Standardisation Organisations (CEN, CENELEC and ETSI), of the Cybersecurity Coordination Group (CSCG) as well as on the expertise of ENISA, the Commission and other relevant players.

The Commission will:

Launch in 2013 a public-private platform on NIS solutions to develop incentives for the adoption of secure ICT solutions and the take-up of good cybersecurity performance to be applied to ICT products used in Europe.

Propose in 2014 recommendations to ensure cybersecurity across the ICT value chain, drawing on the work of this platform
Examine how major providers of ICT hardware and software could inform national competent authorities on detected vulnerabilities that could have significant security-implications. The Commission asks ENISA to:

Develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardisation bodies and the European Commission Joint Research Centre, technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.

The Commission invites public and private stakeholders to:

Stimulate the development and adoption of industry-led security standards, technical norms and security-by-design and privacy-by-design principles by ICT product manufacturers and service providers, including cloud providers; new

generations of software and hardware should be equipped with stronger, embedded and user-friendly security features.

Develop industry-led standards for companies' performance on cybersecurity and improve the information available to the public by developing security labels or kite marks helping the consumer navigate the market.

Fostering R&D investments and innovation

R&D can support a strong industrial policy, promote a trustworthy European ICT industry, boost the internal market and reduce European dependence on foreign technologies. R&D should fill the technology gaps in ICT security, prepare for the next generation of security challenges, take into account the constant evolution of user needs and reap the benefits of dual use technologies. It should also continue supporting the development of cryptography. This has to be complemented by efforts to translate R&D results into commercial solutions by providing the necessary incentives and putting in place the appropriate policy conditions.

The EU should make the best of the Horizon 2020 Framework Programme for Research and Innovation, to be launched in 2014. The Commission's proposal contains specific objectives for trustworthy ICT as well as for combating cyber-crime, which are in line with this strategy. Horizon 2020 will support security research related to emerging ICT technologies; provide solutions for end-to-end secure ICT systems, services and applications; provide the incentives for the implementation and adoption of existing solutions; and address interoperability among network and information systems. Specific attention will be drawn at EU level to optimising and better coordinating various funding programmes (Horizon 2020, Internal Security Fund, EDA research including European Framework Cooperation).

The Commission will:

Use Horizon 2020 to address a range of areas in ICT privacy and security, from R&D to innovation and deployment. Horizon 2020 will also develop tools and instruments to fight criminal and terrorist activities targeting the cyber environment.

Establish mechanisms for better coordination of the research agendas of the European Union institutions and the Member States, and incentivise the Member States to invest more in R&D. ☐The Commission invites the Member States to:

Develop, by the end of 2013, good practices to use the purchasing power of public administrations (such as via public procurement) to stimulate the development and deployment of security features in ICT products and services.

Promote early involvement of industry and academia in developing and coordinating solutions. This should be done by making the most of Europe's Industrial Base and associated R&D technological innovations, and be coordinated between the research agendas of civilian and military organisations;

☐The Commission asks Europol and ENISA to:

☐ Identify emerging trends and needs in view of evolving cybercrime and cybersecurity patterns so as to develop adequate digital forensic tools and technologies.

The Commission invites public and private stakeholders to:

☐ Develop, in cooperation with the insurance sector, harmonised metrics for calculating risk premiums, that would enable companies that have made investments in security to benefit from lower risk premiums.

2.5. Establish a coherent international cyberspace policy for the European Union and promote EU core values

Preserving open, free and secure cyberspace is a global challenge, which the EU should address together with the relevant international partners and organisations, the private sector and civil society.

In its international cyberspace policy, the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyberspace. The EU will also work towards closing the digital divide, and will actively participate in international efforts to build cybersecurity capacity. The EU international engagement in cyber issues will be guided by the

EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights. Mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy

The Commission, the High Representative and the Member States should articulate a coherent EU international cyberspace policy, which will be aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and private sector. EU consultations with international partners on cyber issues should be designed, coordinated and implemented to add value to existing bilateral dialogues between the EU's Member States and third countries. The EU will place a renewed emphasis on dialogue with third countries, with a special focus on like-minded partners that share EU values. It will promote achieving a high level of data protection, including for transfer to a third country of personal data. To address global challenges in cyberspace, the EU will seek closer cooperation with organisations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS. At bilateral level, cooperation with the United States is particularly important and will be further developed, notably in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime.

One of the major elements of the EU international cyber policy will be to promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance. The EU should promote corporate social responsibility, and launch international initiatives to improve global coordination in this field.

The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments. The EU supports the efforts to define norms of behaviour in cyberspace that all stakeholders should adhere to. Just as the EU expects citizens to respect civic duties, social responsibilities and laws online, so should states abide by norms and existing laws. On matters of international security, the EU encourages the development of confidence building measures in cybersecurity, to increase transparency and reduce the risk of misperceptions in state behaviour.

The EU does not call for the creation of new international legal instruments for cyber issues.

The legal obligations enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should be also respected online. The EU will focus on how to ensure that these measures are enforced also in cyberspace.

To address cybercrime, the Budapest Convention is an instrument open for adoption by third countries. It provides a model for drafting national cybercrime legislation and a basis for international co-operation in this field. If armed conflicts extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights law will apply to the case at hand. Developing capacity building on cybersecurity and resilient information infrastructures in third countries

The smooth functioning of the underlying infrastructures that provide and facilitate communication services will benefit from increased international cooperation. This includes exchanging best practices, sharing information, early warning joint incident management exercises, and so on. The EU will contribute towards this goal by intensifying the on-going international efforts to strengthen Critical Information Infrastructure Protection (CIIP) cooperation networks involving governments and the private sector.

Not all parts of the world benefit from the positive effects of the Internet, due to a lack of open, secure, interoperable and reliable access. The European Union will therefore continue to support countries' efforts in their quest to develop the access and use of the Internet for their people, to ensure its integrity and security and to effectively fight cybercrime.

In cooperation with the Member States, the Commission and the High Representative will:

Work towards a coherent EU International cyberspace policy to increase engagement with key international partners and organisations, to mainstream cyber issues into CFSP, and to improve coordination of global cyber issues;

Support the development of norms of behaviour and confidence building measures in cybersecurity. Facilitate dialogues on how to apply existing international law in cyberspace and promote the Budapest Convention to address cybercrime;

Support the promotion and protection of fundamental rights, including access to information and freedom of expression, focusing on: a) developing new public guidelines on freedom of expression online and offline; b) monitoring the export of products or services that might be used for censorship or mass surveillance online; c) developing measures and tools to expand Internet access, openness and resilience to address censorship or mass surveillance by communication technology; d) empowering stakeholders to use communication technology to promote fundamental rights;

Engage with international partners and organisations, the private sector and civil society to support global capacity-building in third countries to improve access to information and to an open Internet, to prevent and counter cyber threats, including accidental events, cybercrime and cyber terrorism, and to develop donor coordination for steering capacity-building efforts;

Utilise different EU aid instruments for cybersecurity capacity building, including assisting the training of law enforcement, judicial and technical personnel to address cyber threats; as well as supporting the creation of relevant national policies, strategies and institutions in third countries;

Increase policy coordination and information sharing through the international Critical Information Infrastructure Protection networks such as the Meridian network, cooperation among NIS competent authorities and others.

3. ROLES AND RESPONSIBILITIES

Cyber incidents do not stop at borders in the interconnected digital economy and society. All actors, from NIS competent authorities, CERTs and law enforcement to industry, must take responsibility both nationally and at EU-level and work together to strengthen cybersecurity. As different legal frameworks and jurisdictions may be involved, a key challenge for the EU is to clarify the roles and responsibilities of the many actors involved.

Given the complexity of the issue and the diverse range of actors involved, centralised, European supervision is not the answer. National governments are best placed to organise the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks. At the same time, due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement. To address cybersecurity in a comprehensive fashion, activities should span across three key pillars— NIS, law enforcement, and defence—which also operate within different legal frameworks:

Industry Academia

3.1. Coordination between NIS competent authorities/CERTs, law enforcement and defence

National level

Member States should have, either already today or as a result of this strategy, structures to deal with cyber resilience, cybercrime and defence; and they should reach the required level of capability to deal with cyber incidents. However, given that a number of entities may have operational responsibilities over different dimensions of cybersecurity, and given the importance of involving the private sector, coordination at national level should be optimised across ministries. Member States should set out in their national cybersecurity strategies the roles and responsibilities of their various national entities. Information sharing between national entities and with the private sector should be encouraged, to enable the Member States and the private sector to maintain an overall view of

different threats and get a better understanding of new trends and techniques used both to commit cyber-attacks and react to them more swiftly. By establishing national NIS cooperation plans to be activated in the case of cyber incidents, the Member States should be able to clearly allocate roles and responsibilities and optimise response actions.

EU level

Just as at national level, there are at EU level a number of actors dealing with cybersecurity. In particular, the ENISA, Europol/EC3 and the EDA are three agencies active from the perspective of NIS, law enforcement and defence respectively. These agencies have Management Boards where the Member States are represented, and offer platforms for coordination at EU level.

Coordination and collaboration will be encouraged among ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, risk assessment, training and sharing of best practices. They should collaborate while preserving their specificities. These agencies together with CERT-EU, the Commission and the Member States should support the development of a trusted community of technical and policy experts in this field.

Informal channels for coordination and collaboration will be complemented by more structural links. EU military staff and the EDA cyber defence project team can be used as the vector for coordination in defence. The Programme Board of Europol/EC3 will bring together among others the EUROJUST, CEPOL, the Member States, ENISA and the Commission, and offer the chance to share their distinct know-how and to make sure EC3's actions are carried out in partnership, recognising the added expertise and respecting the mandates of all stakeholders. The new mandate of ENISA should make it possible to increase its links with Europol and to reinforce links with industry stakeholders. Most importantly, the Commission's legislative proposal on NIS) would establish a cooperation framework via a network of national NIS competent authorities and address information sharing between NIS and law enforcement authorities.

International

The Commission and the High Representative ensure, together with the Member States, coordinated international action in the field of cybersecurity. In so doing, the Commission and the High Representative will uphold EU core values and promote a peaceful, open and transparent use of cyber technologies. The Commission, the High Representative and the Member States engage in policy dialogue with international partners and with international organisations such as Council of Europe, OECD, OSCE, NATO and UN.

3.2. EU support in case of a major cyber incident or attack

Major cyber incidents or attacks are likely to have an impact on EU governments, business and individuals. As a result of this strategy, and in particular the proposed Directive on NIS, the prevention, detection and response to cyber incidents should improve and Member States and the Commission should keep each other more closely informed about major cyber incidents or attacks. However, the response mechanisms will differ depending on the nature, magnitude and cross-border implications of the incident.

If the incident has a serious impact on the business continuity, the NIS Directive proposes that national or Union NIS cooperation plans be triggered, depending on the cross-border nature of the incident. The network of NIS competent authorities would be used in that context to share information and support. This would enable preservation and/or restoration of affected networks and services.

If the incident seems to relate to a crime, Europol/EC3 should be informed so that they - together with the law enforcement authorities from the affected countries - can launch an investigation, preserve the evidence, identify the perpetrators and ultimately make sure they are prosecuted.

If the incident seems to relate to cyber espionage or a state-sponsored attack, or has national security implications, national security and defence authorities will alert their relevant counterparts, so that they know they are under attack

and can defend themselves. Early warning mechanisms will then be activated and, if required, so will crisis management or other procedures. A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union).

If the incident seems having compromised personal data, the national Data Protection Authorities or the national regulatory authority pursuant to Directive 2002/58/EC should be involved.

Finally, the handling of cyber incidents and attacks will benefit from contact networks and support from international partners. This may include technical mitigation, criminal investigation, or activation of crisis management response mechanisms.

4. CONCLUSION AND FOLLOW-UP

This proposed cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, outlines the

EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world.

This vision can only be realised through a true partnership, between many actors, to take responsibility and meet the challenges ahead.

The Commission and the High Representative therefore invite the Council and the European Parliament to endorse the strategy and to help deliver the outlined actions. Strong support and commitment is also needed from the private sector and civil society, who are key actors to enhance our level of security and safeguard citizens' rights. The time to act is now. The Commission and the High Representative are determined to work together with all actors to deliver the security needed for Europe. To ensure that the strategy is being implemented promptly and assessed in the face of possible developments, they will gather together all relevant parties in a high-level conference and assess progress in 12 months.

VII. Copyright Law

Berne Convention for the Protection of Literary and Artistic Works

Paris Act of July 24, 1971,
as amended on September 28, 1979 Berne Convention for the
Protection of Literary and Artistic Works of September 9, 1886,
completed at PARIS on May 4, 1896,
revised at BERLIN on November 13, 1908,
completed at BERNE on March 20, 1914,
revised at ROME on June 2, 1928,
at BRUSSELS on June 26, 1948,
at STOCKHOLM on July 14, 1967, and
at PARIS on July 24, 1971,
and amended on September 28, 1979

The countries of the Union, being equally animated by the
desire to protect, in as effective and uniform a manner as
possible, the rights of authors in their literary and artistic
works,
Recognizing the importance of the work of the Revision
Conference held at Stockholm in 1967,
Have resolved to revise the Act adopted by the Stockholm
Conference, while maintaining without change Articles 1 to 20
and 22 to 26 of that Act.
Consequently, the undersigned Plenipotentiaries, having
presented their full powers, recognized as in good and due
form, have agreed as follows:

Article 1

[Establishment of a Union][...]

1 Each Article and the Appendix have been given titles to
facilitate their identification. There are no titles in the signed
(English) text.

The countries to which this Convention applies constitute a
Union for the protection of the rights of authors in their literary
and artistic works.

Article 2

[Protected Works: 1. "Literary and artistic works"; 2. Possible
requirement of fixation; 3. Derivative works; 4. Official texts; 5.
Collections; 6. Obligation to protect; beneficiaries of
protection; 7. Works of applied art and industrial designs; 8.

News]

(1) The expression "literary and artistic works" shall include
every production in the literary, scientific and artistic domain,
whatever may be the mode or form of its expression, such as
books, pamphlets and other writings; lectures, addresses,
sermons and other works of the same nature; dramatic or
dramatico-musical works; choreographic works and
entertainments in dumb show; musical compositions with or
without words; cinematographic works to which are
assimilated works expressed by a process analogous to
cinematography; works of drawing, painting, architecture,
sculpture, engraving and lithography; photographic works to
which are assimilated works expressed by a process analogous
to photography; works of applied art; illustrations, maps, plans,
sketches and three-dimensional works relative to geography,
topography, architecture or science.

(2) It shall, however, be a matter for legislation in the countries
of the Union to prescribe that works in general or any specified

categories of works shall not be protected unless they have
been fixed in some material form.

(3) Translations, adaptations, arrangements of music and other
alterations of a literary or artistic work shall be protected as
original works without prejudice to the copyright in the original
work.

(4) It shall be a matter for legislation in the countries of the
Union to determine the protection to be granted to official texts
of a legislative, administrative and legal nature, and to official
translations of such texts.

(5) Collections of literary or artistic works such as
encyclopaedias and anthologies which, by reason of the
selection and arrangement of their contents, constitute
intellectual creations shall be protected as such, without
prejudice to the copyright in each of the works forming part of
such collections.

(6) The works mentioned in this Article shall enjoy protection
in all countries of the Union. This protection shall operate for
the benefit of the author and his successors in title.

(7) Subject to the provisions of Article 7(4) of this Convention,
it shall be a matter for legislation in the countries of the Union
to determine the extent of the application of their laws to works
of applied art and industrial designs and models, as well as the
conditions under which such works, designs and models shall
be protected. Works protected in the country of origin solely as
designs and models shall be entitled in another country of the
Union only to such special protection as is granted in that
country to designs and models; however, if no such special
protection is granted in that country, such works shall be
protected as artistic works.

(8) The protection of this Convention shall not apply to news of
the day or to miscellaneous facts having the character of mere
items of press information.

Article 2bis

[Possible Limitation of Protection of Certain Works: 1. Certain
speeches; 2. Certain uses of lectures and addresses; 3. Right to
make collections of such works]

(1) It shall be a matter for legislation in the countries of the
Union to exclude, wholly or in part, from the protection
provided by the preceding Article political speeches and
speeches delivered in the course of legal proceedings.

(2) It shall also be a matter for legislation in the countries of the
Union to determine the conditions under which lectures,
addresses and other works of the same nature which are
delivered in public may be reproduced by the press, broadcast,
communicated to the public by wire and made the subject of
public communication as envisaged in Article 11bis(1) of this
Convention, when such use is justified by the informatory
purpose.

(3) Nevertheless, the author shall enjoy the exclusive right of
making a collection of his works mentioned in the preceding
paragraphs.

Article 3

[Criteria of Eligibility for Protection: 1. Nationality of author;
place of publication of work; 2. Residence of author; 3.
"Published" works; 4. "Simultaneously published" works]

(1) The protection of this Convention shall apply to:
(a) authors who are nationals of one of the countries of the Union, for their works, whether published or not;
(b) authors who are not nationals of one of the countries of the Union, for their works first published in one of those countries, or simultaneously in a country outside the Union and in a country of the Union.

(2) Authors who are not nationals of one of the countries of the Union but who have their habitual residence in one of them shall, for the purposes of this Convention, be assimilated to nationals of that country.

(3) The expression "published works" means works published with the consent of their authors, whatever may be the means of manufacture of the copies, provided that the availability of such copies has been such as to satisfy the reasonable requirements of the public, having regard to the nature of the work. The performance of a dramatic, dramatico-musical, cinematographic or musical work, the public recitation of a literary work, the communication by wire or the broadcasting of literary or artistic works, the exhibition of a work of art and the construction of a work of architecture shall not constitute publication.

(4) A work shall be considered as having been published simultaneously in several countries if it has been published in two or more countries within thirty days of its first publication.

Article 4

[Criteria of Eligibility for Protection of Cinematographic Works, Works of Architecture and Certain Artistic Works]

The protection of this Convention shall apply, even if the conditions of Article 3 are not fulfilled, to:

(a) authors of cinematographic works the maker of which has his headquarters or habitual residence in one of the countries of the Union;

(b) authors of works of architecture erected in a country of the Union or of other artistic works incorporated in a building or other structure located in a country of the Union.

Article 5

[Rights Guaranteed: 1. and 2. Outside the country of origin; 3.

In the country of origin; 4. "Country of origin"]

(1) Authors shall enjoy, in respect of works for which they are protected under this Convention, in countries of the Union other than the country of origin, the rights which their respective laws do now or may hereafter grant to their nationals, as well as the rights specially granted by this Convention.

(2) The enjoyment and the exercise of these rights shall not be subject to any formality; such enjoyment and such exercise shall be independent of the existence of protection in the country of origin of the work. Consequently, apart from the provisions of this Convention, the extent of protection, as well as the means of redress afforded to the author to protect his rights, shall be governed exclusively by the laws of the country where protection is claimed.

(3) Protection in the country of origin is governed by domestic law. However, when the author is not a national of the country of origin of the work for which he is protected under this Convention, he shall enjoy in that country the same rights as national authors.

(4) The country of origin shall be considered to be:

(a) in the case of works first published in a country of the Union, that country; in the case of works published simultaneously in several countries of the Union which grant different terms of protection, the country whose legislation grants the shortest term of protection;

(b) in the case of works published simultaneously in a country outside the Union and in a country of the Union, the latter country;

(c) in the case of unpublished works or of works first published in a country outside the Union, without simultaneous publication in a country of the Union, the country of the Union of which the author is a national, provided that:

(i) when these are cinematographic works the maker of which has his headquarters or his habitual residence in a country of the Union, the country of origin shall be that country, and

(ii) when these are works of architecture erected in a country of the Union or other artistic works incorporated in a building or other structure located in a country of the Union, the country of origin shall be that country.

Article 6

[Possible Restriction of Protection in Respect of Certain Works of Nationals of Certain Countries Outside the Union: 1. In the country of the first publication and in other countries; 2. No retroactivity; 3. Notice]

(1) Where any country outside the Union fails to protect in an adequate manner the works of authors who are nationals of one of the countries of the Union, the latter country may restrict the protection given to the works of authors who are, at the date of the first publication thereof, nationals of the other country and are not habitually resident in one of the countries of the Union. If the country of first publication avails itself of this right, the other countries of the Union shall not be required to grant to works thus subjected to special treatment a wider protection than that granted to them in the country of first publication.

(2) No restrictions introduced by virtue of the preceding paragraph shall affect the rights which an author may have acquired in respect of a work published in a country of the Union before such restrictions were put into force.

(3) The countries of the Union which restrict the grant of copyright in accordance with this Article shall give notice thereof to the Director General of the World Intellectual Property Organization (hereinafter designated as "the Director General") by a written declaration specifying the countries in regard to which protection is restricted, and the restrictions to which rights of authors who are nationals of those countries are subjected. The Director General shall immediately communicate this declaration to all the countries of the Union.

Article 6bis

[Moral Rights: 1. To claim authorship; to object to certain modifications and other derogatory actions; 2. After the author's death; 3. Means of redress]

(1) Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation.

(2) The rights granted to the author in accordance with the preceding paragraph shall, after his death, be maintained, at least until the expiry of the economic rights, and shall be exercisable by the persons or institutions authorized by the legislation of the country where protection is claimed. However, those countries whose legislation, at the moment of their ratification of or accession to this Act, does not provide for the protection after the death of the author of all the rights set out in the preceding paragraph may provide that some of these rights may, after his death, cease to be maintained.

(3) The means of redress for safeguarding the rights granted by this Article shall be governed by the legislation of the country where protection is claimed.

Article 7

[Term of Protection: 1. Generally; 2. For cinematographic works; 3. For anonymous and pseudonymous works; 4. For photographic works and works of applied art; 5. Starting date of computation; 6. Longer terms; 7. Shorter terms; 8. Applicable law; "comparison" of terms]

(1) The term of protection granted by this Convention shall be the life of the author and fifty years after his death.

(2) However, in the case of cinematographic works, the countries of the Union may provide that the term of protection shall expire fifty years after the work has been made available to the public with the consent of the author, or, failing such an

event within fifty years from the making of such a work, fifty years after the making.

(3) In the case of anonymous or pseudonymous works, the term of protection granted by this Convention shall expire fifty years after the work has been lawfully made available to the public. However, when the pseudonym adopted by the author leaves no doubt as to his identity, the term of protection shall be that provided in paragraph (1). If the author of an anonymous or pseudonymous work discloses his identity during the above-mentioned period, the term of protection applicable shall be that provided in paragraph (1). The countries of the Union shall not be required to protect anonymous or pseudonymous works in respect of which it is reasonable to presume that their author has been dead for fifty years.

(4) It shall be a matter for legislation in the countries of the Union to determine the term of protection of photographic works and that of works of applied art in so far as they are protected as artistic works; however, this term shall last at least until the end of a period of twenty-five years from the making of such a work.

(5) The term of protection subsequent to the death of the author and the terms provided by paragraph (2), paragraph (3) and paragraph (4) shall run from the date of death or of the event referred to in those paragraphs, but such terms shall always be deemed to begin on the first of January of the year following the death or such event.

(6) The countries of the Union may grant a term of protection in excess of those provided by the preceding paragraphs.

(7) Those countries of the Union bound by the Rome Act of this Convention which grant, in their national legislation in force at the time of signature of the present Act, shorter terms of protection than those provided for in the preceding paragraphs shall have the right to maintain such terms when ratifying or acceding to the present Act.

(8) In any case, the term shall be governed by the legislation of the country where protection is claimed; however, unless the legislation of that country otherwise provides, the term shall not exceed the term fixed in the country of origin of the work.

Article 7bis

[Term of Protection for Works of Joint Authorship]

The provisions of the preceding Article shall also apply in the case of a work of joint authorship, provided that the terms measured from the death of the author shall be calculated from the death of the last surviving author.

Article 8

[Right of Translation]

Authors of literary and artistic works protected by this Convention shall enjoy the exclusive right of making and of authorizing the translation of their works throughout the term of protection of their rights in the original works.

Article 9

[Right of Reproduction: 1. Generally; 2. Possible exceptions; 3. Sound and visual recordings]

(1) Authors of literary and artistic works protected by this Convention shall have the exclusive right of authorizing the reproduction of these works, in any manner or form.

(2) It shall be a matter for legislation in the countries of the Union to permit the reproduction of such works in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author.

(3) Any sound or visual recording shall be considered as a reproduction for the purposes of this Convention.

Article 10

[Certain Free Uses of Works: 1. Quotations; 2. Illustrations for teaching; 3. Indication of source and author]

(1) It shall be permissible to make quotations from a work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose,

including quotations from newspaper articles and periodicals in the form of press summaries.

(2) It shall be a matter for legislation in the countries of the Union, and for special agreements existing or to be concluded between them, to permit the utilization, to the extent justified by the purpose, of literary or artistic works by way of illustration in publications, broadcasts or sound or visual recordings for teaching, provided such utilization is compatible with fair practice.

(3) Where use is made of works in accordance with the preceding paragraphs of this Article, mention shall be made of the source, and of the name of the author if it appears thereon.

Article 10bis

[Further Possible Free Uses of Works: 1. Of certain articles and broadcast works; 2. Of works seen or heard in connection with current events]

(1) It shall be a matter for legislation in the countries of the Union to permit the reproduction by the press, the broadcasting or the communication to the public by wire of articles published in newspapers or periodicals on current economic, political or religious topics, and of broadcast works of the same character, in cases in which the reproduction, broadcasting or such communication thereof is not expressly reserved. Nevertheless, the source must always be clearly indicated; the legal consequences of a breach of this obligation shall be determined by the legislation of the country where protection is claimed.

(2) It shall also be a matter for legislation in the countries of the Union to determine the conditions under which, for the purpose of reporting current events by means of photography, cinematography, broadcasting or communication to the public by wire, literary or artistic works seen or heard in the course of the event may, to the extent justified by the informative purpose, be reproduced and made available to the public.

Article 11

[Certain Rights in Dramatic and Musical Works: 1. Right of public performance and of communication to the public of a performance; 2. In respect of translations]

(1) Authors of dramatic, dramatico-musical and musical works shall enjoy the exclusive right of authorizing:

(i) the public performance of their works, including such public performance by any means or process;

(ii) any communication to the public of the performance of their works.

(2) Authors of dramatic or dramatico-musical works shall enjoy, during the full term of their rights in the original works, the same rights with respect to translations thereof.

Article 11bis

[Broadcasting and Related Rights: 1. Broadcasting and other wireless communications, public communication of broadcast by wire or rebroadcast, public communication of broadcast by loudspeaker or analogous instruments; 2. Compulsory licenses; 3. Recording; ephemeral recordings]

(1) Authors of literary and artistic works shall enjoy the exclusive right of authorizing:

(i) the broadcasting of their works or the communication thereof to the public by any other means of wireless diffusion of signs, sounds or images;

(ii) any communication to the public by wire or by rebroadcasting of the broadcast of the work, when this communication is made by an organization other than the original one;

(iii) the public communication by loudspeaker or any other analogous instrument transmitting, by signs, sounds or images, the broadcast of the work.

(2) It shall be a matter for legislation in the countries of the Union to determine the conditions under which the rights mentioned in the paragraph 1 may be exercised, but these conditions shall apply only in the countries where they have been prescribed. They shall not in any circumstances be prejudicial to the moral rights of the author, nor to his right to

obtain equitable remuneration which, in the absence of agreement, shall be fixed by competent authority.

(3) In the absence of any contrary stipulation, permission granted in accordance with paragraph (1) of this Article shall not imply permission to record, by means of instruments recording sounds or images, the work broadcast. It shall, however, be a matter for legislation in the countries of the Union to determine the Regulations for ephemeral recordings made by a broadcasting organization by means of its own facilities and used for its own broadcasts. The preservation of these recordings in official archives may, on the ground of their exceptional documentary character, be authorized by such legislation.

Article 11ter

[Certain Rights in Literary Works: 1. Right of public recitation and of communication to the public of a recitation; 2. In respect of translations]

(1) Authors of literary works shall enjoy the exclusive right of authorizing:

(i) the public recitation of their works, including such public recitation by any means or process;

(ii) any communication to the public of the recitation of their works.

(2) Authors of literary works shall enjoy, during the full term of their rights in the original works, the same rights with respect to translations thereof.

Article 12

[Right of Adaptation, Arrangement and Other Alteration]

Authors of literary or artistic works shall enjoy the exclusive right of authorizing adaptations, arrangements and other alterations of their works.

Article 13

[Possible Limitation of the Right of Recording of Musical Works and Any Words Pertaining Thereto: 1. Compulsory licenses; 2. Transitory measures; 3. Seizure on importation of copies made without the author's permission]

(1) Each country of the Union may impose for itself reservations and conditions on the exclusive right granted to the author of a musical work and to the author of any words, the recording of which together with the musical work has already been authorized by the latter, to authorize the sound recording of that musical work, together with such words, if any; but all such reservations and conditions shall apply only in the countries which have imposed them and shall not, in any circumstances, be prejudicial to the rights of these authors to obtain equitable remuneration which, in the absence of agreement, shall be fixed by competent authority.

(2) Recordings of musical works made in a country of the Union in accordance with Article 13(3) of the Conventions signed at Rome on June 2, 1928, and at Brussels on June 26, 1948, may be reproduced in that country without the permission of the author of the musical work until a date two years after that country becomes bound by this Act.

(3) Recordings made in accordance with paragraph (1) and paragraph (2) of this Article and imported without permission from the parties concerned into a country where they are treated as infringing recordings shall be liable to seizure.

Article 14

[Cinematographic and Related Rights: 1. Cinematographic adaptation and reproduction; distribution; public performance and public communication by wire of works thus adapted or reproduced; 2. Adaptation of cinematographic productions; 3. No compulsory licenses]

(1) Authors of literary or artistic works shall have the exclusive right of authorizing:

(i) the cinematographic adaptation and reproduction of these works, and the distribution of the works thus adapted or reproduced;

(ii) the public performance and communication to the public by wire of the works thus adapted or reproduced.

(2) The adaptation into any other artistic form of a cinematographic production derived from literary or artistic works shall, without prejudice to the authorization of the author of the cinematographic production, remain subject to the authorization of the authors of the original works.

(3) The provisions of Article 13(1) shall not apply.

Article 14bis

[Special Provisions Concerning Cinematographic Works: 1. Assimilation to "original" works; 2. Ownership; limitation of certain rights of certain contributors; 3. Certain other contributors]

(1) Without prejudice to the copyright in any work which may have been adapted or reproduced, a cinematographic work shall be protected as an original work. The owner of copyright in a cinematographic work shall enjoy the same rights as the author of an original work, including the rights referred to in the preceding Article.

(2)

(a) Ownership of copyright in a cinematographic work shall be a matter for legislation in the country where protection is claimed.

(b) However, in the countries of the Union which, by legislation, include among the owners of copyright in a cinematographic work authors who have brought contributions to the making of the work, such authors, if they have undertaken to bring such contributions, may not, in the absence of any contrary or special stipulation, object to the reproduction, distribution, public performance, communication to the public by wire, broadcasting or any other communication to the public, or to the subtitling or dubbing of texts, of the work.

(c) The question whether or not the form of the undertaking referred to above should, for the application of the preceding subparagraph (b), be in a written agreement or a written act of the same effect shall be a matter for the legislation of the country where the maker of the cinematographic work has his headquarters or habitual residence. However, it shall be a matter for the legislation of the country of the Union where protection is claimed to provide that the said undertaking shall be in a written agreement or a written act of the same effect. The countries whose legislation so provides shall notify the Director General by means of a written declaration, which will be immediately communicated by him to all the other countries of the Union.

(d) By "contrary or special stipulation" is meant any restrictive condition which is relevant to the aforesaid undertaking.

(3) Unless the national legislation provides to the contrary, the provisions of paragraph (2)(b) above shall not be applicable to authors of scenarios, dialogues and musical works created for the making of the cinematographic work, or to the principal director thereof. However, those countries of the Union whose legislation does not contain rules providing for the application of the said paragraph (2)(b) to such director shall notify the Director General by means of a written declaration, which will be immediately communicated by him to all the other countries of the Union.

Article 14ter

["Droit de suite" in Works of Art and Manuscripts: 1. Right to an interest in resales; 2. Applicable law; 3. Procedure]

(1) The author, or after his death the persons or institutions authorized by national legislation, shall, with respect to original works of art and original manuscripts of writers and composers, enjoy the inalienable right to an interest in any sale of the work subsequent to the first transfer by the author of the work.

(2) The protection provided by the preceding paragraph may be claimed in a country of the Union only if legislation in the country to which the author belongs so permits, and to the extent permitted by the country where this protection is claimed.

(3) The procedure for collection and the amounts shall be matters for determination by national legislation.

Article 15

[Right to Enforce Protected Rights: 1. Where author's name is indicated or where pseudonym leaves no doubt as to author's identity; 2. In the case of cinematographic works; 3. In the case of anonymous and pseudonymous works; 4. In the case of certain unpublished works of unknown authorship]

(1) In order that the author of a literary or artistic work protected by this Convention shall, in the absence of proof to the contrary, be regarded as such, and consequently be entitled to institute infringement proceedings in the countries of the Union, it shall be sufficient for his name to appear on the work in the usual manner. This paragraph shall be applicable even if this name is a pseudonym, where the pseudonym adopted by the author leaves no doubt as to his identity.

(2) The person or body corporate whose name appears on a cinematographic work in the usual manner shall, in the absence of proof to the contrary, be presumed to be the maker of the said work.

(3) In the case of anonymous and pseudonymous works, other than those referred to in paragraph (1) above, the publisher whose name appears on the work shall, in the absence of proof to the contrary, be deemed to represent the author, and in this capacity he shall be entitled to protect and enforce the author's rights. The provisions of this paragraph shall cease to apply when the author reveals his identity and establishes his claim to authorship of the work.

(4) (a) In the case of unpublished works where the identity of the author is unknown, but where there is every ground to presume that he is a national of a country of the Union, it shall be a matter for legislation in that country to designate the competent authority which shall represent the author and shall be entitled to protect and enforce his rights in the countries of the Union.

(b) Countries of the Union which make such designation under the terms of this provision shall notify the Director General by means of a written declaration giving full information concerning the authority thus designated. The Director General shall at once communicate this declaration to all other countries of the Union.

Article 16

[Infringing Copies: 1. Seizure; 2. Seizure on importation; 3. Applicable law]

(1) Infringing copies of a work shall be liable to seizure in any country of the Union where the work enjoys legal protection.

(2) The provisions of the preceding paragraph shall also apply to reproductions coming from a country where the work is not protected, or has ceased to be protected.

(3) The seizure shall take place in accordance with the legislation of each country.

Article 17

[Possibility of Control of Circulation, Presentation and Exhibition of Works]

The provisions of this Convention cannot in any way affect the right of the Government of each country of the Union to permit, to control, or to prohibit, by legislation or Regulation, the circulation, presentation, or exhibition of any work or production in regard to which the competent authority may find it necessary to exercise that right.

Article 18

[Works Existing on Convention's Entry Into Force: 1.

Protectable where protection not yet expired in country of origin; 2. Non-protectable where protection already expired in country where it is claimed; 3. Application of these principles; 4. Special cases]

(1) This Convention shall apply to all works which, at the moment of its coming into force, have not yet fallen into the public domain in the country of origin through the expiry of the term of protection.

(2) If, however, through the expiry of the term of protection which was previously granted, a work has fallen into the public domain of the country where protection is claimed, that work shall not be protected anew.

(3) The application of this principle shall be subject to any provisions contained in special conventions to that effect existing or to be concluded between countries of the Union. In the absence of such provisions, the respective countries shall determine, each in so far as it is concerned, the conditions of application of this principle.

(4) The preceding provisions shall also apply in the case of new accessions to the Union and to cases in which protection is extended by the application of Article 7 or by the abandonment of reservations.

Article 19

[Protection Greater than Resulting from Convention]

The provisions of this Convention shall not preclude the making of a claim to the benefit of any greater protection which may be granted by legislation in a country of the Union.

Article 20

[Special Agreements Among Countries of the Union]

The Governments of the countries of the Union reserve the right to enter into special agreements among themselves, in so far as such agreements grant to authors more extensive rights than those granted by the Convention, or contain other provisions not contrary to this Convention. The provisions of existing agreements which satisfy these conditions shall remain applicable.

[...]

Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations

The Contracting States, moved by the desire to protect the rights of performers, producers of phonograms, and broadcasting organisations, have agreed as follows:

Article 1

Safeguard of Copyright Proper²

Protection granted under this Convention shall leave intact and shall in no way affect the protection of copyright in literary and artistic works. Consequently, no provision of this Convention may be interpreted as prejudicing such protection.

Article 2

Protection given by the Convention.

Definition of National Treatment

1. For the purposes of this Convention, national treatment shall mean the treatment accorded by the domestic law of the Contracting State in which protection is claimed:

(a) to performers who are its nationals, as regards performances taking place, broadcast, or first fixed, on its territory;

(b) to producers of phonograms who are its nationals, as regards phonograms first fixed or first published on its territory;

(c) to broadcasting organisations which have their headquarters on its territory, as regards broadcasts transmitted from transmitters situated on its territory.

2. National treatment shall be subject to the protection specifically guaranteed, and the limitations specifically provided for, in this Convention.

Article 3

Definitions: (a) Performers; (b) Phonogram; (c) Producers of Phonograms;

(d) Publication; (e) Reproduction; (f) Broadcasting; (g) Rebroadcasting

For the purposes of this Convention:

(a) "performers" means actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, or otherwise perform literary or artistic works;

(b) "phonogram" means any exclusively aural fixation of sounds of a performance or of other sounds;

(c) "producer of phonograms" means the person who, or the legal entity which, first fixes the sounds of a performance or other sounds;

(d) "publication" means the offering of copies of a phonogram to the public in reasonable quantity;

(e) "reproduction" means the making of a copy or copies of a fixation;

(f) "broadcasting" means the transmission by wireless means for public reception of sounds or of images and sounds;

(g) "rebroadcasting" means the simultaneous broadcasting by one broadcasting organisation of the broadcast of another broadcasting organisation.

Article 4

Performances Protected.

Points of Attachment for Performers

Each Contracting State shall grant national treatment to performers if any of the following conditions is met:

(a) the performance takes place in another Contracting State;

(b) the performance is incorporated in a phonogram which is protected under Article 5 of this Convention;

(c) the performance, not being fixed on a phonogram, is carried by a broadcast which is protected by Article 6 of this Convention.

Article 5

Protected Phonograms: 1. Points of Attachment for Producers of Phonograms;

2. Simultaneous Publication; 3. Power to exclude certain Criteria

1. Each Contracting State shall grant national treatment to producers of phonograms if any of the following conditions is met:

(a) the producer of the phonogram is a national of another Contracting State (criterion of nationality);

(b) the first fixation of the sound was made in another Contracting State (criterion of fixation);

(c) the phonogram was first published in another Contracting State (criterion of publication).

2. If a phonogram was first published in a non-contracting State but if it was also published, within thirty days of its first publication, in a Contracting State (simultaneous publication), it shall be considered as first published in the Contracting State.

3. By means of a notification deposited with the Secretary-General of the United Nations, any Contracting State may declare that it will not apply the criterion of publication or, alternatively, the criterion of fixation. Such notification may be deposited at the time of ratification, acceptance or accession, or at any time thereafter; in the last case, it shall become effective six months after it has been deposited.

Article 6

Protected Broadcasts: 1. Points of Attachment for Broadcasting Organizations; 2. Power to Reserve

1. Each Contracting State shall grant national treatment to broadcasting organisations if either of the following conditions is met:

(a) the headquarters of the broadcasting organisation is situated in another Contracting State;

(b) the broadcast was transmitted from a transmitter situated in another Contracting State.

2. By means of a notification deposited with the Secretary-General of the United Nations, any Contracting State may declare that it will protect broadcasts only if the headquarters of the broadcasting organisation is situated in another Contracting State and the broadcast was transmitted from a transmitter situated in the same Contracting State. Such notification may be deposited at the time of ratification, acceptance or accession, or at any time thereafter; in the last case, it shall become effective six months after it has been deposited.

Article 7

Minimum Protection for Performers: 1. Particular Rights;

2. Relations between Performers and Broadcasting Organizations

1. The protection provided for performers by this Convention shall include the possibility of preventing:

(a) the broadcasting and the communication to the public, without their consent, of their performance, except where the performance used in the broadcasting or the public communication is itself already a broadcast performance or is made from a fixation;

(b) the fixation, without their consent, of their unfixed performance;

(c) the reproduction, without their consent, of a fixation of their performance:

(i) if the original fixation itself was made without their consent;

(ii) if the reproduction is made for purposes different from those for which the performers gave their consent;

(iii) if the original fixation was made in accordance with the provisions of Article 15, and the reproduction is made for purposes different from those referred to in those provisions.

2. (1) If broadcasting was consented to by the performers, it shall be a matter for the domestic law of the Contracting State where protection is claimed to regulate the protection against rebroadcasting, fixation for broadcasting purposes and the reproduction of such fixation for broadcasting purposes.

(2) The terms and conditions governing the use by broadcasting organisations of fixations made for broadcasting purposes shall be determined in accordance with the domestic law of the Contracting State where protection is claimed.

(3) However, the domestic law referred to in subparagraphs (1) and (2) of this paragraph shall not operate to deprive performers of the ability to control, by contract, their relations with broadcasting organisations.

Article 8

Performers acting jointly

Any Contracting State may, by its domestic laws and Regulations, specify the manner in which performers will be represented in connection with the exercise of their rights if several of them participate in the same performance.

Article 9

Variety and Circus Artists

Any Contracting State may, by its domestic laws and Regulations, extend the protection provided for in this Convention to artists who do not perform literary or artistic works.

Article 10

Right of Reproduction for Phonogram Producers

Producers of phonograms shall enjoy the right to authorize or prohibit the direct or indirect reproduction of their phonograms.

Article 11

Formalities for Phonograms

If, as a condition of protecting the rights of producers of phonograms, or of performers, or both, in relation to phonograms, a Contracting State, under its domestic law, requires compliance with formalities, these shall be considered as fulfilled if all the copies in commerce of the published phonogram or their containers bear a notice consisting of the symbol (P), accompanied by the year date of the first publication, placed in such a manner as to give reasonable notice of claim of protection; and if the copies or their containers do not identify the producer or the licensee of the producer (by carrying his name, trade mark or other appropriate designation), the notice shall also include the name of the owner of the rights of the producer; and, furthermore, if the copies or their containers do not identify the principal performers, the notice shall also include the name of the person who, in the country in which the fixation was effected, owns the rights of such performers.

Article 12

Secondary Uses of Phonograms

If a phonogram published for commercial purposes, or a reproduction of such phonogram, is used directly for broadcasting or for any communication to the public, a single equitable remuneration shall be paid by the user to the performers, or to the producers of the phonograms, or to both. Domestic law may, in the absence of agreement between these parties, lay down the conditions as to the sharing of this remuneration.

Article 13

Minimum Rights for Broadcasting Organizations

Broadcasting organisations shall enjoy the right to authorize or prohibit:

- (a) the rebroadcasting of their broadcasts;
- (b) the fixation of their broadcasts;
- (c) the reproduction:
 - (i) of fixations, made without their consent, of their broadcasts;
 - (ii) of fixations, made in accordance with the provisions of Article 15, of their broadcasts, if the reproduction is made for purposes different from those referred to in those provisions;
- (d) the communication to the public of their television broadcasts if such communication is made in places accessible to the public against payment of an entrance fee; it shall be a matter for the domestic law of the State where protection of this right is claimed to determine the conditions under which it may be exercised.

Article 14

Minimum Duration of Protection

The term of protection to be granted under this Convention shall last at least until the end of a period of twenty years computed from the end of the year in which:

- (a) the fixation was made—for phonograms and for performances incorporated therein;
- (b) the performance took place—for performances not incorporated in phonograms;
- (c) the broadcast took place—for broadcasts.

Article 15

Permitted Exceptions: 1. Specific Limitations;

2. Equivalents with copyright

1. Any Contracting State may, in its domestic laws and Regulations, provide for exceptions to the protection guaranteed by this Convention as regards:

- (a) private use;
- (b) use of short excerpts in connection with the reporting of current events;
- (c) ephemeral fixation by a broadcasting organisation by means of its own facilities and for its own broadcasts;

(d) use solely for the purposes of teaching or scientific research.

2. Irrespective of paragraph 1 of this Article, any Contracting State may, in its domestic laws and Regulations, provide for the same kinds of limitations with regard to the protection of performers, producers of phonograms and broadcasting organisations, as it provides for, in its domestic laws and Regulations, in connection with the protection of copyright in literary and artistic works. However, compulsory licences may be provided for only to the extent to which they are compatible with this Convention.

Article 16

Reservations

1. Any State, upon becoming party to this Convention, shall be bound by all the obligations and shall enjoy all the benefits thereof. However, a State may at any time, in a notification deposited with the Secretary-General of the United Nations, declare that:

(a) as regards Article 12:

- (i) it will not apply the provisions of that Article;
- (ii) it will not apply the provisions of that Article in respect of certain uses;

(iii) as regards phonograms the producer of which is not a national of another Contracting State, it will not apply that Article;

(iv) as regards phonograms the producer of which is a national of another Contracting State, it will limit the protection provided for by that Article to the extent to which, and to the term for which, the latter State grants protection to phonograms first fixed by a national of the State making the declaration; however, the fact that the Contracting State of which the producer is a national does not grant the protection to the same beneficiary or beneficiaries as the State making the declaration shall not be considered as a difference in the extent of the protection;

(b) as regards Article 13, it will not apply item (d) of that Article; if a Contracting State makes such a declaration, the other Contracting States shall not be obliged to grant the right referred to in Article 13, item (d), to broadcasting organisations whose headquarters are in that State.

2. If the notification referred to in paragraph 1 of this Article is made after the date of the deposit of the instrument of ratification, acceptance or accession, the declaration will become effective six months after it has been deposited.

Article 17

Certain countries applying only the "fixation" criterion

Any State which, on October 26, 1961, grants protection to producers of phonograms solely on the basis of the criterion of fixation may, by a notification deposited with the Secretary-General of the United Nations at the time of ratification, acceptance or accession, declare that it will apply, for the purposes of Article 5, the criterion of fixation alone and, for the purposes of paragraph 1(a)(iii) and (iv) of Article 16, the criterion of fixation instead of the criterion of nationality.

Article 18

Withdrawal of reservations

Any State which has deposited a notification under paragraph 3 of Article 5, paragraph 2 of Article 6, paragraph 1 of Article 16 or Article 17, may, by a further notification deposited with the Secretary-General of the United Nations, reduce its scope or withdraw it.

Article 19

Performers' Rights in Films

Notwithstanding anything in this Convention, once a performer has consented to the incorporation of his performance in a visual or audio-visual fixation, Article 7 shall have no further application.

Article 20

Non-retroactivity

1. This Convention shall not prejudice rights acquired in any Contracting State before the date of coming into force of this Convention for that State.
2. No Contracting State shall be bound to apply the provisions of this Convention to performances or broadcasts which took place, or to phonograms which were fixed, before the date of coming into force of this Convention for that State.

Article 21

Protection by other means

The protection provided for in this Convention shall not prejudice any protection otherwise secured to performers, producers of phonograms and broadcasting organisations.

Article 22

Special agreements

Contracting States reserve the right to enter into special agreements among themselves in so far as such agreements grant to performers, producers of phonograms or broadcasting organisations more extensive rights than those granted by this Convention or contain other provisions not contrary to this Convention.

Article 23

Signature and deposit

This Convention shall be deposited with the Secretary-General of the United Nations. It shall be open until June 30, 1962, for signature by any State invited to the Diplomatic Conference on the International Protection of Performers, Producers of Phonograms and Broadcasting Organisations which is a party to the Universal Copyright Convention or a member of the International Union for the Protection of Literary and Artistic Works.

Article 24

Becoming Party to the Convention

1. This Convention shall be subject to ratification or acceptance by the signatory States.
2. This Convention shall be open for accession by any State invited to the Conference referred to in Article 23, and by any State Member of the United Nations, provided that in either case such State is a party to the Universal Copyright Convention or a member of the International Union for the Protection of Literary and Artistic Works.
3. Ratification, acceptance or accession shall be effected by the deposit of an instrument to that effect with the Secretary-General of the United Nations.

[...]

WIPO Copyright Treaty

Preamble

The Contracting Parties,

Desiring to develop and maintain the protection of the rights of authors in their literary and artistic works in a manner as effective and uniform as possible,

Recognizing the need to introduce new international rules and clarify the interpretation of certain existing rules in order to provide adequate solutions to the questions raised by new economic, social, cultural and technological developments,

Recognizing the profound impact of the development and convergence of information and communication technologies on the creation and use of literary and artistic works,

Emphasizing the outstanding significance of copyright protection as an incentive for literary and artistic creation,

Recognizing the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information, as reflected in the Berne Convention,

Have agreed as follows:

Article 1

Relation to the Berne Convention

(1) This Treaty is a special agreement within the meaning of Article 20 of the Berne Convention for the Protection of Literary and Artistic Works, as regards Contracting Parties that are countries of the Union established by that Convention. This Treaty shall not have any connection with treaties other than the Berne Convention, nor shall it prejudice any rights and obligations under any other treaties.

(2) Nothing in this Treaty shall derogate from existing obligations that Contracting Parties have to each other under the Berne Convention for the Protection of Literary and Artistic Works.

(3) Hereinafter, "Berne Convention" shall refer to the Paris Act of July 24, 1971 of the Berne Convention for the Protection of Literary and Artistic Works.

(4) Contracting Parties shall comply with Articles 1 to 21 and the Appendix of the Berne Convention.¹

Article 2

Scope of Copyright Protection

Copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.

Article 3

Application of Articles 2 to 6 of the Berne Convention

Contracting Parties shall apply *mutatis mutandis* the provisions of Articles 2 to 6 of the Berne Convention in respect of the protection provided for in this Treaty.²

Article 4

Computer Programs

Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression.³

Article 5

Compilations of Data (Databases)

Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation.⁴

Article 6

Right of Distribution

(1) Authors of literary and artistic works shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their works through sale or other transfer of ownership.

(2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of the right in paragraph (1) applies after the first sale or other transfer of ownership of the original or a copy of the work with the authorization of the author.⁵

Article 7

Right of Rental

(1) Authors of

(i) computer programs;

(ii) cinematographic works; and

(iii) works embodied in phonograms, as determined in the national law of Contracting Parties,

shall enjoy the exclusive right of authorizing commercial rental to the public of the originals or copies of their works.

(2) Paragraph (1) shall not apply

(i) in the case of computer programs, where the program itself is not the essential object of the rental; and

(ii) in the case of cinematographic works, unless such commercial rental has led to widespread copying of such works materially impairing the exclusive right of reproduction.

(3) Notwithstanding the provisions of paragraph (1), a Contracting Party that, on April 15, 1994, had and continues to have in force a system of equitable remuneration of authors for the rental of copies of their works embodied in phonograms may maintain that system provided that the commercial rental of works embodied in phonograms is not giving rise to the material impairment of the exclusive right of reproduction of authors.^{5,6}

Article 8

Right of Communication to the Public

Without prejudice to the provisions of Articles 11(1)(ii), 11bis(1)(i) and (ii), 11ter(1)(ii), 14(1)(ii) and 14bis(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.⁷

Article 9

Duration of the Protection of Photographic Works

In respect of photographic works, the Contracting Parties shall not apply the provisions of Article 7(4) of the Berne Convention.

Article 10

Limitations and Exceptions

(1) Contracting Parties may, in their national legislation, provide for limitations of or exceptions to the rights granted to authors of literary and artistic works under this Treaty in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.

(2) Contracting Parties shall, when applying the Berne Convention, confine any limitations of or exceptions to rights provided for therein to certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.⁸

Article 11

Obligations concerning Technological Measures

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

Article 12

Obligations concerning Rights Management Information

(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.⁹

Article 13

Application in Time

Contracting Parties shall apply the provisions of Article 18 of the Berne Convention to all protection provided for in this Treaty.

Article 14

Provisions on Enforcement of Rights

(1) Contracting Parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this Treaty.

(2) Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements.

Article 15

Assembly

(1)

(a) The Contracting Parties shall have an Assembly.

(b) Each Contracting Party shall be represented by one delegate who may be assisted by alternate delegates, advisors and experts.

(c) The expenses of each delegation shall be borne by the Contracting Party that has appointed the delegation. The Assembly may ask the World Intellectual Property Organization (hereinafter referred to as "WIPO") to grant financial assistance to facilitate the participation of delegations of Contracting Parties that are regarded as developing countries in conformity with the established practice of the General Assembly of the United Nations or that are countries in transition to a market economy.

(2)

(a) The Assembly shall deal with matters concerning the maintenance and development of this Treaty and the application and operation of this Treaty.

(b) The Assembly shall perform the function allocated to it under Article 17(2) in respect of the admission of certain intergovernmental organizations to become party to this Treaty.

(c) The Assembly shall decide the convocation of any diplomatic conference for the revision of this Treaty and give the necessary instructions to the Director General of WIPO for the preparation of such diplomatic conference.

(3)

(a) Each Contracting Party that is a State shall have one vote and shall vote only in its own name.

(b) Any Contracting Party that is an intergovernmental organization may participate in the vote, in place of its Member States, with a number of votes equal to the number of its Member States which are party to this Treaty. No such intergovernmental organization shall participate in the vote if any one of its Member States exercises its right to vote and *vice versa*.

(4) The Assembly shall meet in ordinary session once every two years upon convocation by the Director General of WIPO.

(5) The Assembly shall establish its own rules of procedure, including the convocation of extraordinary sessions, the requirements of a quorum and, subject to the provisions of this Treaty, the required majority for various kinds of decisions.

Article 16

International Bureau

The International Bureau of WIPO shall perform the administrative tasks concerning the Treaty.

Article 17

Eligibility for Becoming Party to the Treaty

(1) Any Member State of WIPO may become party to this Treaty.

(2) The Assembly may decide to admit any intergovernmental organization to become party to this Treaty which declares that it is competent in respect of, and has its own legislation binding on all its Member States on, matters covered by this Treaty and that it has been duly authorized, in accordance with its internal procedures, to become party to this Treaty.

(3) The European Community, having made the declaration referred to in the preceding paragraph in the Diplomatic Conference that has adopted this Treaty, may become party to this Treaty.

Article 18

Rights and Obligations under the Treaty

Subject to any specific provisions to the contrary in this Treaty, each Contracting Party shall enjoy all of the rights and assume all of the obligations under this Treaty.

Article 19

Signature of the Treaty

This Treaty shall be open for signature until December 31, 1997, by any Member State of WIPO and by the European Community.

Article 20

Entry into Force of the Treaty

This Treaty shall enter into force three months after 30 instruments of ratification or accession by States have been deposited with the Director General of WIPO.

[...]

WIPO Performances and Phonograms Treaty

Preamble

The Contracting Parties,

Desiring to develop and maintain the protection of the rights of performers and producers of phonograms in a manner as effective and uniform as possible,
Recognizing the need to introduce new international rules in order to provide adequate solutions to the questions raised by economic, social, cultural and technological developments,
Recognizing the profound impact of the development and convergence of information and communication technologies on the production and use of performances and phonograms,
Recognizing the need to maintain a balance between the rights of performers and producers of phonograms and the larger public interest, particularly education, research and access to information,

Have agreed as follows:

CHAPTER I General Provisions

Article 1

Relation to Other Conventions

- (1) Nothing in this Treaty shall derogate from existing obligations that Contracting Parties have to each other under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations done in Rome, October 26, 1961 (hereinafter the "Rome Convention").
- (2) Protection granted under this Treaty shall leave intact and shall in no way affect the protection of copyright in literary and artistic works. Consequently, no provision of this Treaty may be interpreted as prejudicing such protection.¹
- (3) This Treaty shall not have any connection with, nor shall it prejudice any rights and obligations under, any other treaties.

Article 2 Definitions

For the purposes of this Treaty:

- (a) "performers" are actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret, or otherwise perform literary or artistic works or expressions of folklore;
- (b) "phonogram" means the fixation of the sounds of a performance or of other sounds, or of a representation of sounds, other than in the form of a fixation incorporated in a cinematographic or other audiovisual work;²
- (c) "fixation" means the embodiment of sounds, or of the representations thereof, from which they can be perceived, reproduced or communicated through a device;
- (d) "producer of a phonogram" means the person, or the legal entity, who or which takes the initiative and has the responsibility for the first fixation of the sounds of a performance or other sounds, or the representations of sounds;
- (e) "publication" of a fixed performance or a phonogram means the offering of copies of the fixed performance or the phonogram to the public, with the consent of the rightholder, and provided that copies are offered to the public in reasonable quantity;³
- (f) "broadcasting" means the transmission by wireless means for public reception of sounds or of images and sounds or of the representations thereof; such transmission by satellite is also "broadcasting"; transmission of encrypted signals is "broadcasting" where the means for decrypting are provided to the public by the broadcasting organization or with its consent;
- (g) "communication to the public" of a performance or a phonogram means the transmission to the public by any

medium, otherwise than by broadcasting, of sounds of a performance or the sounds or the representations of sounds fixed in a phonogram. For the purposes of Article 15, "communication to the public" includes making the sounds or representations of sounds fixed in a phonogram audible to the public.

Article 3

Beneficiaries of Protection under this Treaty

- (1) Contracting Parties shall accord the protection provided under this Treaty to the performers and producers of phonograms who are nationals of other Contracting Parties.
- (2) The nationals of other Contracting Parties shall be understood to be those performers or producers of phonograms who would meet the criteria for eligibility for protection provided under the Rome Convention, were all the Contracting Parties to this Treaty Contracting States of that Convention. In respect of these criteria of eligibility, Contracting Parties shall apply the relevant definitions in Article 2 of this Treaty.⁴
- (3) Any Contracting Party availing itself of the possibilities provided in Article 5(3) of the Rome Convention or, for the purposes of Article 5 of the same Convention, Article 17 thereof shall make a notification as foreseen in those provisions to the Director General of the World Intellectual Property Organization (WIPO).⁵

Article 4

National Treatment

- (1) Each Contracting Party shall accord to nationals of other Contracting Parties, as defined in Article 3(2), the treatment it accords to its own nationals with regard to the exclusive rights specifically granted in this Treaty, and to the right to equitable remuneration provided for in Article 15 of this Treaty.
- (2) The obligation provided for in paragraph (1) does not apply to the extent that another Contracting Party makes use of the reservations permitted by Article 15(3) of this Treaty.

CHAPTER II Rights of Performers

Article 5

Moral Rights of Performers

- (1) Independently of a performer's economic rights, and even after the transfer of those rights, the performer shall, as regards his live aural performances or performances fixed in phonograms, have the right to claim to be identified as the performer of his performances, except where omission is dictated by the manner of the use of the performance, and to object to any distortion, mutilation or other modification of his performances that would be prejudicial to his reputation.
- (2) The rights granted to a performer in accordance with paragraph (1) shall, after his death, be maintained, at least until the expiry of the economic rights, and shall be exercisable by the persons or institutions authorized by the legislation of the Contracting Party where protection is claimed. However, those Contracting Parties whose legislation, at the moment of their ratification of or accession to this Treaty, does not provide for protection after the death of the performer of all rights set out in the preceding paragraph may provide that some of these rights will, after his death, cease to be maintained.
- (3) The means of redress for safeguarding the rights granted under this Article shall be governed by the legislation of the Contracting Party where protection is claimed.

Article 6

Economic Rights of Performers in their Unfixed Performances

Performers shall enjoy the exclusive right of authorizing, as regards their performances:

- (i) the broadcasting and communication to the public of their unfixed performances except where the performance is already a broadcast performance; and
- (ii) the fixation of their unfixed performances.

Article 7
Right of Reproduction

Performers shall enjoy the exclusive right of authorizing the direct or indirect reproduction of their performances fixed in phonograms, in any manner or form.⁶

Article 8
Right of Distribution

(1) Performers shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their performances fixed in phonograms through sale or other transfer of ownership.

(2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of the right in paragraph (1) applies after the first sale or other transfer of ownership of the original or a copy of the fixed performance with the authorization of the performer.⁷

Article 9
Right of Rental

(1) Performers shall enjoy the exclusive right of authorizing the commercial rental to the public of the original and copies of their performances fixed in phonograms as determined in the national law of Contracting Parties, even after distribution of them by, or pursuant to, authorization by the performer.

(2) Notwithstanding the provisions of paragraph (1), a Contracting Party that, on April 15, 1994, had and continues to have in force a system of equitable remuneration of performers for the rental of copies of their performances fixed in phonograms, may maintain that system provided that the commercial rental of phonograms is not giving rise to the material impairment of the exclusive right of reproduction of performers.⁸

Article 10
Right of Making Available of Fixed Performances

Performers shall enjoy the exclusive right of authorizing the making available to the public of their performances fixed in phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.

CHAPTER III
Rights of Producers of Phonograms

Article 11
Right of Reproduction

Producers of phonograms shall enjoy the exclusive right of authorizing the direct or indirect reproduction of their phonograms, in any manner or form.⁹

Article 12
Right of Distribution

(1) Producers of phonograms shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their phonograms through sale or other transfer of ownership.

(2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of the right in paragraph (1) applies after the first sale or other transfer of ownership of the original or a copy of the phonogram with the authorization of the producer of the phonogram.¹⁰

Article 13
Right of Rental

(1) Producers of phonograms shall enjoy the exclusive right of authorizing the commercial rental to the public of the original

and copies of their phonograms, even after distribution of them, by or pursuant to, authorization by the producer.

(2) Notwithstanding the provisions of paragraph (1), a Contracting Party that, on April 15, 1994, had and continues to have in force a system of equitable remuneration of producers of phonograms for the rental of copies of their phonograms, may maintain that system provided that the commercial rental of phonograms is not giving rise to the material impairment of the exclusive rights of reproduction of producers of phonograms.¹¹

Article 14
Right of Making Available of Phonograms

Producers of phonograms shall enjoy the exclusive right of authorizing the making available to the public of their phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.

CHAPTER IV
Common Provisions

Article 15
Right to Remuneration for Broadcasting and Communication to the Public

(1) Performers and producers of phonograms shall enjoy the right to a single equitable remuneration for the direct or indirect use of phonograms published for commercial purposes for broadcasting or for any communication to the public.

(2) Contracting Parties may establish in their national legislation that the single equitable remuneration shall be claimed from the user by the performer or by the producer of a phonogram or by both. Contracting Parties may enact national legislation that, in the absence of an agreement between the performer and the producer of a phonogram, sets the terms according to which performers and producers of phonograms shall share the single equitable remuneration.

(3) Any Contracting Party may, in a notification deposited with the Director General of WIPO, declare that it will apply the provisions of paragraph (1) only in respect of certain uses, or that it will limit their application in some other way, or that it will not apply these provisions at all.

(4) For the purposes of this Article, phonograms made available to the public by wire or wireless means in such a way that members of the public may access them from a place and at a time individually chosen by them shall be considered as if they had been published for commercial purposes.^{12,13}

Article 16
Limitations and Exceptions

(1) Contracting Parties may, in their national legislation, provide for the same kinds of limitations or exceptions with regard to the protection of performers and producers of phonograms as they provide for, in their national legislation, in connection with the protection of copyright in literary and artistic works.

(2) Contracting Parties shall confine any limitations of or exceptions to rights provided for in this Treaty to certain special cases which do not conflict with a normal exploitation of the performance or phonogram and do not unreasonably prejudice the legitimate interests of the performer or of the producer of the phonogram.^{14,15}

Article 17
Term of Protection

(1) The term of protection to be granted to performers under this Treaty shall last, at least, until the end of a period of 50 years computed from the end of the year in which the performance was fixed in a phonogram.

(2) The term of protection to be granted to producers of phonograms under this Treaty shall last, at least, until the end of a period of 50 years computed from the end of the year in which the phonogram was published, or failing such

publication within 50 years from fixation of the phonogram, 50 years from the end of the year in which the fixation was made.

Article 18

Obligations concerning Technological Measures

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.

Article 19

Obligations concerning Rights Management Information

(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty:

- (i) to remove or alter any electronic rights management information without authority;
 - (ii) to distribute, import for distribution, broadcast, communicate or make available to the public, without authority, performances, copies of fixed performances or phonograms knowing that electronic rights management information has been removed or altered without authority.
- (2) As used in this Article, "rights management information" means information which identifies the performer, the performance of the performer, the producer of the phonogram, the phonogram, the owner of any right in the performance or phonogram, or information about the terms and conditions of use of the performance or phonogram, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a fixed performance or a phonogram or appears in connection with the communication

or making available of a fixed performance or a phonogram to the public.¹⁶

Article 20

Formalities

The enjoyment and exercise of the rights provided for in this Treaty shall not be subject to any formality.

Article 21

Reservations

Subject to the provisions of Article 15(3), no reservations to this Treaty shall be permitted.

Article 22

Application in Time

(1) Contracting Parties shall apply the provisions of Article 18 of the Berne Convention, *mutatis mutandis*, to the rights of performers and producers of phonograms provided for in this Treaty.

(2) Notwithstanding paragraph (1), a Contracting Party may limit the application of Article 5 of this Treaty to performances which occurred after the entry into force of this Treaty for that Party.

Article 23

Provisions on Enforcement of Rights

(1) Contracting Parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this Treaty.

(2) Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements.

[...]

Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society

[...]

(1) The Treaty provides for the establishment of an internal market and the institution of a system ensuring that competition in the internal market is not distorted. Harmonisation of the laws of the Member States on copyright and related rights contributes to the achievement of these objectives.

(2) The European Council, meeting at Corfu on 24 and 25 June 1994, stressed the need to create a general and flexible legal framework at Community level in order to foster the development of the information society in Europe. This requires, *inter alia*, the existence of an internal market for new products and services. Important Community legislation to ensure such a regulatory framework is already in place or its adoption is well under way. Copyright and related rights play an important role in this context as they protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content.

(3) The proposed harmonisation will help to implement the four freedoms of the internal market and relates to compliance with the fundamental principles of law and especially of

property, including intellectual property, and freedom of expression and the public interest.

(4) A harmonised legal framework on copyright and related rights, through increased legal certainty and while providing for a high level of protection of intellectual property, will foster substantial investment in creativity and innovation, including network infrastructure, and lead in turn to growth and increased competitiveness of European industry, both in the area of content provision and information technology and more generally across a wide range of industrial and cultural sectors. This will safeguard employment and encourage new job creation.

(5) Technological development has multiplied and diversified the vectors for creation, production and exploitation. While no new concepts for the protection of intellectual property are needed, the current law on copyright and related rights should be adapted and supplemented to respond adequately to economic realities such as new forms of exploitation.

(6) Without harmonisation at Community level, legislative activities at national level which have already been initiated in a number of Member States in order to respond to the technological challenges might result in significant differences in protection and thereby in restrictions on the free movement

of services and products incorporating, or based on, intellectual property, leading to a refragmentation of the internal market and legislative inconsistency. The impact of such legislative differences and uncertainties will become more significant with the further development of the information society, which has already greatly increased transborder exploitation of intellectual property. This development will and should further increase. Significant legal differences and uncertainties in protection may hinder economies of scale for new products and services containing copyright and related rights.

(7) The Community legal framework for the protection of copyright and related rights must, therefore, also be adapted and supplemented as far as is necessary for the smooth functioning of the internal market. To that end, those national provisions on copyright and related rights which vary considerably from one Member State to another or which cause legal uncertainties hindering the smooth functioning of the internal market and the proper development of the information society in Europe should be adjusted, and inconsistent national responses to the technological developments should be avoided, whilst differences not adversely affecting the functioning of the internal market need not be removed or prevented.

(8) The various social, societal and cultural implications of the information society require that account be taken of the specific features of the content of products and services.

(9) Any harmonisation of copyright and related rights must take as a basis a high level of protection, since such rights are crucial to intellectual creation. Their protection helps to ensure the maintenance and development of creativity in the interests of authors, performers, producers, consumers, culture, industry and the public at large. Intellectual property has therefore been recognised as an integral part of property.

(10) If authors or performers are to continue their creative and artistic work, they have to receive an appropriate reward for the use of their work, as must producers in order to be able to finance this work. The investment required to produce products such as phonograms, films or multimedia products, and services such as "on-demand" services, is considerable. Adequate legal protection of intellectual property rights is necessary in order to guarantee the availability of such a reward and provide the opportunity for satisfactory returns on this investment.

(11) A rigorous, effective system for the protection of copyright and related rights is one of the main ways of ensuring that European cultural creativity and production receive the necessary resources and of safeguarding the independence and dignity of artistic creators and performers.

(12) Adequate protection of copyright works and subject-matter of related rights is also of great importance from a cultural standpoint. Article 151 of the Treaty requires the Community to take cultural aspects into account in its action.

(13) A common search for, and consistent application at European level of, technical measures to protect works and other subject-matter and to provide the necessary information on rights are essential insofar as the ultimate aim of these measures is to give effect to the principles and guarantees laid down in law.

(14) This Directive should seek to promote learning and culture by protecting works and other subject-matter while permitting exceptions or limitations in the public interest for the purpose of education and teaching.

(15) The Diplomatic Conference held under the auspices of the World Intellectual Property Organisation (WIPO) in December 1996 led to the adoption of two new Treaties, the "WIPO Copyright Treaty" and the "WIPO Performances and Phonograms Treaty", dealing respectively with the protection of authors and the protection of performers and phonogram producers. Those Treaties update the international protection for copyright and related rights significantly, not least with regard to the so-called "digital agenda", and improve the means to fight piracy world-wide. The Community and a majority of Member States have already signed the Treaties and the process of making arrangements for the ratification of the

Treaties by the Community and the Member States is under way. This Directive also serves to implement a number of the new international obligations.

(16) Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("Directive on electronic commerce")(4), which clarifies and harmonises various legal issues relating to information society services including electronic commerce. This Directive should be implemented within a timescale similar to that for the implementation of the Directive on electronic commerce, since that Directive provides a harmonised framework of principles and provisions relevant inter alia to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive.

(17) It is necessary, especially in the light of the requirements arising out of the digital environment, to ensure that collecting societies achieve a higher level of rationalisation and transparency with regard to compliance with competition rules.

(18) This Directive is without prejudice to the arrangements in the Member States concerning the management of rights such as extended collective licences.

(19) The moral rights of rightholders should be exercised according to the legislation of the Member States and the provisions of the Berne Convention for the Protection of Literary and Artistic Works, of the WIPO Copyright Treaty and of the WIPO Performances and Phonograms Treaty. Such moral rights remain outside the scope of this Directive.

(20) This Directive is based on principles and rules already laid down in the Directives currently in force in this area, in particular Directives 91/250/EEC(5), 92/100/EEC(6), 93/83/EEC(7), 93/98/EEC(8) and 96/9/EC(9), and it develops those principles and rules and places them in the context of the information society. The provisions of this Directive should be without prejudice to the provisions of those Directives, unless otherwise provided in this Directive.

(21) This Directive should define the scope of the acts covered by the reproduction right with regard to the different beneficiaries. This should be done in conformity with the *acquis communautaire*. A broad definition of these acts is needed to ensure legal certainty within the internal market.

(22) The objective of proper support for the dissemination of culture must not be achieved by sacrificing strict protection of rights or by tolerating illegal forms of distribution of counterfeited or pirated works.

(23) This Directive should harmonise further the author's right of communication to the public. This right should be understood in a broad sense covering all communication to the public not present at the place where the communication originates. This right should cover any such transmission or retransmission of a work to the public by wire or wireless means, including broadcasting. This right should not cover any other acts.

(24) The right to make available to the public subject-matter referred to in Article 3(2) should be understood as covering all acts of making available such subject-matter to members of the public not present at the place where the act of making available originates, and as not covering any other acts.

(25) The legal uncertainty regarding the nature and the level of protection of acts of on-demand transmission of copyright works and subject-matter protected by related rights over networks should be overcome by providing for harmonised protection at Community level. It should be made clear that all rightholders recognised by this Directive should have an exclusive right to make available to the public copyright works or any other subject-matter by way of interactive on-demand transmissions. Such interactive on-demand transmissions are

characterised by the fact that members of the public may access them from a place and at a time individually chosen by them.

(26) With regard to the making available in on-demand services by broadcasters of their radio or television productions incorporating music from commercial phonograms as an integral part thereof, collective licensing arrangements are to be encouraged in order to facilitate the clearance of the rights concerned.

(27) The mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Directive.

(28) Copyright protection under this Directive includes the exclusive right to control distribution of the work incorporated in a tangible article. The first sale in the Community of the original of a work or copies thereof by the rightholder or with his consent exhausts the right to control resale of that object in the Community. This right should not be exhausted in respect of the original or of copies thereof sold by the rightholder or with his consent outside the Community. Rental and lending rights for authors have been established in Directive 92/100/EEC. The distribution right provided for in this Directive is without prejudice to the provisions relating to the rental and lending rights contained in Chapter I of that Directive.

(29) The question of exhaustion does not arise in the case of services and on-line services in particular. This also applies with regard to a material copy of a work or other subject-matter made by a user of such a service with the consent of the rightholder. Therefore, the same applies to rental and lending of the original and copies of works or other subject-matter which are services by nature. Unlike CD-ROM or CD-I, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which should be subject to authorisation where the copyright or related right so provides.

(30) The rights referred to in this Directive may be transferred, assigned or subject to the granting of contractual licences, without prejudice to the relevant national legislation on copyright and related rights.

(31) A fair balance of rights and interests between the different categories of rightholders, as well as between the different categories of rightholders and users of protected subject-matter must be safeguarded. The existing exceptions and limitations to the rights as set out by the Member States have to be reassessed in the light of the new electronic environment. Existing differences in the exceptions and limitations to certain restricted acts have direct negative effects on the functioning of the internal market of copyright and related rights. Such differences could well become more pronounced in view of the further development of transborder exploitation of works and cross-border activities. In order to ensure the proper functioning of the internal market, such exceptions and limitations should be defined more harmoniously. The degree of their harmonisation should be based on their impact on the smooth functioning of the internal market.

(32) This Directive provides for an exhaustive enumeration of exceptions and limitations to the reproduction right and the right of communication to the public. Some exceptions or limitations only apply to the reproduction right, where appropriate. This list takes due account of the different legal traditions in Member States, while, at the same time, aiming to ensure a functioning internal market. Member States should arrive at a coherent application of these exceptions and limitations, which will be assessed when reviewing implementing legislation in the future.

(33) The exclusive right of reproduction should be subject to an exception to allow certain acts of temporary reproduction, which are transient or incidental reproductions, forming an integral and essential part of a technological process and carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made. The acts of reproduction concerned should have no separate economic value on their own. To the extent that they

meet these conditions, this exception should include acts which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information. A use should be considered lawful where it is authorised by the rightholder or not restricted by law.

(34) Member States should be given the option of providing for certain exceptions or limitations for cases such as educational and scientific purposes, for the benefit of public institutions such as libraries and archives, for purposes of news reporting, for quotations, for use by people with disabilities, for public security uses and for uses in administrative and judicial proceedings.

(35) In certain cases of exceptions or limitations, rightholders should receive fair compensation to compensate them adequately for the use made of their protected works or other subject-matter. When determining the form, detailed arrangements and possible level of such fair compensation, account should be taken of the particular circumstances of each case. When evaluating these circumstances, a valuable criterion would be the possible harm to the rightholders resulting from the act in question. In cases where rightholders have already received payment in some other form, for instance as part of a licence fee, no specific or separate payment may be due. The level of fair compensation should take full account of the degree of use of technological protection measures referred to in this Directive. In certain situations where the prejudice to the rightholder would be minimal, no obligation for payment may arise.

(36) The Member States may provide for fair compensation for rightholders also when applying the optional provisions on exceptions or limitations which do not require such compensation.

(37) Existing national schemes on reprography, where they exist, do not create major barriers to the internal market. Member States should be allowed to provide for an exception or limitation in respect of reprography.

(38) Member States should be allowed to provide for an exception or limitation to the reproduction right for certain types of reproduction of audio, visual and audio-visual material for private use, accompanied by fair compensation. This may include the introduction or continuation of remuneration schemes to compensate for the prejudice to rightholders. Although differences between those remuneration schemes affect the functioning of the internal market, those differences, with respect to analogue private reproduction, should not have a significant impact on the development of the information society. Digital private copying is likely to be more widespread and have a greater economic impact. Due account should therefore be taken of the differences between digital and analogue private copying and a distinction should be made in certain respects between them.

(39) When applying the exception or limitation on private copying, Member States should take due account of technological and economic developments, in particular with respect to digital private copying and remuneration schemes, when effective technological protection measures are available. Such exceptions or limitations should not inhibit the use of technological measures or their enforcement against circumvention.

(40) Member States may provide for an exception or limitation for the benefit of certain non-profit making establishments, such as publicly accessible libraries and equivalent institutions, as well as archives. However, this should be limited to certain special cases covered by the reproduction right. Such an exception or limitation should not cover uses made in the context of on-line delivery of protected works or other subject-matter. This Directive should be without prejudice to the Member States' option to derogate from the exclusive public lending right in accordance with Article 5 of Directive 92/100/EEC. Therefore, specific contracts or licences should be

promoted which, without creating imbalances, favour such establishments and the disseminative purposes they serve.

(41) When applying the exception or limitation in respect of ephemeral recordings made by broadcasting organisations it is understood that a broadcaster's own facilities include those of a person acting on behalf of and under the responsibility of the broadcasting organisation.

(42) When applying the exception or limitation for non-commercial educational and scientific research purposes, including distance learning, the non-commercial nature of the activity in question should be determined by that activity as such. The organisational structure and the means of funding of the establishment concerned are not the decisive factors in this respect.

(43) It is in any case important for the Member States to adopt all necessary measures to facilitate access to works by persons suffering from a disability which constitutes an obstacle to the use of the works themselves, and to pay particular attention to accessible formats.

(44) When applying the exceptions and limitations provided for in this Directive, they should be exercised in accordance with international obligations. Such exceptions and limitations may not be applied in a way which prejudices the legitimate interests of the rightholder or which conflicts with the normal exploitation of his work or other subject-matter. The provision of such exceptions or limitations by Member States should, in particular, duly reflect the increased economic impact that such exceptions or limitations may have in the context of the new electronic environment. Therefore, the scope of certain exceptions or limitations may have to be even more limited when it comes to certain new uses of copyright works and other subject-matter.

(45) The exceptions and limitations referred to in Article 5(2), (3) and (4) should not, however, prevent the definition of contractual relations designed to ensure fair compensation for the rightholders insofar as permitted by national law.

(46) Recourse to mediation could help users and rightholders to settle disputes. The Commission, in cooperation with the Member States within the Contact Committee, should undertake a study to consider new legal ways of settling disputes concerning copyright and related rights.

(47) Technological development will allow rightholders to make use of technological measures designed to prevent or restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases. The danger, however, exists that illegal activities might be carried out in order to enable or facilitate the circumvention of the technical protection provided by these measures. In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect.

(48) Such legal protection should be provided in respect of technological measures that effectively restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases without, however, preventing the normal operation of electronic equipment and its technological development. Such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6. Such legal protection should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection. In particular, this protection should not hinder research into cryptography.

(49) The legal protection of technological measures is without prejudice to the application of any national provisions which may prohibit the private possession of devices, products or components for the circumvention of technological measures.

(50) Such a harmonised legal protection does not affect the specific provisions on protection provided for by Directive 91/250/EEC. In particular, it should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive. It should neither inhibit nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable acts to be undertaken in accordance with the terms of Article 5(3) or Article 6 of Directive 91/250/EEC. Articles 5 and 6 of that Directive exclusively determine exceptions to the exclusive rights applicable to computer programs.

(51) The legal protection of technological measures applies without prejudice to public policy, as reflected in Article 5, or public security. Member States should promote voluntary measures taken by rightholders, including the conclusion and implementation of agreements between rightholders and other parties concerned, to accommodate achieving the objectives of certain exceptions or limitations provided for in national law in accordance with this Directive. In the absence of such voluntary measures or agreements within a reasonable period of time, Member States should take appropriate measures to ensure that rightholders provide beneficiaries of such exceptions or limitations with appropriate means of benefiting from them, by modifying an implemented technological measure or by other means. However, in order to prevent abuse of such measures taken by rightholders, including within the framework of agreements, or taken by a Member State, any technological measures applied in implementation of such measures should enjoy legal protection.

(52) When implementing an exception or limitation for private copying in accordance with Article 5(2)(b), Member States should likewise promote the use of voluntary measures to accommodate achieving the objectives of such exception or limitation. If, within a reasonable period of time, no such voluntary measures to make reproduction for private use possible have been taken, Member States may take measures to enable beneficiaries of the exception or limitation concerned to benefit from it. Voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, as well as measures taken by Member States, do not prevent rightholders from using technological measures which are consistent with the exceptions or limitations on private copying in national law in accordance with Article 5(2)(b), taking account of the condition of fair compensation under that provision and the possible differentiation between various conditions of use in accordance with Article 5(5), such as controlling the number of reproductions. In order to prevent abuse of such measures, any technological measures applied in their implementation should enjoy legal protection.

(53) The protection of technological measures should ensure a secure environment for the provision of interactive on-demand services, in such a way that members of the public may access works or other subject-matter from a place and at a time individually chosen by them. Where such services are governed by contractual arrangements, the first and second subparagraphs of Article 6(4) should not apply. Non-interactive forms of online use should remain subject to those provisions.

(54) Important progress has been made in the international standardisation of technical systems of identification of works and protected subject-matter in digital format. In an increasingly networked environment, differences between technological measures could lead to an incompatibility of systems within the Community. Compatibility and interoperability of the different systems should be encouraged. It would be highly desirable to encourage the development of global systems.

(55) Technological development will facilitate the distribution of works, notably on networks, and this will entail the need for rightholders to identify better the work or other subject-matter, the author or any other rightholder, and to provide information about the terms and conditions of use of the work or other subject-matter in order to render easier the management of rights attached to them. Rightholders should be

encouraged to use markings indicating, in addition to the information referred to above, *inter alia* their authorisation when putting works or other subject-matter on networks.

(56) There is, however, the danger that illegal activities might be carried out in order to remove or alter the electronic copyright-management information attached to it, or otherwise to distribute, import for distribution, broadcast, communicate to the public or make available to the public works or other protected subject-matter from which such information has been removed without authority. In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against any of these activities.

(57) Any such rights-management information systems referred to above may, depending on their design, at the same time process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour. These technical means, in their technical functions, should incorporate privacy safeguards in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data⁽¹⁰⁾.

(58) Member States should provide for effective sanctions and remedies for infringements of rights and obligations as set out in this Directive. They should take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for should be effective, proportionate and dissuasive and should include the possibility of seeking damages and/or injunctive relief and, where appropriate, of applying for seizure of infringing material.

(59) In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.

(60) The protection provided under this Directive should be without prejudice to national or Community legal provisions in other areas, such as industrial property, data protection, conditional access, access to public documents, and the rule of media exploitation chronology, which may affect the protection of copyright or related rights.

(61) In order to comply with the WIPO Performances and Phonograms Treaty, Directives 92/100/EEC and 93/98/EEC should be amended,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I OBJECTIVE AND SCOPE

Article 1 Scope

1. This Directive concerns the legal protection of copyright and related rights in the framework of the internal market, with particular emphasis on the information society.

2. Except in the cases referred to in Article 11, this Directive shall leave intact and shall in no way affect existing Community provisions relating to:

- (a) the legal protection of computer programs;
- (b) rental right, lending right and certain rights related to copyright in the field of intellectual property;
- (c) copyright and related rights applicable to broadcasting of programmes by satellite and cable retransmission;
- (d) the term of protection of copyright and certain related rights;

(e) the legal protection of databases.

CHAPTER II RIGHTS AND EXCEPTIONS

Article 2 Reproduction right

Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:

- (a) for authors, of their works;
- (b) for performers, of fixations of their performances;
- (c) for phonogram producers, of their phonograms;
- (d) for the producers of the first fixations of films, in respect of the original and copies of their films;
- (e) for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite.

Article 3 Right of communication to the public of works and right of making available to the public other subject-matter

1. Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.

2. Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:

- (a) for performers, of fixations of their performances;
- (b) for phonogram producers, of their phonograms;
- (c) for the producers of the first fixations of films, of the original and copies of their films;
- (d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.

3. The rights referred to in paragraphs 1 and 2 shall not be exhausted by any act of communication to the public or making available to the public as set out in this Article.

Article 4 Distribution right

1. Member States shall provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorise or prohibit any form of distribution to the public by sale or otherwise.

2. The distribution right shall not be exhausted within the Community in respect of the original or copies of the work, except where the first sale or other transfer of ownership in the Community of that object is made by the rightholder or with his consent.

Article 5 Exceptions and limitations

1. Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:

- (a) a transmission in a network between third parties by an intermediary, or
 - (b) a lawful use
- of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.

2. Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases:

- (a) in respect of reproductions on paper or any similar medium, effected by the use of any kind of photographic technique or by some other process having similar effects, with the exception of

sheet music, provided that the rightholders receive fair compensation;

(b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned;

(c) in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage;

(d) in respect of ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts; the preservation of these recordings in official archives may, on the grounds of their exceptional documentary character, be permitted;

(e) in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the rightholders receive fair compensation.

3. Member States may provide for exceptions or limitations to the rights provided for in Articles 2 and 3 in the following cases:

(a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved;

(b) uses, for the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature, to the extent required by the specific disability;

(c) reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics or of broadcast works or other subject-matter of the same character, in cases where such use is not expressly reserved, and as long as the source, including the author's name, is indicated, or use of works or other subject-matter in connection with the reporting of current events, to the extent justified by the informative purpose and as long as the source, including the author's name, is indicated, unless this turns out to be impossible;

(d) quotations for purposes such as criticism or review, provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, that, unless this turns out to be impossible, the source, including the author's name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose;

(e) use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;

(f) use of political speeches as well as extracts of public lectures or similar works or subject-matter to the extent justified by the informative purpose and provided that the source, including the author's name, is indicated, except where this turns out to be impossible;

(g) use during religious celebrations or official celebrations organised by a public authority;

(h) use of works, such as works of architecture or sculpture, made to be located permanently in public places;

(i) incidental inclusion of a work or other subject-matter in other material;

(j) use for the purpose of advertising the public exhibition or sale of artistic works, to the extent necessary to promote the event, excluding any other commercial use;

(k) use for the purpose of caricature, parody or pastiche;

(l) use in connection with the demonstration or repair of equipment;

(m) use of an artistic work in the form of a building or a drawing or plan of a building for the purposes of reconstructing the building;

(n) use by communication or making available, for the purpose of research or private study, to individual members of the

public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections;

(o) use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community, without prejudice to the other exceptions and limitations contained in this Article.

4. Where the Member States may provide for an exception or limitation to the right of reproduction pursuant to paragraphs 2 and 3, they may provide similarly for an exception or limitation to the right of distribution as referred to in Article 4 to the extent justified by the purpose of the authorised act of reproduction.

5. The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.

CHAPTER III PROTECTION OF TECHNOLOGICAL MEASURES AND RIGHTS-MANAGEMENT INFORMATION

Article 6

Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

3. For the purposes of this Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned. A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by rightholders to

the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.

The technological measures applied voluntarily by rightholders, including those applied in implementation of voluntary agreements, and technological measures applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1.

The provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.

When this Article is applied in the context of Directives 92/100/EEC and 96/9/EC, this paragraph shall apply *mutatis mutandis*.

Article 7

Obligations concerning rights-management information

1. Member States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts:

(a) the removal or alteration of any electronic rights-management information;

(b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority,

if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the *sui generis* right provided for in Chapter III of Directive 96/9/EC.

2. For the purposes of this Directive, the expression "rights-management information" means any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or covered by the *sui generis* right provided for in Chapter III of Directive 96/9/EC, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.

The first subparagraph shall apply when any of these items of information is associated with a copy of, or appears in connection with the communication to the public of, a work or other subject-matter referred to in this Directive or covered by the *sui generis* right provided for in Chapter III of Directive 96/9/EC.

CHAPTER IV COMMON PROVISIONS

Article 8

Sanctions and remedies

1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.

2. Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

Article 9

Continued application of other legal provisions

This Directive shall be without prejudice to provisions concerning in particular patent rights, trade marks, design rights, utility models, topographies of semi-conductor products, type faces, conditional access, access to cable of broadcasting services, protection of national treasures, legal deposit requirements, laws on restrictive practices and unfair competition, trade secrets, security, confidentiality, data protection and privacy, access to public documents, the law of contract.

Article 10

Application over time

1. The provisions of this Directive shall apply in respect of all works and other subject-matter referred to in this Directive which are, on 22 December 2002, protected by the Member States' legislation in the field of copyright and related rights, or which meet the criteria for protection under the provisions of this Directive or the provisions referred to in Article 1(2).

2. This Directive shall apply without prejudice to any acts concluded and rights acquired before 22 December 2002.

Article 11

Technical adaptations

1. Directive 92/100/EEC is hereby amended as follows:

(a) Article 7 shall be deleted;

(b) Article 10(3) shall be replaced by the following: "3. The limitations shall only be applied in certain special cases which do not conflict with a normal exploitation of the subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder."

2. Article 3(2) of Directive 93/98/EEC shall be replaced by the following: "2. The rights of producers of phonograms shall expire 50 years after the fixation is made. However, if the phonogram has been lawfully published within this period, the said rights shall expire 50 years from the date of the first lawful publication. If no lawful publication has taken place within the period mentioned in the first sentence, and if the phonogram has been lawfully communicated to the public within this period, the said rights shall expire 50 years from the date of the first lawful communication to the public.

However, where through the expiry of the term of protection granted pursuant to this paragraph in its version before amendment by Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society(11) the rights of producers of phonograms are no longer protected on 22 December 2002, this paragraph shall not have the effect of protecting those rights anew."

Article 12

Final provisions

1. Not later than 22 December 2004 and every three years thereafter, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, in which, *inter alia*, on the basis of specific information supplied by the Member States, it shall examine in particular the application of Articles 5, 6 and 8 in the light of the development of the digital market. In the case of Article 6, it shall examine in particular whether that Article confers a sufficient level of protection and whether acts which are permitted by law are being adversely affected by the use of effective technological measures. Where necessary, in particular to ensure the functioning of the internal market pursuant to Article 14 of the Treaty, it shall submit proposals for amendments to this Directive.

2. Protection of rights related to copyright under this Directive shall leave intact and shall in no way affect the protection of copyright.

3. A contact committee is hereby established. It shall be composed of representatives of the competent authorities of the Member States. It shall be chaired by a representative of the Commission and shall meet either on the initiative of the chairman or at the request of the delegation of a Member State.

4. The tasks of the committee shall be as follows:

- (a) to examine the impact of this Directive on the functioning of the internal market, and to highlight any difficulties;
- (b) to organise consultations on all questions deriving from the application of this Directive;
- (c) to facilitate the exchange of information on relevant developments in legislation and case-law, as well as relevant economic, social, cultural and technological developments;
- (d) to act as a forum for the assessment of the digital market in works and other items, including private copying and the use of technological measures.

Article 13 **Implementation**

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive before 22 December 2002. They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field governed by this Directive.

Article 14

C-5/08 Infopaq International

1. An act occurring during a data capture process, which consists of storing an extract of a protected work comprising 11 words and printing out that extract, is such as to come within the concept of reproduction in part within the meaning of Article 2 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, if the elements thus reproduced are the expression of the intellectual creation of their author; it is for the national court to make this determination.

2. The act of printing out an extract of 11 words, during a data capture process such as that at issue in the main proceedings, does not fulfil the condition of being transient in nature as required by Article 5(1) of Directive 2001/29 and, therefore, that process cannot be carried out without the consent of the relevant rightholders.

C-467/08 Padawan

The concept of 'fair compensation', within the meaning of Article 5(2)(b) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, is an autonomous concept of European Union law which must be interpreted uniformly in all the Member States that have introduced a private copying exception, irrespective of the power conferred on the Member States to determine, within the limits imposed by European Union law in particular by that Directive, the form, detailed

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

[...]

(1) OJ C 108, 7.4.1998, p. 6 and OJ C 180, 25.6.1999, p. 6.

(2) OJ C 407, 28.12.1998, p. 30.

(3) Opinion of the European Parliament of 10 February 1999 (OJ C 150, 28.5.1999, p. 171), Council Common Position of 28 September 2000 (OJ C 344, 1.12.2000, p. 1) and Decision of the European Parliament of 14 February 2001 (not yet published in the Official Journal). Council Decision of 9 April 2001.

(4) OJ L 178, 17.7.2000, p. 1.

(5) Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (OJ L 122, 17.5.1991, p. 42). Directive as amended by Directive 93/98/EEC.

(6) Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (OJ L 346, 27.11.1992, p. 61). Directive as amended by Directive 93/98/EEC.

(7) Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission (OJ L 248, 6.10.1993, p. 15).

(8) Council Directive 93/98/EEC of 29 October 1993 harmonising the term of protection of copyright and certain related rights (OJ L 290, 24.11.1993, p. 9).

(9) Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (OJ L 77, 27.3.1996, p. 20).

(10) OJ L 281, 23.11.1995, p. 31.

(11) OJ L 167, 22.6.2001, p. 10.

arrangements for financing and collection, and the level of that fair compensation.

Article 5(2)(b) of Directive 2001/29 must be interpreted as meaning that the 'fair balance' between the persons concerned means that fair compensation must be calculated on the basis of the criterion of the harm caused to authors of protected works by the introduction of the private copying exception. It is consistent with the requirements of that 'fair balance' to provide that persons who have digital reproduction equipment, devices and media and who on that basis, in law or in fact, make that equipment available to private users or provide them with copying services are the persons liable to finance the fair compensation, inasmuch as they are able to pass on to private users the actual burden of financing it.

Article 5(2)(b) of Directive 2001/29 must be interpreted as meaning that a link is necessary between the application of the levy intended to finance fair compensation with respect to digital reproduction equipment, devices and media and the deemed use of them for the purposes of private copying. Consequently, the indiscriminate application of the private copying levy, in particular with respect to digital reproduction equipment, devices and media not made available to private users and clearly reserved for uses other than private copying, is incompatible with Directive 2001/29.

C-462/09 Stichting de ThuisKopie

1. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, in particular Article 5(2)(b) and (5) thereof, must be interpreted

as meaning that the final user who carries out, on a private basis, the reproduction of a protected work must, in principle, be regarded as the person responsible for paying the fair compensation provided for in Article 5(2)(b). However, it is open to the Member States to establish a private copying levy chargeable to the persons who make reproduction equipment, devices and media available to that final user, since they are able to pass on the amount of that levy in the price paid by the final user for that service.

2. Directive 2001/29, in particular Article 5(2)(b) and (5) thereof, must be interpreted as meaning that it is for the Member State which has introduced a system of private copying levies chargeable to the manufacturer or importer of media for reproduction of protected works, and on the territory of which the harm caused to authors by the use for private purposes of their work by purchasers who reside there occurs, to ensure that those authors actually receive the fair compensation intended to compensate them for that harm. In that regard, the mere fact that the commercial seller of reproduction equipment, devices and media is established in a Member State other than that in which the purchasers reside has no bearing on that obligation to achieve a certain result. It is for the national court, where it is impossible to ensure recovery of the fair compensation from the purchasers, to interpret national law in order to allow recovery of that compensation from the person responsible for payment who is acting on a commercial basis.

C-135/10 SCF ("Del Corso")

The provisions of the Agreement on Trade-Related Aspects of Intellectual Property Rights, which constitutes Annex 1C to the Agreement establishing the World Trade Organisation (WTO) signed at Marrakesh on 15 April 1994 and approved by Council Decision 94/800/EC of 22 December 1994 concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994) and of the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty of 20 December 1996 are applicable in the legal order of the European Union.

As the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations, adopted at Rome on 26 October 1961, does not form part of the legal order of the European Union it is not applicable there; however, it has indirect effects within the European Union.

Individuals may not rely directly either on that convention or on the agreement or the treaty mentioned above.

The concept of 'communication to the public' which appears in Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted in the light of the equivalent concepts contained in the convention, the agreement and the treaty mentioned above and in such a way that it is compatible with those agreements, taking account of the context in which those concepts are found and the purpose of the relevant provisions of the agreements as regards intellectual property.

2. The concept of 'communication to the public' for the purposes of Article 8(2) of Directive 92/100 must be interpreted as meaning that it does not cover the broadcasting, free of charge, of phonograms within private dental practices engaged in professional economic activity, such as the one at issue in the main proceedings, for the benefit of patients of those practices and enjoyed by them without any active choice on their part. Therefore such an act of transmission does not entitle the phonogram producers to the payment of remuneration.

C-145/10 Painer

1. Article 6(1) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as not precluding its application solely because actions against several defendants for substantially identical copyright infringements are brought on national legal grounds which vary according to the Member States concerned. It is for the referring court to assess, in the light of all the elements of the case, whether there is a risk of irreconcilable judgments if those actions were determined separately.

2. Article 6 of Council Directive 93/98/EEC of 29 October 1993 harmonising the term of protection of copyright and certain related rights must be interpreted as meaning that a portrait photograph can, under that provision, be protected by copyright if, which it is for the national court to determine in each case, such photograph is an intellectual creation of the author reflecting his personality and expressing his free and creative choices in the production of that photograph. Since it has been determined that the portrait photograph in question is a work, its protection is not inferior to that enjoyed by any other work, including other photographic works.

3. Article 5(3)(e) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, read in the light of Article 5(5) of that Directive, must be interpreted as meaning that the media, such as newspaper publishers, may not use, of their own volition, a work protected by copyright by invoking an objective of public security. However, it is conceivable that a newspaper publisher might, in specific cases, contribute to the fulfilment of such an objective by publishing a photograph of a person for whom a search has been launched. It should be required that such initiative is taken, first, within the framework of a decision or action taken by the competent national authorities to ensure public security and, second, by agreement and in coordination with those authorities, in order to avoid the risk of interfering with the measures taken by them, without, however, a specific, current and express appeal, on the part of the security authorities, for publication of a photograph for the purposes of an investigation being necessary.

4. Article 5(3)(d) of Directive 2001/29, read in the light of Article 5(5) of that Directive, must be interpreted as not precluding its application where a press report quoting a work or other protected subject-matter is not a literary work protected by copyright.

5. Article 5(3)(d) of Directive 2001/29, read in the light of Article 5(5) of that Directive, must be interpreted as meaning that its application is subject to the obligation to indicate the source, including the name of the author or performer, of the work or other protected subject-matter quoted. However, if, in applying Article 5(3)(e) of Directive 2001/29, that name was not indicated, that obligation must be regarded as having been fulfilled if the source alone is indicated.

C-277/10 Luksan

1. Articles 1 and 2 of Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, and Articles 2 and 3 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society in conjunction with Articles 2 and 3 of Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property and with Article 2 of Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights, must be interpreted as meaning that rights to exploit a cinematographic work such as those at issue in the main proceedings (reproduction right, satellite broadcasting right and any other right of communication to the

public through the making available to the public) vest by operation of law, directly and originally, in the principal director. Consequently, those provisions must be interpreted as precluding national legislation which allocates those exploitation rights by operation of law exclusively to the producer of the work in question.

2. European Union law must be interpreted as allowing the Member States the option of laying down a presumption of transfer, in favour of the producer of a cinematographic work, of rights to exploit the cinematographic work such as those at issue in the main proceedings (satellite broadcasting right, reproduction right and any other right of communication to the public through the making available to the public), provided that such a presumption is not an irrebuttable one precluding the principal director of that work from agreeing otherwise.

3. European Union law must be interpreted as meaning that, in his capacity as author of a cinematographic work, the principal director thereof must be entitled, by operation of law, directly and originally, to the right to the fair compensation provided for in Article 5(2)(b) of Directive 2001/29 under the 'private copying' exception.

4. European Union law must be interpreted as not allowing the Member States the option of laying down a presumption of transfer, in favour of the producer of a cinematographic work, of the right to fair compensation vesting in the principal director of that work, whether that presumption is couched in irrebuttable terms or may be departed from.

C-360/10 SABAM

Directives:

- 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce);
- 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; and
- 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights,

read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering:

- information which is stored on its servers by its service users;
- which applies indiscriminately to all of those users;
- as a preventative measure;
- exclusively at its expense; and
- for an unlimited period,

which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright.

C-607/11 ITV Broadcasting and Others

1. The concept of 'communication to the public', within the meaning of Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, must be interpreted as meaning that it covers a retransmission of the works included in a terrestrial television broadcast

- where the retransmission is made by an organisation other than the original broadcaster;
- by means of an internet stream made available to the subscribers of that other organisation who may receive that retransmission by logging on to its server;
- even though those subscribers are within the area of reception of that terrestrial television broadcast and may lawfully receive the broadcast on a television receiver.

2. The answer to Question 1 is not influenced by the fact that a retransmission, such as that at issue in the main proceedings, is funded by advertising and is therefore of a profit-making nature.

3. The answer to Question 1 is not influenced by the fact that a retransmission, such as that at issue in the main proceedings, is made by an organisation which is acting in direct competition with the original broadcaster.

C-351/12 OSA

1. Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as precluding national legislation which excludes the right of authors to authorise or prohibit the communication of their works, by a spa establishment which is a business, through the intentional distribution of a signal by means of television or radio sets in the bedrooms of the establishment's patients. Article 5(2)(e), (3)(b) and (5) of that Directive is not such as to affect that interpretation.

2. Article 3(1) of Directive 2001/29 must be interpreted as meaning that it cannot be relied on by a copyright collecting society in a dispute between individuals for the purpose of setting aside national legislation contrary to that provision. However, the national court hearing such a case is required to interpret that legislation, so far as possible, in the light of the wording and purpose of the Directive in order to achieve an outcome consistent with the objective pursued by the Directive.

3. Article 16 of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, and Articles 56 TFEU and 102 TFEU must be interpreted as not precluding national legislation, such as that at issue in the main proceedings, which reserves the exercise of collective management of copyright in respect of certain protected works in the territory of the Member State concerned to a single copyright collecting society and thereby prevents users of such works, such as the spa establishment in the main proceedings, from benefiting from the services provided by another collecting society established in another Member State.

However, Article 102 TFEU must be interpreted as meaning that the imposition by that copyright collecting society of fees for its services which are appreciably higher than those charged in other Member States (a comparison of the fee levels having been made on a consistent basis) or the imposition of a price which is excessive in relation to the economic value of the service provided are indicative of an abuse of a dominant position.

C-355/12 Nintendo and Others

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that the concept of an 'effective technological measure', for the purposes of Article 6(3) of that Directive, is capable of covering technological measures comprising, principally, equipping not only the housing system containing the protected work, such as the videogame, with a recognition device in order to protect it against acts not authorised by the holder of any copyright, but also portable equipment or consoles intended to ensure access to those games and their use.

It is for the national court to determine whether other measures or measures which are not installed in consoles could cause less interference with the activities of third parties or limitations to those activities, while still providing comparable protection of the rightholder's rights. Accordingly, it is relevant to take account, inter alia, of the relative costs of different types of technological measures, of technological and practical aspects of their implementation, and of a comparison of the effectiveness of those different types of technological measures as regards the protection of the rightholder's rights, that effectiveness however not having to be absolute. That court

must also examine the purpose of devices, products or components, which are capable of circumventing those technological measures. In that regard, the evidence of use which third parties actually make of them will, in the light of the circumstances at issue, be particularly relevant. The national court may, in particular, examine how often those devices, products or components are in fact used in disregard of copyright and how often they are used for purposes which do not infringe copyright.

C-435/12 ACI Adam BV and Others

1. EU law, in particular Article 5(2)(b) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, read in conjunction with paragraph 5 of that article, must be interpreted as precluding national legislation, such as that at issue in the main proceedings, which does not distinguish the situation in which the source from which a reproduction for private use is made is lawful from that in which that source is unlawful.

2. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights must be interpreted as not applying to proceedings, such as those in the main proceedings, in which those liable for payment of the fair compensation bring an action before the referring court for a ruling against the body responsible for collecting that remuneration and distributing it to copyright holders, which defends that action.

C-463/12 Copydan Båndkopi

1. Article 5(2)(b) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society does not preclude national legislation which provides that fair compensation is to be paid, in accordance with the exception to the reproduction right for copies made for private use, in respect of multifunctional media such as mobile telephone memory cards, irrespective of whether the main function of such media is to make such copies, provided that one of the functions of the media, be it merely an ancillary function, enables the operator to use them for that purpose. However, the question whether the function is a main or an ancillary one and the relative importance of the medium's capacity to make copies are liable to affect the amount of fair compensation payable. In so far as the prejudice to the rightholder may be regarded as minimal, the making available of such a function need not give rise to an obligation to pay fair compensation.

2. Article 5(2)(b) of Directive 2001/29 does not preclude national legislation which makes the supply of media that may be used for copying for private use, such as mobile telephone memory cards, subject to the levy intended to finance fair compensation payable in accordance with the exception to the reproduction right for copies for private use, but does not make the supply of components whose main purpose is to store copies for private use, such as the internal memories of MP3 players, subject to that levy, provided that those different categories of media and components are not comparable or the different treatment they receive is justified, which is a matter for the national court to determine.

3. Article 5(2)(b) of Directive 2001/29 must be interpreted as not precluding national legislation which requires payment of the levy intended to finance fair compensation, in accordance with the exception to the reproduction right for copies for private use, by producers and importers who sell mobile telephone memory cards to business customers and are aware that those cards will be sold on by those customers but do not know whether the final purchasers of the cards will be individuals or business customers, on condition that:

- the introduction of such a system is justified by practical difficulties;
- the persons responsible for payment are exempt from the levy if they can establish that they have supplied the mobile

telephone memory cards to persons other than natural persons for purposes clearly unrelated to copying for private use, it being understood that the exemption cannot be restricted to the supply of business customers registered with the organisation responsible for administering the levy;

- the system provides for a right to reimbursement of that levy which is effective and does not make it excessively difficult to repay the levy and only the final purchaser of such a memory card may obtain reimbursement by submitting an appropriate application to that organisation.

4. Article 5(2)(b) of Directive 2001/29, read in the light of recital 35 in the preamble to that Directive, must be interpreted as permitting the Member States to provide, in certain cases covered by the exception to the reproduction right for copies for private use, for an exemption from the requirement under that exception to pay fair compensation, provided that the prejudice caused to rightholders in such cases is minimal. It is within the discretion of the Member States to set the threshold for such prejudice, it being understood that that threshold must, *inter alia*, be applied in a manner consistent with the principle of equal treatment.

5. Directive 2001/29 is to be interpreted as meaning that, where a Member State has decided, pursuant to Article 5(2) of that Directive, to exclude, from the material scope of that provision, any right for rightholders to authorise reproduction of their works for private use, any authorisation given by a rightholder for the use of files containing his works can have no bearing on the fair compensation payable in accordance with the exception to the reproduction right for reproductions made in accordance with Article 5(2)(b) of that Directive with the aid of such files and cannot, of itself, give rise to an obligation on the part of the user of the files concerned to pay remuneration of any kind to the rightholder.

6. The implementation of technological measures under Article 6 of Directive 2001/29 for devices used to reproduce protected works, such as DVDs, CDs, MP3 players and computers, can have no effect on the requirement to pay fair compensation in accordance with the exception to the reproduction right in respect of reproductions made for private use by means of such devices. However, the implementation of such measures may have an effect on the actual level of such compensation.

7. Directive 2001/29 precludes national legislation which provides for fair compensation, in accordance with the exception to the reproduction right, in respect of reproductions made using unlawful sources, namely from protected works which are made available to the public without the rightholder's consent.

8. Directive 2001/29 does not preclude national legislation which provides for fair compensation, in accordance with the exception to the reproduction right, in respect of reproductions of protected works made by a natural person by or with the aid of a device which belongs to a third party.

C-466/12 Svensson and Others

1. Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, must be interpreted as meaning that the provision on a website of clickable links to works freely available on another website does not constitute an 'act of communication to the public', as referred to in that provision.

2. Article 3(1) of Directive 2001/29 must be interpreted as precluding a Member State from giving wider protection to copyright holders by laying down that the concept of communication to the public includes a wider range of activities than those referred to in that provision.

C-117/13 Eugen Ulmer ("TU Darmstadt")

1. The concept of 'purchase or licensing terms' provided for in Article 5(3)(n) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be understood as requiring that the rightholder and an establishment, such as a publicly

accessible library, referred to in that provision must have concluded a licensing agreement in respect of the work in question that sets out the conditions in which that establishment may use that work.

2. Article 5(3)(n) of Directive 2001/29, read in conjunction with Article 5(2)(c) of that Directive, must be interpreted to mean that it does not preclude Member States from granting to publicly accessible libraries covered by those provisions the right to digitise the works contained in their collections, if such act of reproduction is necessary for the purpose of making those works available to users, by means of dedicated terminals, within those establishments.

3. Article 5(3)(n) of Directive 2001/29 must be interpreted to mean that it does not extend to acts such as the printing out of works on paper or their storage on a USB stick, carried out by users from dedicated terminals installed in publicly accessible libraries covered by that provision. However, such acts may, if appropriate, be authorised under national legislation transposing the exceptions or limitations provided for in Article 5(2)(a) or (b) of that Directive provided that, in each individual case, the conditions laid down by those provisions are met.

C-201/13 Deckmyn and Vrijheidsfonds

1. Article 5(3)(k) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, must be interpreted as meaning that the concept of ‘parody’ appearing in that provision is an autonomous concept of EU law.

2. Article 5(3)(k) of Directive 2001/29 must be interpreted as meaning that the essential characteristics of parody, are, first, to evoke an existing work, while being noticeably different from it, and secondly, to constitute an expression of humour or mockery. The concept of ‘parody’, within the meaning of that provision, is not subject to the conditions that the parody should display an original character of its own, other than that of displaying noticeable differences with respect to the original parodied work; that it could reasonably be attributed to a person other than the author of the original work itself; that it should relate to the original work itself or mention the source of the parodied work.

However, the application, in a particular case, of the exception for parody, within the meaning of Article 5(3)(k) of Directive 2001/29, must strike a fair balance between, on the one hand, the interests and rights of persons referred to in Articles 2 and 3 of that Directive, and, on the other, the freedom of expression of the user of a protected work who is relying on the exception for parody, within the meaning of Article 5(3)(k).

It is for the national court to determine, in the light of all the circumstances of the case in the main proceedings, whether the application of the exception for parody, within the meaning of Article 5(3)(k) of Directive 2001/29, on the assumption that the drawing at issue fulfils the essential requirements of parody, preserves that fair balance.

C-279/13 C More Entertainment

Article 3(2) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as not precluding national legislation extending the exclusive right of the broadcasting organisations referred to in Article 3(2)(d) as regards acts of communication to the public which broadcasts of sporting fixtures made live on internet, such as those at issue in the main proceedings, may constitute, provided that such an extension does not undermine the protection of copyright.

C-360/13 Public Relations Consultants Association (“Meltwater”)

Article 5 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that the copies on the user’s computer screen and the copies in the internet ‘cache’ of that computer’s hard disk, made by an end-user in the course of viewing a website, satisfy the conditions that those copies must be temporary, that they must be transient or incidental in nature and that they must constitute an integral and essential part of a technological process, as well as the conditions laid down in Article 5(5) of that Directive, and that they may therefore be made without the authorisation of the copyright holders.

C-419/13 Art & Allposters International

Article 4(2) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that the rule of exhaustion of the distribution right set out in Article 4(2) of Directive 2001/29 does not apply in a situation where a reproduction of a protected work, after having been marketed in the European Union with the copyright holder’s consent, has undergone an alteration of its medium, such as the transfer of that reproduction from a paper poster onto a canvas, and is placed on the market again in its new form.

C-516/13 Dimensione Direct Sales and Labianca

Article 4(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that it allows a holder of an exclusive right to distribute a protected work to prevent an offer for sale or a targeted advertisement of the original or a copy of that work, even if it is not established that that advertisement gave rise to the purchase of the protected work by an EU buyer, in so far as that advertisement invites consumers of the Member State in which that work is protected by copyright to purchase it.

Directive 2009/24/EC on the legal protection of computer programs

[...]

(1) The content of Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs [3] has been amended [4]. In the interests of clarity and rationality the said Directive should be codified.

(2) The development of computer programs requires the investment of considerable human, technical and financial resources while computer programs can be copied at a fraction of the cost needed to develop them independently.

(3) Computer programs are playing an increasingly important role in a broad range of industries and computer program technology can accordingly be considered as being of fundamental importance for the Community’s industrial development.

(4) Certain differences in the legal protection of computer programs offered by the laws of the Member States have direct and negative effects on the functioning of the internal market as regards computer programs.

(5) Existing differences having such effects need to be removed and new ones prevented from arising, while differences not adversely affecting the functioning of the internal market to a substantial degree need not be removed or prevented from arising.

(6) The Community's legal framework on the protection of computer programs can accordingly in the first instance be limited to establishing that Member States should accord protection to computer programs under copyright law as literary works and, further, to establishing who and what should be protected, the exclusive rights on which protected persons should be able to rely in order to authorise or prohibit certain acts and for how long the protection should apply.

(7) For the purpose of this Directive, the term "computer program" shall include programs in any form, including those which are incorporated into hardware. This term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage.

(8) In respect of the criteria to be applied in determining whether or not a computer program is an original work, no tests as to the qualitative or aesthetic merits of the program should be applied.

(9) The Community is fully committed to the promotion of international standardisation.

(10) The function of a computer program is to communicate and work together with other components of a computer system and with users and, for this purpose, a logical and, where appropriate, physical interconnection and interaction is required to permit all elements of software and hardware to work with other software and hardware and with users in all the ways in which they are intended to function. The parts of the program which provide for such interconnection and interaction between elements of software and hardware are generally known as "interfaces". This functional interconnection and interaction is generally known as "interoperability"; such interoperability can be defined as the ability to exchange information and mutually to use the information which has been exchanged.

(11) For the avoidance of doubt, it has to be made clear that only the expression of a computer program is protected and that ideas and principles which underlie any element of a program, including those which underlie its interfaces, are not protected by copyright under this Directive. In accordance with this principle of copyright, to the extent that logic, algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected under this Directive. In accordance with the legislation and case-law of the Member States and the international copyright conventions, the expression of those ideas and principles is to be protected by copyright.

(12) For the purposes of this Directive, the term "rental" means the making available for use, for a limited period of time and for profit-making purposes, of a computer program or a copy thereof. This term does not include public lending, which, accordingly, remains outside the scope of this Directive.

(13) The exclusive rights of the author to prevent the unauthorised reproduction of his work should be subject to a limited exception in the case of a computer program to allow the reproduction technically necessary for the use of that program by the lawful acquirer. This means that the acts of loading and running necessary for the use of a copy of a program which has been lawfully acquired, and the act of correction of its errors, may not be prohibited by contract. In the absence of specific contractual provisions, including when a copy of the program has been sold, any other act necessary for the use of the copy of a program may be performed in accordance with its intended purpose by a lawful acquirer of that copy.

(14) A person having a right to use a computer program should not be prevented from performing acts necessary to observe, study or test the functioning of the program, provided that those acts do not infringe the copyright in the program.

(15) The unauthorised reproduction, translation, adaptation or transformation of the form of the code in which a copy of a computer program has been made available constitutes an infringement of the exclusive rights of the author. Nevertheless, circumstances may exist when such a reproduction of the code and translation of its form are indispensable to obtain the necessary information to achieve the interoperability of an independently created program with other programs. It has therefore to be considered that, in these limited circumstances only, performance of the acts of reproduction and translation by or on behalf of a person having a right to use a copy of the program is legitimate and compatible with fair practice and must therefore be deemed not to require the authorisation of the rightholder. An objective of this exception is to make it possible to connect all components of a computer system, including those of different manufacturers, so that they can work together. Such an exception to the author's exclusive rights may not be used in a way which prejudices the legitimate interests of the rightholder or which conflicts with a normal exploitation of the program.

(16) Protection of computer programs under copyright laws should be without prejudice to the application, in appropriate cases, of other forms of protection. However, any contractual provisions contrary to the provisions of this Directive laid down in respect of decompilation or to the exceptions provided for by this Directive with regard to the making of a back-up copy or to observation, study or testing of the functioning of a program should be null and void.

(17) The provisions of this Directive are without prejudice to the application of the competition rules under Articles 81 and 82 of the Treaty if a dominant supplier refuses to make information available which is necessary for interoperability as defined in this Directive.

(18) The provisions of this Directive should be without prejudice to specific requirements of Community law already enacted in respect of the publication of interfaces in the telecommunications sector or Council Decisions relating to standardisation in the field of information technology and telecommunication.

(19) This Directive does not affect derogations provided for under national legislation in accordance with the Berne Convention on points not covered by this Directive.

(20) This Directive should be without prejudice to the obligations of the Member States relating to the time-limits for transposition into national law of the Directives set out in Annex I, Part B,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Object of protection

1. In accordance with the provisions of this Directive, Member States shall protect computer programs, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works. For the purposes of this Directive, the term "computer programs" shall include their preparatory design material.

2. Protection in accordance with this Directive shall apply to the expression in any form of a computer program. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive.

3. A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection.

4. The provisions of this Directive shall apply also to programs created before 1 January 1993, without prejudice to any acts concluded and rights acquired before that date.

Article 2

Authorship of computer programs

1. The author of a computer program shall be the natural person or group of natural persons who has created the program or, where the legislation of the Member State permits,

the legal person designated as the rightholder by that legislation.

Where collective works are recognised by the legislation of a Member State, the person considered by the legislation of the Member State to have created the work shall be deemed to be its author.

2. In respect of a computer program created by a group of natural persons jointly, the exclusive rights shall be owned jointly.

3. Where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by contract.

Article 3

Beneficiaries of protection

Protection shall be granted to all natural or legal persons eligible under national copyright legislation as applied to literary works.

Article 4 Restricted acts

1. Subject to the provisions of Articles 5 and 6, the exclusive rights of the rightholder within the meaning of Article 2 shall include the right to do or to authorise:

(a) the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole; in so far as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the rightholder;

(b) the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program;

(c) any form of distribution to the public, including the rental, of the original computer program or of copies thereof.

2. The first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof.

Article 5 Exceptions to the restricted acts

1. In the absence of specific contractual provisions, the acts referred to in points (a) and (b) of Article 4(1) shall not require authorisation by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.

2. The making of a back-up copy by a person having a right to use the computer program may not be prevented by contract in so far as it is necessary for that use.

3. The person having a right to use a copy of a computer program shall be entitled, without the authorisation of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do.

Article 6 Decompilation

1. The authorisation of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of points (a) and (b) of Article 4(1) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

(a) those acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so;

(b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in point (a); and

(c) those acts are confined to the parts of the original program which are necessary in order to achieve interoperability.

2. The provisions of paragraph 1 shall not permit the information obtained through its application:

(a) to be used for goals other than to achieve the interoperability of the independently created computer program;

(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or

(c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

3. In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the rightholder's legitimate interests or conflicts with a normal exploitation of the computer program.

Article 7 Special measures of protection

1. Without prejudice to the provisions of Articles 4, 5 and 6, Member States shall provide, in accordance with their national legislation, appropriate remedies against a person committing any of the following acts:

(a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;

(b) the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;

(c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.

2. Any infringing copy of a computer program shall be liable to seizure in accordance with the legislation of the Member State concerned.

3. Member States may provide for the seizure of any means referred to in point (c) of paragraph 1.

Article 8

Continued application of other legal provisions

The provisions of this Directive shall be without prejudice to any other legal provisions such as those concerning patent rights, trade-marks, unfair competition, trade secrets, protection of semi-conductor products or the law of contract.

Any contractual provisions contrary to Article 6 or to the exceptions provided for in Article 5(2) and (3) shall be null and void.

[...]

Article 11 Entry into force

This Directive shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

[...]

[1] OJ C 204, 9.8.2008, p. 24.

[2] Opinion of the European Parliament of 17 June 2008 (not yet published in the Official Journal) and Council Decision of 23 March 2009.

[3] OJ L 122, 17.5.1991, p. 42.

[4] See Annex I, Part A.

Relevant Case-Law on Directive 2009/24/EC

C-393/09 Bezpečnostní softwarová asociace

1. A graphic user interface is not a form of expression of a computer program within the meaning of Article 1(2) of Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs and cannot be protected by copyright as a computer program under that Directive. Nevertheless, such an interface can be protected by copyright as a work by Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society if that interface is its author's own intellectual creation.

2. Television broadcasting of a graphic user interface does not constitute communication to the public of a work protected by copyright within the meaning of Article 3(1) of Directive 2001/29.

C-406/10 SAS Institute

1. Article 1(2) of Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs must be interpreted as meaning that neither the functionality of a computer program nor the programming language and the format of data files used in a computer program in order to exploit certain of its functions constitute a form of expression of that program and, as such, are not protected by copyright in computer programs for the purposes of that Directive.

2. Article 5(3) of Directive 91/250 must be interpreted as meaning that a person who has obtained a copy of a computer program under a licence is entitled, without the authorisation of the owner of the copyright, to observe, study or test the functioning of that program so as to determine the ideas and principles which underlie any element of the program, in the case where that person carries out acts covered by that licence and acts of loading and running necessary for the use of the computer program, and on condition that that person does not infringe the exclusive rights of the owner of the copyright in that program.

3. Article 2(a) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that the reproduction, in a computer program or a user manual for that program, of certain elements described in the user manual for another computer program protected by copyright is capable of constituting an infringement of the copyright in the latter manual if - this being a matter for the national court to ascertain - that reproduction constitutes the expression of the intellectual creation of the author of the user manual for the computer program protected by copyright.

C-128/11 UsedSoft

1. Article 4(2) of Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs must be interpreted as meaning that the right of distribution of a copy of a computer program is exhausted if the copyright holder who has authorised, even free of charge, the downloading of that copy from the internet onto a data carrier has also conferred, in return for payment of a fee intended to enable him to obtain a remuneration corresponding to the economic value of the copy of the work of which he is the proprietor, a right to use that copy for an unlimited period.

2. Articles 4(2) and 5(1) of Directive 2009/24 must be interpreted as meaning that, in the event of the resale of a user licence entailing the resale of a copy of a computer program downloaded from the copyright holder's website, that licence having originally been granted by that rightholder to the first acquirer for an unlimited period in return for payment of a fee intended to enable the rightholder to obtain a remuneration corresponding to the economic value of that copy of his work, the second acquirer of the licence, as well as any subsequent acquirer of it, will be able to rely on the exhaustion of the distribution right under Article 4(2) of that Directive, and hence be regarded as lawful acquirers of a copy of a computer program within the meaning of Article 5(1) of that Directive and benefit from the right of reproduction provided for in that provision.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 57 (2), 66 and 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure laid down in Article 189b of the Treaty (3),

(1) Whereas databases are at present not sufficiently protected in all Member States by existing legislation; whereas such protection, where it exists, has different attributes;

(2) Whereas such differences in the legal protection of databases offered by the legislation of the Member States have direct negative effects on the functioning of the internal market

as regards databases and in particular on the freedom of natural and legal persons to provide on-line database goods and services on the basis of harmonized legal arrangements throughout the Community; whereas such differences could well become more pronounced as Member States introduce new legislation in this field, which is now taking on an increasingly international dimension;

(3) Whereas existing differences distorting the functioning of the internal market need to be removed and new ones prevented from arising, while differences not adversely affecting the functioning of the internal market or the development of an information market within the Community need not be removed or prevented from arising;

(4) Whereas copyright protection for databases exists in varying forms in the Member States according to legislation or case-law, and whereas, if differences in legislation in the scope

and conditions of protection remain between the Member States, such unharmonized intellectual property rights can have the effect of preventing the free movement of goods or services within the Community;

(5) Whereas copyright remains an appropriate form of exclusive right for authors who have created databases;

(6) Whereas, nevertheless, in the absence of a harmonized system of unfair-competition legislation or of case-law, other measures are required in addition to prevent the unauthorized extraction and/or re-utilization of the contents of a database;

(7) Whereas the making of databases requires the investment of considerable human, technical and financial resources while such databases can be copied or accessed at a fraction of the cost needed to design them independently;

(8) Whereas the unauthorized extraction and/or re-utilization of the contents of a database constitute acts which can have serious economic and technical consequences;

(9) Whereas databases are a vital tool in the development of an information market within the Community; whereas this tool will also be of use in many other fields;

(10) Whereas the exponential growth, in the Community and worldwide, in the amount of information generated and processed annually in all sectors of commerce and industry calls for investment in all the Member States in advanced information processing systems;

(11) Whereas there is at present a very great imbalance in the level of investment in the database sector both as between the Member States and between the Community and the world's largest database-producing third countries;

(12) Whereas such an investment in modern information storage and processing systems will not take place within the Community unless a stable and uniform legal protection regime is introduced for the protection of the rights of makers of databases;

(13) Whereas this Directive protects collections, sometimes called 'compilations', of works, data or other materials which are arranged, stored and accessed by means which include electronic, electromagnetic or electro-optical processes or analogous processes;

(14) Whereas protection under this Directive should be extended to cover non-electronic databases;

(15) Whereas the criteria used to determine whether a database should be protected by copyright should be defined to the fact that the selection or the arrangement of the contents of the database is the author's own intellectual creation; whereas such protection should cover the structure of the database;

(16) Whereas no criterion other than originality in the sense of the author's intellectual creation should be applied to determine the eligibility of the database for copyright protection, and in particular no aesthetic or qualitative criteria should be applied;

(17) Whereas the term 'database' should be understood to include literary, artistic, musical or other collections of works or collections of other material such as texts, sound, images, numbers, facts, and data; whereas it should cover collections of independent works, data or other materials which are systematically or methodically arranged and can be individually accessed; whereas this means that a recording or an audiovisual, cinematographic, literary or musical work as such does not fall within the scope of this Directive;

(18) Whereas this Directive is without prejudice to the freedom of authors to decide whether, or in what manner, they will allow their works to be included in a database, in particular whether or not the authorization given is exclusive; whereas the protection of databases by the sui generis right is without prejudice to existing rights over their contents, and whereas in particular where an author or the holder of a related right permits some of his works or subject matter to be included in a database pursuant to a non-exclusive agreement, a third party may make use of those works or subject matter subject to the required consent of the author or of the holder of the related right without the sui generis right of the maker of the database being invoked to prevent him doing so, on condition that those

works or subject matter are neither extracted from the database nor re-utilized on the basis thereof;

(19) Whereas, as a rule, the compilation of several recordings of musical performances on a CD does not come within the scope of this Directive, both because, as a compilation, it does not meet the conditions for copyright protection and because it does not represent a substantial enough investment to be eligible under the sui generis right;

(20) Whereas protection under this Directive may also apply to the materials necessary for the operation or consultation of certain databases such as thesaurus and indexation systems;

(21) Whereas the protection provided for in this Directive relates to databases in which works, data or other materials have been arranged systematically or methodically; whereas it is not necessary for those materials to have been physically stored in an organized manner;

(22) Whereas electronic databases within the meaning of this Directive may also include devices such as CD-ROM and CD-i;

(23) Whereas the term 'database' should not be taken to extend to computer programs used in the making or operation of a database, which are protected by Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (4);

(24) Whereas the rental and lending of databases in the field of copyright and related rights are governed exclusively by Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (5);

(25) Whereas the term of copyright is already governed by Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights (6);

(26) Whereas works protected by copyright and subject matter protected by related rights, which are incorporated into a database, remain nevertheless protected by the respective exclusive rights and may not be incorporated into, or extracted from, the database without the permission of the rightholder or his successors in title;

(27) Whereas copyright in such works and related rights in subject matter thus incorporated into a database are in no way affected by the existence of a separate right in the selection or arrangement of these works and subject matter in a database;

(28) Whereas the moral rights of the natural person who created the database belong to the author and should be exercised according to the legislation of the Member States and the provisions of the Berne Convention for the Protection of Literary and Artistic Works; whereas such moral rights remain outside the scope of this Directive;

(29) Whereas the arrangements applicable to databases created by employees are left to the discretion of the Member States; whereas, therefore nothing in this Directive prevents Member States from stipulating in their legislation that where a database is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the database so created, unless otherwise provided by contract;

(30) Whereas the author's exclusive rights should include the right to determine the way in which his work is exploited and by whom, and in particular to control the distribution of his work to unauthorized persons;

(31) Whereas the copyright protection of databases includes making databases available by means other than the distribution of copies;

(32) Whereas Member States are required to ensure that their national provisions are at least materially equivalent in the case of such acts subject to restrictions as are provided for by this Directive;

(33) Whereas the question of exhaustion of the right of distribution does not arise in the case of on-line databases, which come within the field of provision of services; whereas this also applies with regard to a material copy of such a database made by the user of such a service with the consent of the rightholder; whereas, unlike CD-ROM or CD-i, where the

intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which will have to be subject to authorization where the copyright so provides;

(34) Whereas, nevertheless, once the rightholder has chosen to make available a copy of the database to a user, whether by an on-line service or by other means of distribution, that lawful user must be able to access and use the database for the purposes and in the way set out in the agreement with the rightholder, even if such access and use necessitate performance of otherwise restricted acts;

(35) Whereas a list should be drawn up of exceptions to restricted acts, taking into account the fact that copyright as covered by this Directive applies only to the selection or arrangements of the contents of a database; whereas Member States should be given the option of providing for such exceptions in certain cases; whereas, however, this option should be exercised in accordance with the Berne Convention and to the extent that the exceptions relate to the structure of the database; whereas a distinction should be drawn between exceptions for private use and exceptions for reproduction for private purposes, which concerns provisions under national legislation of some Member States on levies on blank media or recording equipment;

(36) Whereas the term 'scientific research' within the meaning of this Directive covers both the natural sciences and the human sciences;

(37) Whereas Article 10 (1) of the Berne Convention is not affected by this Directive;

(38) Whereas the increasing use of digital recording technology exposes the database maker to the risk that the contents of his database may be copied and rearranged electronically, without his authorization, to produce a database of identical content which, however, does not infringe any copyright in the arrangement of his database;

(39) Whereas, in addition to aiming to protect the copyright in the original selection or arrangement of the contents of a database, this Directive seeks to safeguard the position of makers of databases against misappropriation of the results of the financial and professional investment made in obtaining and collection the contents by protecting the whole or substantial parts of a database against certain acts by a user or competitor;

(40) Whereas the object of this sui generis right is to ensure protection of any investment in obtaining, verifying or presenting the contents of a database for the limited duration of the right; whereas such investment may consist in the deployment of financial resources and/or the expending of time, effort and energy;

(41) Whereas the objective of the sui generis right is to give the maker of a database the option of preventing the unauthorized extraction and/or re-utilization of all or a substantial part of the contents of that database; whereas the maker of a database is the person who takes the initiative and the risk of investing; whereas this excludes subcontractors in particular from the definition of maker;

(42) Whereas the special right to prevent unauthorized extraction and/or re-utilization relates to acts by the user which go beyond his legitimate rights and thereby harm the investment; whereas the right to prohibit extraction and/or re-utilization of all or a substantial part of the contents relates not only to the manufacture of a parasitical competing product but also to any user who, through his acts, causes significant detriment, evaluated qualitatively or quantitatively, to the investment;

(43) Whereas, in the case of on-line transmission, the right to prohibit re-utilization is not exhausted either as regards the database or as regards a material copy of the database or of part thereof made by the addressee of the transmission with the consent of the rightholder;

(44) Whereas, when on-screen display of the contents of a database necessitates the permanent or temporary transfer of all or a substantial part of such contents to another medium, that act should be subject to authorization by the rightholder;

(45) Whereas the right to prevent unauthorized extraction and/or re-utilization does not in any way constitute an extension of copyright protection to mere facts or data;

(46) Whereas the existence of a right to prevent the unauthorized extraction and/or re-utilization of the whole or a substantial part of works, data or materials from a database should not give rise to the creation of a new right in the works, data or materials themselves;

(47) Whereas, in the interests of competition between suppliers of information products and services, protection by the sui generis right must not be afforded in such a way as to facilitate abuses of a dominant position, in particular as regards the creation and distribution of new products and services which have an intellectual, documentary, technical, economic or commercial added value; whereas, therefore, the provisions of this Directive are without prejudice to the application of Community or national competition rules;

(48) Whereas the objective of this Directive, which is to afford an appropriate and uniform level of protection of databases as a means to secure the remuneration of the maker of the database, is different from the aim of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (7), which is to guarantee free circulation of personal data on the basis of harmonized rules designed to protect fundamental rights, notably the right to privacy which is recognized in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas the provisions of this Directive are without prejudice to data protection legislation;

(49) Whereas, notwithstanding the right to prevent extraction and/or re-utilization of all or a substantial part of a database, it should be laid down that the maker of a database or rightholder may not prevent a lawful user of the database from extracting and re-utilizing insubstantial parts; whereas, however, that user may not unreasonably prejudice either the legitimate interests of the holder of the sui generis right or the holder of copyright or a related right in respect of the works or subject matter contained in the database;

(50) Whereas the Member States should be given the option of providing for exceptions to the right to prevent the unauthorized extraction and/or re-utilization of a substantial part of the contents of a database in the case of extraction for private purposes, for the purposes of illustration for teaching or scientific research, or where extraction and/or re-utilization are/is carried out in the interests of public security or for the purposes of an administrative or judicial procedure; whereas such operations must not prejudice the exclusive rights of the maker to exploit the database and their purpose must not be commercial;

(51) Whereas the Member States, where they avail themselves of the option to permit a lawful user of a database to extract a substantial part of the contents for the purposes of illustration for teaching or scientific research, may limit that permission to certain categories of teaching or scientific research institution;

(52) Whereas those Member States which have specific rules providing for a right comparable to the sui generis right provided for in this Directive should be permitted to retain, as far as the new right is concerned, the exceptions traditionally specified by such rules;

(53) Whereas the burden of proof regarding the date of completion of the making of a database lies with the maker of the database;

(54) Whereas the burden of proof that the criteria exist for concluding that a substantial modification of the contents of a database is to be regarded as a substantial new investment lies with the maker of the database resulting from such investment;

(55) Whereas a substantial new investment involving a new term of protection may include a substantial verification of the contents of the database;

(56) Whereas the right to prevent unauthorized extraction and/or re-utilization in respect of a database should apply to databases whose makers are nationals or habitual residents of third countries or to those produced by legal persons not

established in a Member State, within the meaning of the Treaty, only if such third countries offer comparable protection to databases produced by nationals of a Member State or persons who have their habitual residence in the territory of the Community;

(57) Whereas, in addition to remedies provided under the legislation of the Member States for infringements of copyright or other rights, Member States should provide for appropriate remedies against unauthorized extraction and/or re-utilization of the contents of a database;

(58) Whereas, in addition to the protection given under this Directive to the structure of the database by copyright, and to its contents against unauthorized extraction and/or re-utilization under the sui generis right, other legal provisions in the Member States relevant to the supply of database goods and services continue to apply;

(59) Whereas this Directive is without prejudice to the application to databases composed of audiovisual works of any rules recognized by a Member State's legislation concerning the broadcasting of audiovisual programmes;

(60) Whereas some Member States currently protect under copyright arrangements databases which do not meet the criteria for eligibility for copyright protection laid down in this Directive; whereas, even if the databases concerned are eligible for protection under the right laid down in this Directive to prevent unauthorized extraction and/or re-utilization of their contents, the term of protection under that right is considerably shorter than that which they enjoy under the national arrangements currently in force; whereas harmonization of the criteria for determining whether a database is to be protected by copyright may not have the effect of reducing the term of protection currently enjoyed by the rightholders concerned; whereas a derogation should be laid down to that effect; whereas the effects of such derogation must be confined to the territories of the Member States concerned,
HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

SCOPE

Article 1 Scope

1. This Directive concerns the legal protection of databases in any form.
2. For the purposes of this Directive, 'database' shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.
3. Protection under this Directive shall not apply to computer programs used in the making or operation of databases accessible by electronic means.

Article 2

Limitations on the scope

This Directive shall apply without prejudice to Community provisions relating to:

- (a) the legal protection of computer programs;
- (b) rental right, lending right and certain rights related to copyright in the field of intellectual property;
- (c) the term of protection of copyright and certain related rights.

CHAPTER II COPYRIGHT

Article 3

Object of protection

1. In accordance with this Directive, databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection.
2. The copyright protection of databases provided for by this Directive shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves.

Article 4

Database authorship

1. The author of a database shall be the natural person or group of natural persons who created the base or, where the legislation of the Member States so permits, the legal person designated as the rightholder by that legislation.
2. Where collective works are recognized by the legislation of a Member State, the economic rights shall be owned by the person holding the copyright.
3. In respect of a database created by a group of natural persons jointly, the exclusive rights shall be owned jointly.

Article 5

Restricted acts

In respect of the expression of the database which is protectable by copyright, the author of a database shall have the exclusive right to carry out or to authorize:

- (a) temporary or permanent reproduction by any means and in any form, in whole or in part;
- (b) translation, adaptation, arrangement and any other alteration;
- (c) any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community;
- (d) any communication, display or performance to the public;
- (e) any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b).

Article 6

Exceptions to restricted acts

1. The performance by the lawful user of a database or of a copy thereof of any of the acts listed in Article 5 which is necessary for the purposes of access to the contents of the databases and normal use of the contents by the lawful user shall not require the authorization of the author of the database. Where the lawful user is authorized to use only part of the database, this provision shall apply only to that part.
2. Member States shall have the option of providing for limitations on the rights set out in Article 5 in the following cases:
 - (a) in the case of reproduction for private purposes of a non-electronic database;
 - (b) where there is use for the sole purpose of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;
 - (c) where there is use for the purposes of public security or for the purposes of an administrative or judicial procedure;
 - (d) where other exceptions to copyright which are traditionally authorized under national law are involved, without prejudice to points (a), (b) and (c).
3. In accordance with the Berne Convention for the protection of Literary and Artistic Works, this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the rightholder's legitimate interests or conflicts with normal exploitation of the database.

CHAPTER III

SUI GENERIS RIGHT

Article 7

Object of protection

1. Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.
2. For the purposes of this Chapter:

(a) 'extraction' shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form;

(b) 're-utilization' shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community;

Public lending is not an act of extraction or re-utilization.

3. The right referred to in paragraph 1 may be transferred, assigned or granted under contractual licence.

4. The right provided for in paragraph 1 shall apply irrespective of the eligibility of that database for protection by copyright or by other rights. Moreover, it shall apply irrespective of eligibility of the contents of that database for protection by copyright or by other rights. Protection of databases under the right provided for in paragraph 1 shall be without prejudice to rights existing in respect of their contents.

5. The repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database shall not be permitted.

Article 8

Rights and obligations of lawful users

1. The maker of a database which is made available to the public in whatever manner may not prevent a lawful user of the database from extracting and/or re-utilizing insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. Where the lawful user is authorized to extract and/or re-utilize only part of the database, this paragraph shall apply only to that part.

2. A lawful user of a database which is made available to the public in whatever manner may not perform acts which conflict with normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database.

3. A lawful user of a database which is made available to the public in any manner may not cause prejudice to the holder of a copyright or related right in respect of the works or subject matter contained in the database.

Article 9

Exceptions to the sui generis right

Member States may stipulate that lawful users of a database which is made available to the public in whatever manner may, without the authorization of its maker, extract or re-utilize a substantial part of its contents:

(a) in the case of extraction for private purposes of the contents of a non-electronic database;

(b) in the case of extraction for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved;

(c) in the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure.

Article 10

Term of protection

1. The right provided for in Article 7 shall run from the date of completion of the making of the database. It shall expire fifteen years from the first of January of the year following the date of completion.

2. In the case of a database which is made available to the public in whatever manner before expiry of the period provided for in paragraph 1, the term of protection by that right shall expire fifteen years from the first of January of the year following the date when the database was first made available to the public.

3. Any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of

successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection.

Article 11

Beneficiaries of protection under the sui generis right

1. The right provided for in Article 7 shall apply to database whose makers or rightholders are nationals of a Member State or who have their habitual residence in the territory of the Community.

2. Paragraph 1 shall also apply to companies and firms formed in accordance with the law of a Member State and having their registered office, central administration or principal place of business within the Community; however, where such a company or firm has only its registered office in the territory of the Community, its operations must be genuinely linked on an ongoing basis with the economy of a Member State.

3. Agreements extending the right provided for in Article 7 to databases made in third countries and falling outside the provisions of paragraphs 1 and 2 shall be concluded by the Council acting on a proposal from the Commission. The term of any protection extended to databases by virtue of that procedure shall not exceed that available pursuant to Article 10.

CHAPTER IV

COMMON PROVISIONS

Article 12

Remedies

Member States shall provide appropriate remedies in respect of infringements of the rights provided for in this Directive.

Article 13

Continued application of other legal provisions

This Directive shall be without prejudice to provisions concerning in particular copyright, rights related to copyright or any other rights or obligations subsisting in the data, works or other materials incorporated into a database, patent rights, trade marks, design rights, the protection of national treasures, laws on restrictive practices and unfair competition, trade secrets, security, confidentiality, data protection and privacy, access to public documents, and the law of contract.

Article 14

Application over time

1. Protection pursuant to this Directive as regards copyright shall also be available in respect of databases created prior to the date referred to in Article 16 (1) which on that date fulfil the requirements laid down in this Directive as regards copyright protection of databases.

2. Notwithstanding paragraph 1, where a database protected under copyright arrangements in a Member State on the date of publication of this Directive does not fulfil the eligibility criteria for copyright protection laid down in Article 3 (1), this Directive shall not result in any curtailment in that Member State of the remaining term of protection afforded under those arrangements.

3. Protection pursuant to the provisions of this Directive as regards the right provided for in Article 7 shall also be available in respect of databases the making of which was completed not more than fifteen years prior to the date referred to in Article 16 (1) and which on that date fulfil the requirements laid down in Article 7.

4. The protection provided for in paragraphs 1 and 3 shall be without prejudice to any acts concluded and rights acquired before the date referred to in those paragraphs.

5. In the case of a database the making of which was completed not more than fifteen years prior to the date referred to in Article 16 (1), the term of protection by the right provided for in Article 7 shall expire fifteen years from the first of January following that date.

Article 15

Binding nature of certain provisions

Any contractual provision contrary to Articles 6 (1) and 8 shall be null and void.

Article 16

Final provisions

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive before 1 January 1998.

When Member States adopt these provisions, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field governed by this Directive.

3. Not later than at the end of the third year after the date referred to in paragraph 1, and every three years thereafter, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, in which, inter alia, on the basis of specific information supplied by the Member States, it shall

examine in particular the application of the sui generis right, including Articles 8 and 9, and shall verify especially whether the application of this right has led to abuse of a dominant position or other interference with free competition which would justify appropriate measures being taken, including the establishment of non-voluntary licensing arrangements. Where necessary, it shall submit proposals for adjustment of this Directive in line with developments in the area of databases.

[...]

(1) OJ No C 156, 23. 6. 1992, p. 4 and

OJ No C 308, 15. 11. 1993, p. 1.

(2) OJ No C 19, 25. 1. 1993, p. 3.

(3) Opinion of the European Parliament of 23 June 1993 (OJ No C 194, 19. 7. 1993, p. 144), Common Position of the Council of 10 July 1995 (OJ No C 288, 30. 10. 1995, p. 14), Decision of the European Parliament of 14 December 1995 (OJ No C 17, 22. 1. 1996) and Council Decision of 26 February 1996.

(4) OJ No L 122, 17. 5. 1991, p. 42. Directive as last amended by Directive 93/98/EEC (OJ No L 290, 24. 11. 1993, p. 9.)

(5) OJ No L 346, 27. 11. 1992, p. 61.

(6) OJ No L 290, 24. 11. 1993, p. 9.

(7) OJ No L 281, 23. 11. 1995, p. 31.

Relevant Case-Law on Directive 96/9/EC

C-203/02 The British Horseracing Board Ltd and Others

1. The expression 'investment in ... the obtaining ... of the contents' of a database in Article 7(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases must be understood to refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the resources used for the creation of materials which make up the contents of a database.

The expression 'investment in ... the ... verification ... of the contents' of a database in Article 7(1) of Directive 96/9 must be understood to refer to the resources used, with a view to ensuring the reliability of the information contained in that database, to monitor the accuracy of the materials collected when the database was created and during its operation. The resources used for verification during the stage of creation of materials which are subsequently collected in a database do not fall within that definition.

The resources used to draw up a list of horses in a race and to carry out checks in that connection do not constitute investment in the obtaining and verification of the contents of the database in which that list appears.

2. The terms 'extraction' and 're-utilisation' as defined in Article 7 of Directive 96/9 must be interpreted as referring to any unauthorised act of appropriation and distribution to the public of the whole or a part of the contents of a database. Those terms do not imply direct access to the database concerned.

The fact that the contents of a database were made accessible to the public by its maker or with his consent does not affect the right of the maker to prevent acts of extraction and/or re-utilisation of the whole or a substantial part of the contents of a database.

3. The expression 'substantial part, evaluated ... quantitatively, of the contents of [a] database' in Article 7 of Directive 96/9 refers to the volume of data extracted from the database and/or re-utilised and must be assessed in relation to the total volume of the contents of the database.

The expression 'substantial part, evaluated qualitatively ... of the contents of [a] database' refers to the scale of the investment in the obtaining, verification or presentation of the contents of the subject of the act of extraction and/or re-utilisation, regardless of whether that subject represents a

quantitatively substantial part of the general contents of the protected database.

Any part which does not fulfil the definition of a substantial part, evaluated both quantitatively and qualitatively, falls within the definition of an insubstantial part of the contents of a database.

4. The prohibition laid down by Article 7(5) of Directive 96/9 refers to unauthorised acts of extraction or re-utilisation the cumulative effect of which is to reconstitute and/or make available to the public, without the authorisation of the maker of the database, the whole or a substantial part of the contents of that database and thereby seriously prejudice the investment by the maker.

C-444/02 Fixtures Marketing ("OPAP")

The term 'database' as defined in Article 1(2) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases refers to any collection of works, data or other materials, separable from one another without the value of their contents being affected, including a method or system of some sort for the retrieval of each of its constituent materials.

A fixture list for a football league such as that at issue in the case in the main proceedings constitutes a database within the meaning of Article 1(2) of Directive 96/9.

The expression 'investment in ... the obtaining ... of the contents' of a database in Article 7(1) of Directive 96/9 must be understood to refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the resources used for the creation of materials which make up the contents of a database. In the context of drawing up a fixture list for the purpose of organising football league fixtures, therefore, it does not cover the resources used to establish the dates, times and the team pairings for the various matches in the league.

C-338/02 Fixtures Marketing ("Svenska Spel AB")

The expression 'investment in ... the obtaining ... of the contents' of a database in Article 7(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases must be understood to refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the

resources used for the creation of materials which make up the contents of a database. In the context of drawing up a fixture list for the purpose of organising football league fixtures, therefore, it does not cover the resources used to establish the dates, times and the team pairings for the various matches in the league.

C-304/07 Directmedia Publishing

The transfer of material from a protected database to another database following an on-screen consultation of the first database and an individual assessment of the material contained in that first database is capable of constituting an 'extraction', within the meaning of Article 7 of Directive 96/9 of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, to the extent that – which it is for the referring court to ascertain – that operation amounts to the transfer of a substantial part, evaluated qualitatively or quantitatively, of the contents of the protected database, or to transfers of insubstantial parts which, by their repeated or systematic nature, would have resulted in the reconstruction of a substantial part of those contents.

C-545/07 Apis-Hristovich

1. The delimitation of the concepts of 'permanent transfer' and 'temporary transfer' in Article 7 of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases is based on the criterion of the length of time during which materials extracted from a protected database are stored in a medium other than that database. The time at which there is an extraction, within the meaning of Article 7, from a protected database, accessible electronically, is when the materials which are the subject of the act of transfer are stored in a medium other than that database. The concept of extraction is independent of the objective pursued by the perpetrator of the act at issue, of any modifications he may make to the contents of the materials thus transferred, and of any differences in the structural organisation of the databases concerned. The fact that the physical and technical characteristics present in the contents of a protected database made by a particular person also appear in the contents of a database made by another person may be interpreted as evidence of extraction within the meaning of Article 7 of Directive 96/9, unless that coincidence can be explained by factors other than a transfer between the two databases concerned. The fact that materials obtained by the maker of a database from sources not accessible to the public also appear in a database made by another person is not sufficient, in itself, to prove the existence of such extraction but can constitute circumstantial evidence thereof.

The nature of the computer program used to manage two electronic databases is not a factor in assessing the existence of extraction within the meaning of Article 7 of Directive 96/9.

2. Article 7 of Directive 96/9 must be interpreted as meaning that, where there is a body of materials composed of separate modules, the volume of the materials allegedly extracted and/or re-utilised from one of those modules must, in order to assess whether there has been extraction and/or re-utilisation of a substantial part, evaluated quantitatively, of the contents of a database within the meaning of that article, be compared with the total contents of that module, if the latter constitutes, in itself, a database which fulfils the conditions for protection by the sui generis right. Otherwise, and in so far as the body of materials constitutes a database protected by that right, the comparison must be made between the volume of the materials allegedly extracted and/or re-utilised from the various modules of that database and its total contents.

The fact that the materials allegedly extracted and/or re-utilised from a database protected by the sui generis right were obtained by the maker of that database from sources not accessible to the public may, according to the amount of human, technical and/or financial resources deployed by the maker to collect the materials at issue from those sources, affect the classification of those materials as a substantial part, evaluated

qualitatively, of the contents of the database concerned, within the meaning of Article 7 of Directive 96/9.

The fact that part of the materials contained in a database are official and accessible to the public does not relieve the national court of an obligation, in assessing whether there has been extraction and/or re-utilisation of a substantial part of the contents of that database, to verify whether the materials allegedly extracted and/or re-utilised from that database constitute a substantial part, evaluated quantitatively, of its contents or, as the case may be, whether they constitute a substantial part, evaluated qualitatively, of the database inasmuch as they represent, in terms of the obtaining, verification and presentation thereof, a substantial human, technical or financial investment.

C-604/10 Football Dataco and Others

1. Article 3(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases must be interpreted as meaning that a 'database' within the meaning of Article 1(2) of that Directive is protected by the copyright laid down by that Directive provided that the selection or arrangement of the data which it contains amounts to an original expression of the creative freedom of its author, which is a matter for the national court to determine.

As a consequence:

- the intellectual effort and skill of creating that data are not relevant in order to assess the eligibility of that database for protection by that right;
- it is irrelevant, for that purpose, whether or not the selection or arrangement of that data includes the addition of important significance to that data, and
- the significant labour and skill required for setting up that database cannot as such justify such a protection if they do not express any originality in the selection or arrangement of the data which that database contains.

2. Directive 96/9 must be interpreted as meaning that, subject to the transitional provision contained in Article 14(2) of that Directive, it precludes national legislation which grants databases, as defined in Article 1(2) of the Directive, copyright protection under conditions which are different to those set out in Article 3(1) of the Directive.

C-202/12 Innoweb

Article 7(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases must be interpreted as meaning that an operator who makes available on the Internet a dedicated meta search engine such as that at issue in the main proceedings re-utilises the whole or a substantial part of the contents of a database protected under Article 7, where that dedicated meta engine:

- provides the end user with a search form which essentially offers the same range of functionality as the search form on the database site;
- 'translates' queries from end users into the search engine for the database site 'in real time', so that all the information on that database is searched through; and
- presents the results to the end user using the format of its website, grouping duplications together into a single block item but in an order that reflects criteria comparable to those used by the search engine of the database site concerned for presenting results.

C-30/14 Ryanair

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases must be interpreted as meaning that it is not applicable to a database which is not protected either by copyright or by the sui generis right under that Directive, so that Articles 6(1), 8 and 15 of that Directive do not preclude the author of such a database from laying down contractual limitations on its use by third parties, without prejudice to the applicable national law.

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights

Article 1 – Subject matter

This Directive concerns the measures, procedures and remedies necessary to ensure the enforcement of intellectual property rights. For the purposes of this Directive, the term 'intellectual property rights' includes industrial property rights.

Article 2 – Scope

1. Without prejudice to the means which are or may be provided for in Community or national legislation, in so far as those means may be more favourable for rightholders, the measures,

procedures and remedies provided for by this Directive shall apply, in accordance with Article 3, to any infringement of intellectual property rights as provided for by Community law and/or by the national law of the Member State concerned.

2. This Directive shall be without prejudice to the specific provisions on the enforcement of rights and on exceptions contained in Community legislation concerning copyright and rights related

to copyright, notably those found in Directive 91/250/EEC and, in particular, Article 7 thereof or in Directive 2001/29/EC and, in particular, Articles 2 to 6 and Article 8 thereof.

3. This Directive shall not affect:

(a) the Community provisions governing the substantive law on intellectual property, Directive 95/46/EC, Directive 1999/93/EC or Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular;

(b) Member States' international obligations and notably the TRIPS Agreement, including those relating to criminal procedures and penalties;

(c) any national provisions in Member States relating to criminal procedures or penalties in respect of infringement of intellectual property rights.

CHAPTER II MEASURES, PROCEDURES AND REMEDIES

Section 1 General provisions

Article 3 – General obligation

1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.

2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.

Article 4 – Persons entitled to apply for the application of the measures, procedures and remedies

Member States shall recognise as persons entitled to seek application of the measures, procedures and remedies referred to in this chapter:

(a) the holders of intellectual property rights, in accordance with the provisions of the applicable law;

(b) all other persons authorised to use those rights, in particular licensees, in so far as permitted by and in accordance with the provisions of the applicable law;

(c) intellectual property collective rights-management bodies which are regularly recognised as having a right to represent holders of intellectual property rights, in so far as permitted by and in accordance with the provisions of the applicable law;

(d) professional defence bodies which are regularly recognised as having a right to represent holders of intellectual property rights, in so far as permitted by and in accordance with the provisions of the applicable law.

Article 5 – Presumption of authorship or ownership

For the purposes of applying the measures, procedures and remedies provided for in this Directive,

(a) for the author of a literary or artistic work, in the absence of proof to the contrary, to be regarded as such, and consequently to be entitled to institute infringement proceedings, it shall be sufficient for his/her name to appear on the work in the usual manner;

(b) the provision under (a) shall apply mutatis mutandis to the holders of rights related to copyright with regard to their protected subject matter.

Section 2 Evidence

Article 6 – Evidence

1. Member States shall ensure that, on application by a party which has presented reasonably available evidence sufficient to support its claims, and has, in substantiating those claims, specified evidence which lies in the control of the opposing party, the competent judicial authorities may order that such evidence be presented by the opposing party, subject to the protection of confidential information. For the purposes of this paragraph, Member States may provide that a reasonable sample of a substantial number of copies of a work or any other protected object be considered by the competent judicial authorities to constitute reasonable evidence.

2. Under the same conditions, in the case of an infringement committed on a commercial scale Member States shall take such measures as are necessary to enable the competent judicial

authorities to order, where appropriate, on application by a party, the communication of banking, financial or commercial documents under the control of the opposing party, subject to the protection of confidential information.

Article 7 – Measures for preserving evidence

1. Member States shall ensure that, even before the commencement of proceedings on the merits of the case, the competent judicial authorities may, on application by a party who has presented reasonably available evidence to support his/her claims that his/her intellectual property right has been infringed or is about to be infringed, order prompt and effective provisional measures to preserve relevant evidence in respect of the alleged infringement, subject to the protection of confidential information.

Such measures may include the detailed description, with or without the taking of samples, or the physical seizure of the

infringing goods, and, in appropriate cases, the materials and implements used in the production and/or distribution of these goods and the documents relating thereto. Those measures shall be taken, if necessary without the other party having been heard, in particular where any delay is likely to cause irreparable harm to the rightholder or where there is a demonstrable risk of evidence being destroyed.

Where measures to preserve evidence are adopted without the other party having been heard, the parties affected shall be given notice, without delay after the execution of the measures at the

latest. A review, including a right to be heard, shall take place upon request of the parties affected with a view to deciding, within a reasonable period after the notification of the measures, whether

the measures shall be modified, revoked or confirmed.

2. Member States shall ensure that the measures to preserve evidence may be subject to the lodging by the applicant of adequate security or an equivalent assurance intended to ensure

compensation for any prejudice suffered by the defendant as provided for in paragraph 4.

3. Member States shall ensure that the measures to preserve evidence are revoked or otherwise cease to have effect, upon request of the defendant, without prejudice to the damages which may be claimed, if the applicant does not institute, within a reasonable period, proceedings leading to a decision on the merits of the case before the competent judicial authority, the period to be

determined by the judicial authority ordering the measures where the law of a Member State so permits or, in the absence of such determination, within a period not exceeding 20 working days or 31 calendar days, whichever is the longer.

4. Where the measures to preserve evidence are revoked, or where they lapse due to any act or omission by the applicant, or where it is subsequently found that there has been no infringement

or threat of infringement of an intellectual property right, the judicial authorities shall have the authority to order the applicant, upon request of the defendant, to provide the defendant

appropriate compensation for any injury caused by those measures.

5. Member States may take measures to protect witnesses' identity.

Section 3 **Right of information**

Article 8 – Right of information

1. Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided

by the infringer and/or any other person who:

(a) was found in possession of the infringing goods on a commercial scale;

(b) was found to be using the infringing services on a commercial scale;

(c) was found to be providing on a commercial scale services used in infringing activities;

or

(d) was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services.

2. The information referred to in paragraph 1 shall, as appropriate, comprise:

(a) the names and addresses of the producers, manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers;

(b) information on the quantities produced, manufactured, delivered, received or ordered, as well as the price obtained for the goods or services in question.

3. Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which:

(a) grant the rightholder rights to receive fuller information;

(b) govern the use in civil or criminal proceedings of the information communicated pursuant to this Article;

(c) govern responsibility for misuse of the right of information; or

(d) afford an opportunity for refusing to provide information which would force the person referred to in paragraph 1 to admit to his/her own participation or that of his/her close relatives in an infringement of an intellectual property right; or

(e) govern the protection of confidentiality of information sources or the processing of personal data.

Section 4 **Provisional and precautionary measures**

Article 9 – Provisional and precautionary measures

1. Member States shall ensure that the judicial authorities may, at the request of the applicant:

(a) issue against the alleged infringer an interlocutory injunction intended to prevent any imminent infringement of an intellectual property right, or to forbid, on a provisional basis and subject, where appropriate, to a recurring penalty payment where provided for by national law, the continuation of the alleged infringements of that right, or to make such continuation subject to the lodging of guarantees intended to ensure the compensation of the rightholder; an interlocutory injunction may also be issued, under the same conditions, against an intermediary whose services are being used by a third party to infringe an intellectual property right; injunctions against intermediaries whose services are used by a third party to infringe a copyright or a related right are covered by Directive 2001/29/EC;

(b) order the seizure or delivery up of the goods suspected of infringing an intellectual property right so as to prevent their entry into or movement within the channels of commerce.

2. In the case of an infringement committed on a commercial scale, the Member States shall ensure that, if the injured party demonstrates circumstances likely to endanger the recovery of damages, the judicial authorities may order the precautionary seizure of the movable and immovable property of the alleged infringer, including the blocking of his/her bank accounts and other assets. To that end, the competent authorities may order the communication of bank, financial or commercial documents, or appropriate access to the relevant information.

3. The judicial authorities shall, in respect of the measures referred to in paragraphs 1 and 2, have the authority to require the applicant to provide any reasonably available evidence in order to satisfy themselves with a sufficient degree of certainty that the applicant is the rightholder and that the applicant's right is being infringed, or that such infringement is imminent.

4. Member States shall ensure that the provisional measures referred to in paragraphs 1 and 2 may, in appropriate cases, be taken without the defendant having been heard, in particular where any delay would cause irreparable harm to the rightholder. In that event, the parties shall be so informed without delay after the execution of the measures at the latest. A review, including a right to be heard, shall take place upon request of the defendant with a view to deciding, within a reasonable time after notification of the measures, whether those measures shall be modified, revoked or confirmed.

5. Member States shall ensure that the provisional measures referred to in paragraphs 1 and 2 are revoked or otherwise cease to have effect, upon request of the defendant, if the applicant does

not institute, within a reasonable period, proceedings leading to a decision on the merits of the case before the competent judicial authority, the period to be determined by the judicial authority

ordering the measures where the law of a Member State so permits or, in the absence of such determination, within a period not exceeding 20 working days or 31 calendar days, whichever is the longer.

6. The competent judicial authorities may make the provisional measures referred to in paragraphs 1 and 2 subject to the lodging by the applicant of adequate security or an equivalent assurance intended to ensure compensation for any prejudice suffered by the defendant as provided for in paragraph 7.

7. Where the provisional measures are revoked or where they lapse due to any act or omission by the applicant, or where it is subsequently found that there has been no infringement or threat of infringement of an intellectual property right, the judicial authorities shall have the authority to order the applicant, upon request of the defendant, to provide the defendant appropriate

compensation for any injury caused by those measures.

Section 5

Measures resulting from a decision on the merits of the case

Article 10 – Corrective measures

1. Without prejudice to any damages due to the rightholder by reason of the infringement, and without compensation of any sort, Member States shall ensure that the competent judicial authorities may order, at the request of the applicant, that appropriate measures be taken with regard to goods that they have found to be infringing an intellectual property right and, in appropriate cases, with regard to materials and implements principally used in the creation or manufacture of those goods. Such measures shall include:

- (a) recall from the channels of commerce;
- (b) definitive removal from the channels of commerce;
- or
- (c) destruction.

2. The judicial authorities shall order that those measures be carried out at the expense of the infringer, unless particular reasons are invoked for not doing so.

3. In considering a request for corrective measures, the need for proportionality between the seriousness of the infringement and the remedies ordered as well as the interests of third parties shall be taken into account.

Article 11 - Injunctions

Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction

aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a

third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC.

Article 12 – Alternative measures

Member States may provide that, in appropriate cases and at the request of the person liable to be subject to the measures provided for in this section, the competent judicial authorities may order

pecuniary compensation to be paid to the injured party instead of applying the measures provided for in this section if that person acted unintentionally and without negligence, if execution of the

measures in question would cause him/her disproportionate harm and if pecuniary compensation to the injured party appears reasonably satisfactory.

Section 6

Damages and legal costs

Article 13 – Damages

1. Member States shall ensure that the competent judicial authorities, on application of the injured party, order the infringer who knowingly, or with reasonable grounds to know, engaged in an infringing activity, to pay the rightholder damages appropriate to the actual prejudice suffered by him/her as a result of the infringement.

When the judicial authorities set the damages:

(a) they shall take into account all appropriate aspects, such as the negative economic consequences, including lost profits, which the injured party has suffered, any unfair profits made by the infringer and, in appropriate cases, elements other than economic factors, such as the moral prejudice caused to the rightholder by the infringement;

or

(b) as an alternative to (a), they may, in appropriate cases, set the damages as a lump sum on the basis of elements such as at least the amount of royalties or fees which would have been due if the infringer had requested authorisation to use the intellectual property right in question.

2. Where the infringer did not knowingly, or with reasonable grounds know, engage in infringing activity, Member States may lay down that the judicial authorities may order the recovery of profits or the payment of damages, which may be pre-established.

Article 14 – Legal costs

Member States shall ensure that reasonable and proportionate legal costs and other expenses incurred by the successful party shall, as a general rule, be borne by the unsuccessful party, unless equity does not allow this.

Section 7

Publicity measures

Article 15 – Publication of judicial decisions

Member States shall ensure that, in legal proceedings instituted for infringement of an intellectual property right, the judicial authorities may order, at the request of the applicant and at the expense of the infringer, appropriate measures for the dissemination of the information concerning the decision, including displaying the decision and publishing it in full or in part. Member States may provide for other additional publicity measures which are appropriate to the particular circumstances, including prominent advertising.

CHAPTER III

SANCTIONS BY MEMBER STATES

Article 16 – Sanctions by Member States

Without prejudice to the civil and administrative measures, procedures and remedies laid down by this Directive, Member States may apply other appropriate sanctions in cases where intellectual property rights have been infringed.

CHAPTER IV

CODES OF CONDUCT AND ADMINISTRATIVE COOPERATION

Article 17 – Codes of conduct

Member States shall encourage:

(a) the development by trade or professional associations or organisations of codes of conduct at Community level aimed at contributing towards the enforcement of the intellectual property rights, particularly by recommending the use on optical discs of a code enabling the identification of the origin of their manufacture;

(b) the submission to the Commission of draft codes of conduct at national and Community level and of any evaluations of the application of these codes of conduct.

Article 18 – Assessment

1. Three years after the date laid down in Article 20(1), each Member State shall submit to the Commission a report on the implementation of this Directive. On the basis of those reports, the Commission shall draw up a report on the application of this Directive, including an assessment of the effectiveness of the measures taken, as well as an evaluation of its impact on innovation and the development of the information society. That report shall then be transmitted to the European Parliament, the Council and the European Economic and Social Committee. It shall be accompanied, if necessary and in the light of developments in the Community legal order, by proposals for amendments to this Directive.
2. Member States shall provide the Commission with all the aid and assistance it may need when drawing up the report referred to in the second subparagraph of paragraph 1.

Article 19 – Exchange of information and correspondents

For the purpose of promoting cooperation, including the exchange of information, among Member States and between Member States and the Commission, each Member State shall designate one or more national correspondents for any question relating to the implementation of the measures provided for by this Directive. It shall communicate the details of the national correspondent(s) to the other Member States and to the Commission.

CHAPTER V FINAL PROVISIONS

Article 20 – Implementation

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive by 29 April 2006. They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the texts of the provisions of national law which they adopt in the field governed by this Directive.

Article 21 – Entry into force

This Directive shall enter into force on the 20th day following that of its publication in the Official Journal of the European Union.

[...]

Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof, Having regard to the proposal from the Commission, Having regard to the opinion of the European Economic and Social Committee [1],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [2],

Whereas:

(1) Council Directive 93/98/EEC of 29 October 1993 harmonising the term of protection of copyright and certain related rights [3] has been substantially amended [4]. In the interests of clarity and rationality the said Directive should be codified.

(2) The Berne Convention for the protection of literary and artistic works and the International Convention for the protection of performers, producers of phonograms and broadcasting organisations (Rome Convention) lay down only minimum terms of protection of the rights they refer to, leaving the Contracting States free to grant longer terms. Certain Member States have exercised this entitlement. In addition, some Member States have not yet become party to the Rome Convention.

(3) There are consequently differences between the national laws governing the terms of protection of copyright and related rights, which are liable to impede the free movement of goods and freedom to provide services and to distort competition in the common market. Therefore, with a view to the smooth operation of the internal market, the laws of the Member States should be harmonised so as to make terms of protection identical throughout the Community.

(4) It is important to lay down not only the terms of protection as such, but also certain implementing arrangements, such as the date from which each term of protection is calculated.

(5) The provisions of this Directive should not affect the application by the Member States of the provisions of Article 14 bis (2)(b), (c) and (d) and (3) of the Berne Convention.

(6) The minimum term of protection laid down by the Berne Convention, namely the life of the author and 50 years after his death, was intended to provide protection for the author and the first two generations of his descendants. The average lifespan in the Community has grown longer, to the point where this term is no longer sufficient to cover two generations.

(7) Certain Member States have granted a term longer than 50 years after the death of the author in order to offset the effects of the world wars on the exploitation of authors' works.

(8) For the protection of related rights certain Member States have introduced a term of 50 years after lawful publication or lawful communication to the public.

(9) The Diplomatic Conference held in December 1996, under the auspices of the World Intellectual Property Organization (WIPO), led to the adoption of the WIPO Performances and Phonograms Treaty, which deals with the protection of performers and producers of phonograms. This Treaty took the form of a substantial up-date of the international protection of related rights.

(10) Due regard for established rights is one of the general principles of law protected by the Community legal order. Therefore, the terms of protection of copyright and related rights established by Community law cannot have the effect of reducing the protection enjoyed by rightholders in the Community before the entry into force of Directive 93/98/EEC. In order to keep the effects of transitional measures to a minimum and to allow the internal market to function smoothly, those terms of protection should be applied for long periods.

(11) The level of protection of copyright and related rights should be high, since those rights are fundamental to intellectual creation. Their protection ensures the maintenance

and development of creativity in the interest of authors, cultural industries, consumers and society as a whole.

(12) In order to establish a high level of protection which at the same time meets the requirements of the internal market and the need to establish a legal environment conducive to the harmonious development of literary and artistic creation in the Community, the term of protection for copyright should be harmonised at 70 years after the death of the author or 70 years after the work is lawfully made available to the public, and for related rights at 50 years after the event which sets the term running.

(13) Collections are protected according to Article 2(5) of the Berne Convention when, by reason of the selection and arrangement of their content, they constitute intellectual creations. Those works are protected as such, without prejudice to the copyright in each of the works forming part of such collections. Consequently, specific terms of protection may apply to works included in collections.

(14) In all cases where one or more physical persons are identified as authors, the term of protection should be calculated after their death. The question of authorship of the whole or a part of a work is a question of fact which the national courts may have to decide.

(15) Terms of protection should be calculated from the first day of January of the year following the relevant event, as they are in the Berne and Rome Conventions.

(16) The protection of photographs in the Member States is the subject of varying regimes. A photographic work within the meaning of the Berne Convention is to be considered original if it is the author's own intellectual creation reflecting his personality, no other criteria such as merit or purpose being taken into account. The protection of other photographs should be left to national law.

(17) In order to avoid differences in the term of protection as regards related rights it is necessary to provide the same starting point for the calculation of the term throughout the Community. The performance, fixation, transmission, lawful publication, and lawful communication to the public, that is to say the means of making a subject of a related right perceptible in all appropriate ways to persons in general, should be taken into account for the calculation of the term of protection regardless of the country where this performance, fixation, transmission, lawful publication, or lawful communication to the public takes place.

(18) The rights of broadcasting organisations in their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite, should not be perpetual. It is therefore necessary to have the term of protection running from the first transmission of a particular broadcast only. This provision is understood to avoid a new term running in cases where a broadcast is identical to a previous one.

(19) The Member States should remain free to maintain or introduce other rights related to copyright in particular in relation to the protection of critical and scientific publications. In order to ensure transparency at Community level, it is however necessary for Member States which introduce new related rights to notify the Commission.

(20) It should be made clear that this Directive does not apply to moral rights.

(21) For works whose country of origin within the meaning of the Berne Convention is a third country and whose author is not a Community national, comparison of terms of protection should be applied, provided that the term accorded in the Community does not exceed the term laid down in this Directive.

(22) Where a rightholder who is not a Community national qualifies for protection under an international agreement, the term of protection of related rights should be the same as that laid down in this Directive. However, this term should not exceed that fixed in the third country of which the rightholder is a national.

(23) Comparison of terms should not result in Member States being brought into conflict with their international obligations.

(24) Member States should remain free to adopt provisions on the interpretation, adaptation and further execution of contracts on the exploitation of protected works and other subject matter which were concluded before the extension of the term of protection resulting from this Directive.

(25) Respect of acquired rights and legitimate expectations is part of the Community legal order. Member States may provide in particular that in certain circumstances the copyright and related rights which are revived pursuant to this Directive may not give rise to payments by persons who undertook in good faith the exploitation of the works at the time when such works lay within the public domain.

(26) This Directive should be without prejudice to the obligations of the Member States relating to the time-limits for transposition into national law and application of the Directives, as set out in Part B of Annex I,
HAVE ADOPTED THIS DIRECTIVE:

Article 1

Duration of authors' rights

1. The rights of an author of a literary or artistic work within the meaning of Article 2 of the Berne Convention shall run for the life of the author and for 70 years after his death, irrespective of the date when the work is lawfully made available to the public.

2. In the case of a work of joint authorship, the term referred to in paragraph 1 shall be calculated from the death of the last surviving author.

3. In the case of anonymous or pseudonymous works, the term of protection shall run for 70 years after the work is lawfully made available to the public. However, when the pseudonym adopted by the author leaves no doubt as to his identity, or if the author discloses his identity during the period referred to in the first sentence, the term of protection applicable shall be that laid down in paragraph 1.

4. Where a Member State provides for particular provisions on copyright in respect of collective works or for a legal person to be designated as the rightholder, the term of protection shall be calculated according to the provisions of paragraph 3, except if the natural persons who have created the work are identified as such in the versions of the work which are made available to the public. This paragraph is without prejudice to the rights of identified authors whose identifiable contributions are included in such works, to which contributions paragraph 1 or 2 shall apply.

5. Where a work is published in volumes, parts, instalments, issues or episodes and the term of protection runs from the time when the work was lawfully made available to the public, the term of protection shall run for each such item separately.

6. In the case of works for which the term of protection is not calculated from the death of the author or authors and which have not been lawfully made available to the public within 70 years from their creation, the protection shall terminate.

7. The term of protection of a musical composition with words shall expire 70 years after the death of the last of the following persons to survive, whether or not those persons are designated as co-authors: the author of the lyrics and the composer of the musical composition, provided that both contributions were specifically created for the respective musical composition with words.

Article 2

Cinematographic or audiovisual works

1. The principal director of a cinematographic or audiovisual work shall be considered as its author or one of its authors. Member States shall be free to designate other co-authors.

2. The term of protection of cinematographic or audiovisual works shall expire 70 years after the death of the last of the following persons to survive, whether or not these persons are designated as co-authors: the principal director, the author of the screenplay, the author of the dialogue and the composer of music specifically created for use in the cinematographic or audiovisual work.

Article 3 **Duration of related rights**

1. The rights of performers shall expire 50 years after the date of the performance. However, if a fixation of the performance is lawfully published or lawfully communicated to the public within this period, the rights shall expire 50 years from the date of the first such publication or the first such communication to the public, whichever is the earlier.

However,

— if a fixation of the performance otherwise than in a phonogram is lawfully published or lawfully communicated to the public within this period, the rights shall expire 50 years from the date of the first such publication or the first such communication to the public, whichever is the earlier,

— if a fixation of the performance in a phonogram is lawfully published or lawfully communicated to the public within this period, the rights shall expire 70 years from the date of the first such publication or the first such communication to the public, whichever is the earlier.

2. The rights of producers of phonograms shall expire 50 years after the fixation is made. However, if the phonogram has been lawfully published within this period, the said rights shall expire 70 years from the date of the first lawful publication. If no lawful publication has taken place within the period mentioned in the first sentence, and if the phonogram has been lawfully communicated to the public within this period, the said rights shall expire 70 years from the date of the first lawful communication to the public.

2. However, this paragraph shall not have the effect of protecting anew the rights of producers of phonograms where, through the expiry of the term of protection granted them pursuant to Article 3(2) of Directive 93/98/EEC in its version before amendment by Directive 2001/29/EEC, they were no longer protected on 22 December 2002.

2a. If, 50 years after the phonogram was lawfully published or, failing such publication, 50 years after it was lawfully communicated to the public, the phonogram producer does not offer copies of the phonogram for sale in sufficient quantity or does not make it available to the public, by wire or wireless means, in such a way that members of the public may access it from a place and at a time individually chosen by them, the performer may terminate the contract by which the performer has transferred or assigned his rights in the fixation of his performance to a phonogram producer (hereinafter a 'contract on transfer or assignment'). The right to terminate the contract on transfer or assignment may be exercised if the producer, within a year from the notification by the performer of his intention to terminate the contract on transfer or assignment pursuant to the previous sentence, fails to carry out both of the acts of exploitation referred to in that sentence. This right to terminate may not be waived by the performer. Where a phonogram contains the fixation of the performances of a plurality of performers, they may terminate their contracts on transfer or assignment in accordance with applicable national law. If the contract on transfer or assignment is terminated pursuant to this paragraph, the rights of the phonogram producer in the phonogram shall expire.

2b. Where a contract on transfer or assignment gives the performer a right to claim a non-recurring remuneration, the performer shall have the right to obtain an annual supplementary remuneration from the phonogram producer for each full year immediately following the 50th year after the phonogram was lawfully published or, failing such publication, the 50th year after it was lawfully communicated to the public. The right to obtain such annual supplementary remuneration may not be waived by the performer.

2c. The overall amount to be set aside by a phonogram producer for payment of the annual supplementary remuneration referred to in paragraph 2b shall correspond to 20 % of the revenue which the phonogram producer has derived, during the year preceding that for which the said remuneration is paid, from the reproduction, distribution and making available of the phonogram in question, following the 50th year after it was lawfully published or, failing such

publication, the 50th year after it was lawfully communicated to the public.

Member States shall ensure that phonogram producers are required on request to provide to performers who are entitled to the annual supplementary remuneration referred to in paragraph 2b any information which may be necessary in order to secure payment of that remuneration.

2d. Member States shall ensure that the right to obtain an annual supplementary remuneration as referred to in paragraph 2b is administered by collecting societies.

2e. Where a performer is entitled to recurring payments, neither advance payments nor any contractually defined deductions shall be deducted from the payments made to the performer following the 50th year after the phonogram was lawfully published or, failing such publication, the 50th year after it was lawfully communicated to the public.

3. The rights of producers of the first fixation of a film shall expire 50 years after the fixation is made. However, if the film is lawfully published or lawfully communicated to the public during this period, the rights shall expire 50 years from the date of the first such publication or the first such communication to the public, whichever is the earlier. The term 'film' shall designate a cinematographic or audiovisual work or moving images, whether or not accompanied by sound.

4. The rights of broadcasting organisations shall expire 50 years after the first transmission of a broadcast, whether this broadcast is transmitted by wire or over the air, including by cable or satellite.

Article 4

Protection of previously unpublished works

Any person who, after the expiry of copyright protection, for the first time lawfully publishes or lawfully communicates to the public a previously unpublished work, shall benefit from a protection equivalent to the economic rights of the author. The term of protection of such rights shall be 25 years from the time when the work was first lawfully published or lawfully communicated to the public.

Article 5

Critical and scientific publications

Member States may protect critical and scientific publications of works which have come into the public domain. The maximum term of protection of such rights shall be 30 years from the time when the publication was first lawfully published.

Article 6

Protection of photographs

Photographs which are original in the sense that they are the author's own intellectual creation shall be protected in accordance with Article 1. No other criteria shall be applied to determine their eligibility for protection. Member States may provide for the protection of other photographs.

Article 7

Protection vis-à-vis third countries

1. Where the country of origin of a work, within the meaning of the Berne Convention, is a third country, and the author of the work is not a Community national, the term of protection granted by the Member States shall expire on the date of expiry of the protection granted in the country of origin of the work, but may not exceed the term laid down in Article 1.

2. The terms of protection laid down in Article 3 shall also apply in the case of rightholders who are not Community nationals, provided Member States grant them protection. However, without prejudice to the international obligations of the Member States, the term of protection granted by Member States shall expire no later than the date of expiry of the protection granted in the country of which the rightholder is a national and may not exceed the term laid down in Article 3.

3. Member States which, on 29 October 1993, in particular pursuant to their international obligations, granted a longer term of protection than that which would result from the

provisions of paragraphs 1 and 2 may maintain this protection until the conclusion of international agreements on the term of protection of copyright or related rights.

Article 8

Calculation of terms

The terms laid down in this Directive shall be calculated from the first day of January of the year following the event which gives rise to them.

Article 9

Moral rights

This Directive shall be without prejudice to the provisions of the Member States regulating moral rights.

Article 10

Application in time

1. Where a term of protection which is longer than the corresponding term provided for by this Directive was already running in a Member State on 1 July 1995, this Directive shall not have the effect of shortening that term of protection in that Member State.
2. The terms of protection provided for in this Directive shall apply to all works and subject matter which were protected in at least one Member State on the date referred to in paragraph 1, pursuant to national provisions on copyright or related rights, or which meet the criteria for protection under [Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property] (5).
3. This Directive shall be without prejudice to any acts of exploitation performed before the date referred to in paragraph 1. Member States shall adopt the necessary provisions to protect in particular acquired rights of third parties.
4. Member States need not apply the provisions of Article 2(1) to cinematographic or audiovisual works created before 1 July 1994.
5. Article 3(1) to (2e) in the version thereof in force on 31 October 2011 shall apply to fixations of performances and phonograms in regard to which the performer and the phonogram producer are still protected, by virtue of those provisions in the version thereof in force on 30 October 2011, as at 1 November 2013 and to fixations of performances and phonograms which come into being after that date.

6. Article 1(7) shall apply to musical compositions with words of which at least the musical composition or the lyrics are protected in at least one Member State on 1 November 2013, and to musical compositions with words which come into being after that date.

The first subparagraph of this paragraph shall be without prejudice to any acts of exploitation performed before 1 November 2013. Member States shall adopt the necessary provisions to protect, in particular, acquired rights of third parties.

Article 10a

Transitional measures

1. In the absence of clear contractual indications to the contrary, a contract on transfer or assignment concluded before 1 November 2013 shall be deemed to continue to produce its effects beyond the moment at which, by virtue of Article 3(1) in the version thereof in force on 30 October 2011, the performer would no longer be protected.
2. Member States may provide that contracts on transfer or assignment which entitle a performer to recurring payments and which are concluded before 1 November 2013 can be modified following the 50th year after the phonogram was lawfully published or, failing such publication, the 50th year after it was lawfully communicated to the public.

Article 11

Notification and communication

1. Member States shall immediately notify the Commission of any governmental plan to grant new related rights, including the basic reasons for their introduction and the term of protection envisaged.
 2. Member States shall communicate to the Commission the texts of the provisions of internal law which they adopt in the field governed by this Directive.
- [...]

Article 13

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

on.

VIII. Electronic documents

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Having regard to the opinion of the Committee of the Regions (3),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (4),

Whereas:

(1) On 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce;

(2) On 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on ensuring security and trust in electronic communication — towards a European framework for digital signatures and encryption;***(3) On 1 December 1997 the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures;***(4) Electronic communication and commerce necessitate ' electronic signatures' and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;***(5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods (5) and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use

goods (6);***(6)***This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;***(7)***The internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect;***(8)***Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;***(9)***Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;***(10)***The internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;***(11)***Voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;***(12)***Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services;***(13)***Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-

providers to apply to be supervised under any applicable accreditation scheme;**(14)**It is important to strike a balance between consumer and business needs;**(15)**Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient;**(16)**This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;**(17)**This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;**(18)**The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;**(19)**Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;**(20)**Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of hand-written signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to hand-written signatures only if the requirements for hand-written signatures are fulfilled;**(21)**In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;**(22)**Certification-service-providers providing certification-services to the public are subject to national rules regarding liability;**(23)**The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;**(24)**In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;**(25)**Provisions on the use of pseudonyms in

certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;**(26)**The measures necessary for the implementation of this Directive are to be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (7);**(27)**Two years after its implementation the Commission will carry out a review of this Directive so as, inter alia, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;**(28)**In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community; this Directive does not go beyond what is necessary to achieve that objective,

HAVE ADOPTED THIS DIRECTIVE:

Article 1 Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market. It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2 Definitions

For the purpose of this Directive:

1. 'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
2. 'advanced electronic signature' means an electronic signature which meets the following requirements:
 - (a) it is uniquely linked to the signatory;
 - (b) it is capable of identifying the signatory;
 - (c) it is created using means that the signatory can maintain under his sole control; and
 - (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
3. 'signatory' means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;
4. 'signature-creation data' means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
5. 'signature-creation device' means configured software or hardware used to implement the signature-creation data;
6. 'secure-signature-creation device' means a signature-creation device which meets the requirements laid down in Annex III;
7. 'signature-verification-data' means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;
8. 'signature-verification device' means configured software or hardware used to implement the signature-verification-data;
9. 'certificate' means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;
10. 'qualified certificate' means a certificate which meets the requirements laid down in Annex I and is provided by a

certification-service-provider who fulfils the requirements laid down in Annex II;

11. 'certification-service-provider' means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;

12. 'electronic-signature product' means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;

13. 'voluntary accreditation' means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Article 3

Market access

1. Member States shall not make the provision of certification services subject to prior authorisation.

2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.

3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.

4. ►M1 The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall establish criteria for Member States to determine whether a body should be so designated. That measure, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 9(3). ◀

A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.

5. The Commission may, in accordance with the procedure laid down ►M1 in Article 9(2) ◀, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.

7. Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

Article 4

Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.

2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market.

Article 5

Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

— in electronic form, or

— not based upon a qualified certificate, or

— not based upon a qualified certificate issued by an accredited certification-service-provider, or

— not created by a secure signature-creation device.

Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate; (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

1. unless the certification-service-provider proves that he has not acted negligently.

2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.

The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (8).

Article 7

International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:

(a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or

(b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or

(c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.

3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.

Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

Article 8

Data protection

1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (9).

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

▼M1

Article 9

Committee procedure

1. The Commission shall be assisted by the Electronic-Signature Committee.

2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

The period provided for in Article 4(3) of Decision 1999/468/EC shall be set at three months.

3. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

▼B

Article 10

Tasks of the committee

The committee shall clarify the requirements laid down in the Annexes of this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9(2).

Article 11

Notification

1. Member States shall notify to the Commission and the other Member States the following:

(a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);

(b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);

(c) the names and addresses of all accredited national certification service providers.

2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

Article 12

Review

1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest.

2. The review shall inter alia assess whether the scope of this Directive should be modified, taking account of technological, market and legal developments. The report shall in particular include an assessment, on the basis of experience gained, of aspects of harmonisation. The report shall be accompanied, where appropriate, by legislative proposals.

Article 13

Implementation

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive before 19 July 2001. They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

Article 14

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 15

Addressees

This Directive is addressed to the Member States.

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

- (a) an indication that the certificate is issued as a qualified certificate;
- (b) the identification of the certification-service-provider and the State in which it is established;
- (c) the name of the signatory or a pseudonym, which shall be identified as such;
- (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- (e) signature-verification data which correspond to signature-creation data under the control of the signatory;
- (f) an indication of the beginning and end of the period of validity of the certificate;
- (g) the identity code of the certificate;
- (h) the advanced electronic signature of the certification-service-provider issuing it;
- (i) limitations on the scope of use of the certificate, if applicable; and
- (j) limits on the value of transactions for which the certificate can be used, if applicable.

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

- (a) demonstrate the reliability necessary for providing certification services;
- (b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
- (c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
- (d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
- (e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
- (f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
- (g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
- (h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
- (i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
- (j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
- (k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the

certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

ANNEX III

Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

- (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
 - (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
 - (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

ANNEX IV

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:

- (a) the data used for verifying the signature correspond to the data displayed to the verifier;
- (b) the signature is reliably verified and the result of that verification is correctly displayed;
- (c) the verifier can, as necessary, reliably establish the contents of the signed data;
- (d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
- (e) the result of verification and the signatory's identity are correctly displayed;
- (f) the use of a pseudonym is clearly indicated; and
- (g) any security-relevant changes can be detected.

(1) OJ C 325, 23.10.1998, p. 5.

(2) OJ C 40, 15.2.1999, p. 29.

(3) OJ C 93, 6.4.1999, p. 33.

(4) Opinion of the European Parliament of 13 January 1999 (OJ C 104, 14.4.1999, p. 49), Council Common Position of 28 June 1999 (OJ C 243, 27.8.1999, p. 33) and Decision of the European Parliament of 27 October 1999 (not yet published in the Official Journal). Council Decision of 30 November 1999.

(5) OJ L 367, 31.12.1994, p. 1. Regulation as amended by Regulation (EC) No 837/95 (OJ L 90, 21.4.1995, p. 1).

(6) OJ L 367, 31.12.1994, p. 8. Decision as last amended by Decision 99/193/CFSP (OJ L 73, 19.3.1999, p. 1).

(7) OJ L 184, 17.7.1999, p. 23.

(8) OJ L 95, 21.4.1993, p. 29.

(9) OJ L 281, 23.11.1995, p. 31.

Amended by:

		Official Journal		
		No	page	date
►M1	<u>Regulation (EC) No 1137/2008 of the European Parliament and of the Council of 22 October 2008</u>	L 311	1	21.11.2008

Regulation (EU) No 910/2014 Of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

(2) This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

(3) Directive 1999/93/EC of the European Parliament and of the Council (3), dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the acquis of that Directive.

(4) The Commission communication of 26 August 2010 entitled 'A Digital Agenda for Europe' identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its EU Citizenship Report 2010, entitled 'Dismantling the obstacles to EU citizens' rights', the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services.

(5) In its conclusions of 4 February 2011 and of 23 October 2011, the European Council invited the Commission to create a digital single market by 2015, to make rapid progress in key areas of the digital economy and to promote a fully integrated

digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

(6) In its conclusions of 27 May 2011, the Council invited the Commission to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable e-government services across the European Union.

(7) The European Parliament, in its resolution of 21 September 2010 on completing the internal market for e-commerce (4), stressed the importance of the security of electronic services, especially of electronic signatures, and of the need to create a public key infrastructure at pan-European level, and called on the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet.

(8) Directive 2006/123/EC of the European Parliament and of the Council (5) requires Member States to establish 'points of single contact' (PSCs) to ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof can be easily completed, at a distance and by electronic means, through the appropriate PSC with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.

(9) In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States. That electronic barrier excludes service providers from enjoying the full benefits of the internal market. Mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.

(10) Directive 2011/24/EU of the European Parliament and of the Council (6) set up a network of national authorities responsible for e-health. To enhance the safety and the continuity of cross-border healthcare, the network is required to produce guidelines on cross-border access to electronic health data and services, including by supporting 'common identification and authentication measures to facilitate transferability of data in cross-border healthcare'. Mutual recognition of electronic identification and authentication is

key to making cross-border healthcare for European citizens a reality. When people travel for treatment, their medical data need to be accessible in the country of treatment. That requires a solid, safe and trusted electronic identification framework.

(11) This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council (7). In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.

(12) One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services. This Regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States. The aim of this Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible.

(13) Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means. Member States should not be obliged to notify their electronic identification schemes to the Commission. The choice to notify the Commission of all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services is up to Member States.

(14) Some conditions need to be set out in this Regulation with regard to which electronic identification means have to be recognised and how the electronic identification schemes should be notified. Those conditions should help Member States to build the necessary trust in each other's electronic identification schemes and to mutually recognise electronic identification means falling under their notified schemes. The principle of mutual recognition should apply if the notifying Member State's electronic identification scheme meets the conditions of notification and the notification was published in the Official Journal of the European Union. However, the principle of mutual recognition should only relate to authentication for an online service. The access to those online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set out in national legislation.

(15) The obligation to recognise electronic identification means should relate only to those means the identity assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. In addition, that obligation should only apply when the public sector body in question uses the assurance level 'substantial' or 'high' in relation to accessing that service online. Member States should remain free, in accordance with Union law, to recognise electronic identification means having lower identity assurance levels.

(16) Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing

electronic identification means and the procedure to issue such means) and technical controls implemented. Various technical definitions and descriptions of assurance levels exist as the result of Union-funded Large-Scale Pilots, standardisation and international activities. In particular, the Large-Scale Pilot STORK and ISO 29115 refer, inter alia, to levels 2, 3 and 4, which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurance levels low, substantial and high within the meaning of this Regulation, while ensuring consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for issuing qualified certificates. The requirements established should be technology-neutral. It should be possible to achieve the necessary security requirements through different technologies.

(17) Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions. The possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member States at least for public services and to make it easier for businesses and citizens to access their online services across borders. In order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by any Member State should be available to private sector relying parties established outside of the territory of that Member State under the same conditions as applied to private sector relying parties established within that Member State. Consequently, with regard to private sector relying parties, the notifying Member State may define terms of access to the authentication means. Such terms of access may inform whether the authentication means related to the notified scheme is presently available to private sector relying parties. (18) This Regulation should provide for the liability of the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure for failure to comply with the relevant obligations under this Regulation. However, this Regulation should be applied in accordance with national rules on liability. Therefore, it does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof.

(19) The security of electronic identification schemes is key to trustworthy cross-border mutual recognition of electronic identification means. In this context, Member States should cooperate with regard to the security and interoperability of the electronic identification schemes at Union level. Whenever electronic identification schemes require specific hardware or software to be used by relying parties at the national level, cross-border interoperability calls for those Member States not to impose such requirements and related costs on relying parties established outside of their territory. In that case appropriate solutions should be discussed and developed within the scope of the interoperability framework. Nevertheless technical requirements stemming from the inherent specifications of national electronic identification means and likely to affect the holders of such electronic means (e.g. smartcards), are unavoidable.

(20) Cooperation by Member States should facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering a high level of trust and security appropriate to the degree of risk. The exchange of information and the sharing of best practices between Member States with a view to their mutual recognition should help such cooperation.

(21) This Regulation should also establish a general legal framework for the use of trust services. However, it should not create a general obligation to use them or to install an access point for all existing trust services. In particular, it should not cover the provision of services used exclusively within closed

systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation. Neither should this Regulation cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.

(22) In order to contribute to their general cross-border use, it should be possible to use trust services as evidence in legal proceedings in all Member States. It is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation.

(23) To the extent that this Regulation creates an obligation to recognise a trust service, such a trust service may only be rejected if the addressee of the obligation is unable to read or verify it due to technical reasons lying outside the immediate control of the addressee. However, that obligation should not in itself require a public body to obtain the hardware and software necessary for the technical readability of all existing trust services.

(24) Member States may maintain or introduce national provisions, in conformity with Union law, relating to trust services as far as those services are not fully harmonised by this Regulation. However, trust services that comply with this Regulation should circulate freely in the internal market.

(25) Member States should remain free to define other types of trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services.

(26) Because of the pace of technological change, this Regulation should adopt an approach which is open to innovation.

(27) This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.

(28) To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider should be introduced with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust services and products are used or provided.

(29) In line with the obligations under the United Nations Convention on the Rights of Persons with Disabilities, approved by Council Decision 2010/48/EC (8), in particular Article 9 of the Convention, persons with disabilities should be able to use trust services and end-user products used in the provision of those services on an equal basis with other consumers. Therefore, where feasible, trust services provided and end-user products used in the provision of those services should be made accessible for persons with disabilities. The feasibility assessment should include, inter alia, technical and economic considerations.

(30) Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation. Member States should also be able to decide, upon a mutual agreement with another Member State, to designate a supervisory body in the territory of that other Member State.

(31) Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached. The provision of information should in particular cover security incidents and personal data breaches.

(32) It should be incumbent on all trust service providers to apply good security practice appropriate to the risks related to their activities so as to boost users' trust in the single market.

(33) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Union or national law.

(34) All Member States should follow common essential supervision requirements to ensure a comparable security level of qualified trust services. To ease the consistent application of those requirements across the Union, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field.

(35) All trust service providers should be subject to the requirements of this Regulation, in particular those on security and liability to ensure due diligence, transparency and accountability of their operations and services. However, taking into account the type of services provided by trust service providers, it is appropriate to distinguish as far as those requirements are concerned between qualified and non-qualified trust service providers.

(36) Establishing a supervisory regime for all trust service providers should ensure a level playing field for the security and accountability of their operations and services, thus contributing to the protection of users and to the functioning of the internal market. Non-qualified trust service providers should be subject to a light touch and reactive ex post supervisory activities justified by the nature of their services and operations. The supervisory body should therefore have no general obligation to supervise non-qualified service providers. The supervisory body should only take action when it is informed (for example, by the non-qualified trust service provider itself, by another supervisory body, by a notification from a user or a business partner or on the basis of its own investigation) that a non-qualified trust service provider does not comply with the requirements of this Regulation.

(37) This Regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.

(38) Notification of security breaches and security risk assessments is essential with a view to providing adequate information to concerned parties in the event of a breach of security or loss of integrity.

(39) To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA).

(40) To enable the Commission and the Member States to assess the effectiveness of the enhanced supervision mechanism introduced by this Regulation, supervisory bodies should be requested to report on their activities. This would be instrumental in facilitating the exchange of good practice

between supervisory bodies and would ensure the verification of the consistent and efficient implementation of the essential supervision requirements in all Member States.

(41) To ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should verify the existence and the correct application of provisions on termination plans in cases where qualified trust service providers cease their activities.

(42) To facilitate the supervision of qualified trust service providers, for example, when a provider is providing its services in the territory of another Member State and is not subject to supervision there, or when the computers of a provider are located in the territory of a Member State other than the one where it is established, a mutual assistance system between supervisory bodies in the Member States should be established.

(43) In order to ensure the compliance of qualified trust service providers and the services they provide with the requirements set out in this Regulation, a conformity assessment should be carried out by a conformity assessment body and the resulting conformity assessment reports should be submitted by the qualified trust service providers to the supervisory body. Whenever the supervisory body requires a qualified trust service provider to submit an ad hoc conformity assessment report, the supervisory body should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Therefore, the supervisory body should duly justify its decision to require an ad hoc conformity assessment.

(44) This Regulation aims to ensure a coherent framework with a view to providing a high level of security and legal certainty of trust services. In this regard, when addressing the conformity assessment of products and services, the Commission should, where appropriate, seek synergies with existing relevant European and international schemes such as the Regulation (EC) No 765/2008 of the European Parliament and of the Council (9) which sets out the requirements for accreditation of conformity assessment bodies and market surveillance of products.

(45) In order to allow an efficient initiation process, which should lead to the inclusion of qualified trust service providers and the qualified trust services they provide into trusted lists, preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with a view to facilitating the due diligence leading to the provisioning of qualified trust services.

(46) Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision.

(47) Confidence in and convenience of online services are essential for users to fully benefit and consciously rely on electronic services. To this end, an EU trust mark should be created to identify the qualified trust services provided by qualified trust service providers. Such an EU trust mark for qualified trust services would clearly differentiate qualified trust services from other trust services thus contributing to transparency in the market. The use of an EU trust mark by qualified trust service providers should be voluntary and should not lead to any requirement other than those provided for in this Regulation.

(48) While a high level of security is needed to ensure mutual recognition of electronic signatures, in specific cases, such as in the context of Commission Decision 2009/767/EC (10), electronic signatures with a lower security assurance should also be accepted.

(49) This Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided

for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature.

(50) As competent authorities in the Member States currently use different formats of advanced electronic signatures to sign their documents electronically, it is necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically. Similarly, when competent authorities in the Member States use advanced electronic seals, it would be necessary to ensure that they support at least a number of advanced electronic seal formats.

(51) It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.

(52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.

(53) The suspension of qualified certificates is an established operational practice of trust service providers in a number of Member States, which is different from revocation and entails the temporary loss of validity of a certificate. Legal certainty calls for the suspension status of a certificate to always be clearly indicated. To that end, trust service providers should have the responsibility to clearly indicate the status of the certificate and, if suspended, the precise period of time during which the certificate has been suspended. This Regulation should not impose the use of suspension on trust service providers or Member States, but should provide for transparency rules when and where such a practice is available.

(54) Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in qualified certificates should be allowed, provided that such specific attributes do not hamper cross-border interoperability and recognition of qualified certificates and electronic signatures.

(55) IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organisational solutions for qualified electronic signature creation devices for which security standards may not yet be available or for which the first IT security certification is ongoing. The level of security of such qualified electronic signature creation devices could be evaluated by using alternative processes only where such security standards are not available or where the first IT security certification is ongoing. Those processes should be comparable to the standards for IT security certification

insofar as their security levels are equivalent. Those processes could be facilitated by a peer review.

(56) This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications.

(57) To ensure legal certainty as regards the validity of the signature, it is essential to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation. Moreover, specifying the requirements for qualified trust service providers that can provide a qualified validation service to relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves, should stimulate the private and public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level.

(58) When a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable.

(59) Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.

(60) Trust service providers issuing qualified certificates for electronic seals should implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided, when such identification is necessary at national level in the context of judicial or administrative proceedings.

(61) This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

(62) In order to ensure the security of qualified electronic time stamps, this Regulation should require the use of an advanced electronic seal or an advanced electronic signature or of other equivalent methods. It is foreseeable that innovation may lead to new technologies that may ensure an equivalent level of security for time stamps. Whenever a method other than an advanced electronic seal or an advanced electronic signature is used, it should be up to the qualified trust service provider to demonstrate, in the conformity assessment report, that such a method ensures an equivalent level of security and complies with the obligations set out in this Regulation.

(63) Electronic documents are important for further development of cross-border electronic transactions in the internal market. This Regulation should establish the principle that an electronic document should not be denied legal effect on the grounds that it is in an electronic form in order to ensure that an electronic transaction will not be rejected only on the grounds that a document is in electronic form.

(64) When addressing formats of advanced electronic signatures and seals, the Commission should build on existing practices, standards and legislation, in particular Commission Decision 2011/130/EU (11).

(65) In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.

(66) It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal

systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new pan-European electronic registered delivery services.

(67) Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum — CA/B Forum, have been taken into account. In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a third country provider should only have its website authentication services recognised as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded.

(68) The concept of 'legal persons', according to the provisions of the Treaty on the Functioning of the European Union (TFEU) on establishment, leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, 'legal persons', within the meaning of the TFEU, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.

(69) The Union institutions, bodies, offices and agencies are encouraged to recognise electronic identification and trust services covered by this Regulation for the purpose of administrative cooperation capitalising, in particular, on existing good practices and the results of ongoing projects in the areas covered by this Regulation.

(70) In order to complement certain detailed technical aspects of this Regulation in a flexible and rapid manner, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of criteria to be met by the bodies responsible for the certification of qualified electronic signature creation devices. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(71) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards the use of which would raise a presumption of compliance with certain requirements laid down in this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (12).

(72) When adopting delegated or implementing acts, the Commission should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services.

(73) For reasons of legal certainty and clarity, Directive 1999/93/EC should be repealed.

(74) To ensure legal certainty for market operators already using qualified certificates issued to natural persons in compliance with Directive 1999/93/EC, it is necessary to provide for a sufficient period of time for transitional purposes. Similarly, transitional measures should be established for secure signature creation devices, the conformity of which has been determined in accordance with Directive 1999/93/EC, as well as for certification service providers issuing qualified certificates before 1 July 2016. Finally, it is also necessary to provide the Commission with the means to adopt the implementing acts and delegated acts before that date.

(75) The application dates set out in this Regulation do not affect existing obligations that Member States already have under Union law, in particular under Directive 2006/123/EC.

(76) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the scale of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(77) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council (13) and delivered an opinion on 27 September 2012 (14),

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:

(a) lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;

(b) lays down rules for trust services, in particular for electronic transactions; and

(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

Article 2

Scope

1. This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union.

2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.

3. This Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

(2) 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

(3) 'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

(4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;

(5) 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;

(6) 'relying party' means a natural or legal person that relies upon an electronic identification or a trust service;

(7) 'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;

(8) 'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council (15);

(9) 'signatory' means a natural person who creates an electronic signature;

(10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

(11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;

(12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

(13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;

(14) 'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

(15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;

(16) 'trust service' means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;

(17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;

(18) 'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;

(19) 'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

(20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

(21) 'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;

(22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;

(23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;

(24) 'creator of a seal' means a legal person who creates an electronic seal;

(25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

(26) 'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;

(27) 'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;

(28) 'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;

(29) 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;

(30) 'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;

(31) 'electronic seal creation device' means configured software or hardware used to create an electronic seal;

(32) 'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;

(33) 'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

(34) 'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42;

(35) 'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;

(36) 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

(37) 'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44;

(38) 'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;

(39) 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

(40) 'validation data' means data that is used to validate an electronic signature or an electronic seal;

(41) 'validation' means the process of verifying and confirming that an electronic signature or a seal is valid.

Article 4

Internal market principle

1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.

2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.

Article 5

Data processing and protection

1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.

2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.

CHAPTER II

ELECTRONIC IDENTIFICATION

Article 6

Mutual recognition

1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:

(a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;

(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;

(c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online. Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.

Article 7

Eligibility for notification of electronic identification schemes

An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:

(a) the electronic identification means under the electronic identification scheme are issued:

(i) by the notifying Member State;

(ii) under a mandate from the notifying Member State; or

(iii) independently of the notifying Member State and are recognised by that Member State;

(b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State;

(c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);

(d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant

assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;

(e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);

(f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.

For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body.

Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;

(g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(7);

(h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).

Article 8

Assurance levels of electronic identification schemes

1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.

2. The assurance levels low, substantial and high shall meet respectively the following criteria:

(a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;

(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;

(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and

high are specified for electronic identification means for the purposes of paragraph 1.

Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements:

(a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

(b) the procedure for the issuance of the requested electronic identification means;

(c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;

(d) the entity issuing the electronic identification means;

(e) any other body involved in the application for the issuance of the electronic identification means; and

(f) the technical and security specifications of the issued electronic identification means.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 9

Notification

1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto:

(a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;

(b) the applicable supervisory regime and information on the liability regime with respect to the following:

(i) the party issuing the electronic identification means; and

(ii) the party operating the authentication procedure;

(c) the authority or authorities responsible for the electronic identification scheme;

(d) information on the entity or entities which manage the registration of the unique person identification data;

(e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;

(f) a description of the authentication referred to in point (f) of Article 7;

(g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

2. One year from the date of application of the implementing acts referred to in Articles 8(3) and 12(8), the Commission shall publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification.

4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the Member State's request.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 10

Security breach

1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in

point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.

2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.

3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.

The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 9(2) without undue delay.

Article 11 Liability

1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.

2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.

3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.

4. Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.

5. Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.

Article 12 Cooperation and interoperability

1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable.

2. For the purposes of paragraph 1, an interoperability framework shall be established.

3. The interoperability framework shall meet the following criteria:

(a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;

(b) it follows European and international standards, where possible;

(c) it facilitates the implementation of the principle of privacy by design; and

(d) it ensures that personal data is processed in accordance with Directive 95/46/EC.

4. The interoperability framework shall consist of:

(a) a reference to minimum technical requirements related to the assurance levels under Article 8;

(b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;

(c) a reference to minimum technical requirements for interoperability;

(d) a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes;

(e) rules of procedure;

(f) arrangements for dispute resolution; and

(g) common operational security standards.

5. Member States shall cooperate with regard to the following:

(a) the interoperability of the electronic identification schemes notified pursuant to Article 9(1) and the electronic identification schemes which Member States intend to notify; and

(b) the security of the electronic identification schemes.

6. The cooperation between Member States shall consist of:

(a) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability and assurance levels;

(b) the exchange of information, experience and good practice as regards working with assurance levels of electronic identification schemes under Article 8;

(c) peer review of electronic identification schemes falling under this Regulation; and

(d) examination of relevant developments in the electronic identification sector.

7. By 18 March 2015, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraphs 5 and 6 with a view to fostering a high level of trust and security appropriate to the degree of risk.

8. By 18 September 2015, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4.

9. The implementing acts referred to in paragraphs 7 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER III TRUST SERVICES

SECTION 1 General provisions

Article 13 Liability and burden of proof

1. Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.

The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.

The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.

2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

3. Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.

Article 14 International aspects

1. Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified

trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU.

2. Agreements referred to in paragraph 1 shall ensure, in particular, that:

- (a) the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide;
- (b) the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded.

Article 15

Accessibility for persons with disabilities

Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

Article 16

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive.

SECTION 2

Supervision

Article 17

Supervisory body

1. Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That body shall be responsible for supervisory tasks in the designating Member State.

Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.

2. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.

3. The role of the supervisory body shall be the following:

(a) to supervise qualified trust service providers established in the territory of the designating Member State to ensure, through ex ante and ex post supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;

(b) to take action if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, through ex post supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.

4. For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular:

- (a) to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;
- (b) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);
- (c) to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);
- (d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;

(e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);

(f) to cooperate with the data protection authorities, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached;

(g) to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;

(h) to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the supervisory body;

(i) to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2);

(j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.

5. Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.

6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2).

7. The Commission shall make the annual report referred to in paragraph 6 available to Member States.

8. The Commission may, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 18

Mutual assistance

1. Supervisory bodies shall cooperate with a view to exchanging good practice.

A supervisory body shall, upon receipt of a justified request from another supervisory body, provide that body with assistance so that the activities of supervisory bodies can be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21.

2. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds:

- (a) the supervisory body is not competent to provide the requested assistance;
- (b) the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Article 17;
- (c) providing the requested assistance would be incompatible with this Regulation.

3. Where appropriate, Member States may authorise their respective supervisory bodies to carry out joint investigations in which staff from other Member States' supervisory bodies is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.

Article 19

Security requirements applicable to trust service providers

1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of

security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

4. The Commission may, by means of implementing acts:
(a) further specify the measures referred to in paragraph 1; and
(b) define the formats and procedures, including deadlines, applicable for the purpose of paragraph 2.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 3

Qualified trust services

Article 20

Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.

3. Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

4. The Commission may, by means of implementing acts, establish reference number of the following standards:

(a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;
(b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 21

Initiation of a qualified trust service

1. Where trust service providers, without qualified status, intend to start providing qualified trust services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body.

2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.

3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).

4. The Commission may, by means of implementing acts, define the formats and procedures for the purpose of paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 22

Trusted lists

1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.

4. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.

5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 23

EU trust mark for qualified trust services

1. After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide.
2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.
3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 24

Requirements for qualified trust service providers

1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued. The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:
 - (a) by the physical presence of the natural person or of an authorised representative of the legal person; or
 - (b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or
 - (c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or
 - (d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.
2. A qualified trust service provider providing qualified trust services shall:
 - (a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;
 - (b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;
 - (c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;
 - (d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;
 - (e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;
 - (f) use trustworthy systems to store data provided to it, in a verifiable form so that:

- (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,
 - (ii) only authorised persons can make entries and changes to the stored data,
 - (iii) the data can be checked for authenticity;
- (g) take appropriate measures against forgery and theft of data;
 - (h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;
 - (i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);
 - (j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;
 - (k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.
3. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.
 4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.
 5. The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of this Article. Compliance with the requirements laid down in this Article shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 4

Electronic signatures

Article 25

Legal effects of electronic signatures

1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.
2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.
3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.

Article 26

Requirements for advanced electronic signatures

- An advanced electronic signature shall meet the following requirements:
- (a) it is uniquely linked to the signatory;
 - (b) it is capable of identifying the signatory;
 - (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Article 27

Electronic signatures in public services

1. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.

2. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.

3. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature.

4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 shall be presumed when an advanced electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 28

Qualified certificates for electronic signatures

1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.

2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.

3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.

4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:

(a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;

(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in

accordance with the examination procedure referred to in Article 48(2).

Article 29

Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 30

Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.

2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.

3. The certification referred to in paragraph 1 shall be based on one of the following:

(a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or

(b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.

Article 31

Publication of a list of certified qualified electronic signature creation devices

1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified.

2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.

3. The Commission may, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 32
Requirements for the validation of qualified electronic signatures

1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:

- (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;
- (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
- (c) the signature validation data corresponds to the data provided to the relying party;
- (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
- (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
- (f) the electronic signature was created by a qualified electronic signature creation device;
- (g) the integrity of the signed data has not been compromised;
- (h) the requirements provided for in Article 26 were met at the time of signing.

2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of qualified electronic signatures meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 33
Qualified validation service for qualified electronic signatures

1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:

- (a) provides validation in compliance with Article 32(1); and
- (b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation service for a qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 34
Qualified preservation service for qualified electronic signatures

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet those standards. Those implementing acts shall be adopted in

accordance with the examination procedure referred to in Article 48(2).

SECTION 5
Electronic seals

Article 35
Legal effects of electronic seals

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.

2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.

Article 36
Requirements for advanced electronic seals

An advanced electronic seal shall meet the following requirements:

- (a) it is uniquely linked to the creator of the seal;
- (b) it is capable of identifying the creator of the seal;
- (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and
- (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

Article 37
Electronic seals in public services

1. If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.

2. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.

3. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal.

4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Compliance with the requirements for advanced electronic seals referred to in paragraphs 1 and 2 of this Article and Article 36 shall be presumed when an advanced electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 38
Qualified certificates for electronic seals

1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.
2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.
3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.
4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.
5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:
 - (a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension;
 - (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.
6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 39

Qualified electronic seal creation devices

1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.
2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.
3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.

Article 40

Validation and preservation of qualified electronic seals

Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.

SECTION 6

Electronic time stamps

Article 41

Legal effect of electronic time stamps

1. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.
2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.
3. A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.

Article 42

Requirements for qualified electronic time stamps

1. A qualified electronic time stamp shall meet the following requirements:
 - (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

(b) it is based on an accurate time source linked to Coordinated Universal Time; and

(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 7

Electronic registered delivery services

Article 43

Legal effect of an electronic registered delivery service

1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.

2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

Article 44

Requirements for qualified electronic registered delivery services

1. Qualified electronic registered delivery services shall meet the following requirements:

(a) they are provided by one or more qualified trust service provider(s);

(b) they ensure with a high level of confidence the identification of the sender;

(c) they ensure the identification of the addressee before the delivery of the data;

(d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;

(e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;

(f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 8

Website authentication

Article 45

Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER IV ELECTRONIC DOCUMENTS

Article 46 Legal effects of electronic documents

An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

CHAPTER V DELEGATIONS OF POWER AND IMPLEMENTING PROVISIONS

Article 47 Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.
3. The delegation of power referred to in Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 48 Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER VI FINAL PROVISIONS

Article 49 Review

The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, including

Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments.

The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals.

In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.

Article 50 Repeal

1. Directive 1999/93/EC is repealed with effect from 1 July 2016.
2. References to the repealed Directive shall be construed as references to this Regulation.

Article 51 Transitional measures

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation.
2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire.
3. A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, that certification-service-provider shall be considered as qualified trust service provider under this Regulation.
4. If a certification-service-provider issuing qualified certificates under Directive 1999/93/EC does not submit a conformity assessment report to the supervisory body within the time limit referred to in paragraph 3, that certification-service-provider shall not be considered as qualified trust service provider under this Regulation from 2 July 2017.

Article 52 Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. This Regulation shall apply from 1 July 2016, except for the following:
 - (a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014;
 - (b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8);
 - (c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8).
3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.
4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means

under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 23 July 2014.

For the Parliament
The President
M. SCHULZ

For the Council
The President
S. GOZI

- (1) OJ C 351, 15.11.2012, p. 73.
- (2) Position of the European Parliament of 3 April 2014 (not yet published in the Official Journal) and decision of the Council of 23 July 2014.
- (3) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).
- (4) OJ C 50 E, 21.2.2012, p. 1.
- (5) Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36).
- (6) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).
- (7) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
- (8) Council Decision 2010/48/EC of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities (OJ L 23, 27.1.2010, p. 35).
- (9) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).
- (10) Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 274, 20.10.2009, p. 36).
- (11) Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 53, 26.2.2011, p. 66).
- (12) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).
- (13) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).
- (14) OJ C 28, 30.1.2013, p. 6.
- (15) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

ANNEX I REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURES

Qualified certificates for electronic signatures shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;
- (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:
 -
 - for a legal person: the name and, where applicable, registration number as stated in the official records,
 -
 - for a natural person: the person's name;
- (c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;
- (d) electronic signature validation data that corresponds to the electronic signature creation data;
- (e) details of the beginning and end of the certificate's period of validity;
- (f) the certificate identity code, which must be unique for the qualified trust service provider;
- (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
- (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
- (i) the location of the services that can be used to enquire about the validity status of the qualified certificate;
- (j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX II REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
 - (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
 - (b) the electronic signature creation data used for electronic signature creation can practically occur only once;
 - (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
 - (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.
2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.
3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.
4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:
 - (a) the security of the duplicated datasets must be at the same level as for the original datasets;
 - (b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

ANNEX III

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS

Qualified certificates for electronic seals shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;
- (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:

—
for a legal person: the name and, where applicable, registration number as stated in the official records,

—
for a natural person: the person's name;

- (c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;

- (d) electronic seal validation data, which corresponds to the electronic seal creation data;

- (e) details of the beginning and end of the certificate's period of validity;

- (f) the certificate identity code, which must be unique for the qualified trust service provider;

- (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

- (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;

- (i) the location of the services that can be used to enquire as to the validity status of the qualified certificate;

- (j) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.

- (j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.

ANNEX IV REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION

Qualified certificates for website authentication shall contain:

- (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;

- (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:

—
for a legal person: the name and, where applicable, registration number as stated in the official records,

—
for a natural person: the person's name;

- (c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated;

- for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;

- (d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;

- (e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;

- (f) details of the beginning and end of the certificate's period of validity;

- (g) the certificate identity code, which must be unique for the qualified trust service provider;

- (h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

- (i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;

IX. Data protection

Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14

[...]

Article 5 – Right to liberty and security

1. Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law:
 - a. the lawful detention of a person after conviction by a competent court;
 - b. the lawful arrest or detention of a person for non-compliance with the lawful order of a court or in order to secure the fulfilment of any obligation prescribed by law;
 - c. the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so;
 - d. the detention of a minor by lawful order for the purpose of educational supervision or his lawful detention for the purpose of bringing him before the competent legal authority;
 - e. the lawful detention of persons for the prevention of the spreading of infectious diseases, of persons of unsound mind, alcoholics or drug addicts or vagrants;
 - f. the lawful arrest or detention of a person to prevent his effecting an unauthorised entry into the country or of a person against whom action is being taken with a view to deportation or extradition.
2. Everyone who is arrested shall be informed promptly, in a language which he understands, of the reasons for his arrest and of any charge against him.
3. Everyone arrested or detained in accordance with the provisions of paragraph 1.c of this article shall be brought promptly before a judge or other officer authorised by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial. Release may be conditioned by guarantees to appear for trial.
4. Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful.
5. Everyone who has been the victim of arrest or detention in contravention of the provisions of this article shall have an enforceable right to compensation.

Article 6 – Right to a fair trial

6. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special

circumstances where publicity would prejudice the interests of justice.

7. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
8. Everyone charged with a criminal offence has the following minimum rights:
 - a. to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
 - b. to have adequate time and facilities for the preparation of his defence;
 - c. to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
 - d. to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
 - e. to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 9 – Freedom of thought, conscience and religion

1. Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance.
2. Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others.

Article 10 – Freedom of expression

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities,

conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[...]

Article 13 – Right to an effective remedy

Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

Charter of Fundamental Rights of the European Union (2007/C 303/01)

[...]

Article 3 Right to the integrity of the person

1. Everyone has the right to respect for his or her physical and mental integrity.
2. In the fields of medicine and biology, the following must be respected in particular:

- (a) the free and informed consent of the person concerned, according to the procedures laid down by law;
- (b) the prohibition of eugenic practices, in particular those aiming at the selection of persons;
- (c) the prohibition on making the human body and its parts as such a source of financial gain;
- (d) the prohibition of the reproductive cloning of human beings.

[...]

Article 6 Right to liberty and security

Everyone has the right to liberty and security of person.

Article 7 Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Article 9

Right to marry and right to found a family

The right to marry and the right to found a family shall be guaranteed in accordance with the national laws governing the exercise of these rights.

Article 10 Freedom of thought, conscience and religion

1. Everyone has the right to freedom of thought, conscience and religion. This right includes freedom to change religion or belief and freedom, either alone or in community with others and in public or in private, to manifest religion or belief, in worship, teaching, practice and observance.

2. The right to conscientious objection is recognised, in accordance with the national laws governing the exercise of this right.

Article 11 Freedom of expression and information

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
2. The freedom and pluralism of the media shall be respected.

[...]

Article 47 Right to an effective remedy and to a fair trial

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

[...]

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Strasbourg, 28.I.1981

Preamble

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

Chapter I – General provisions

Article 1 – Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2 – Definitions

For the purposes of this convention:

"personal data" means any information relating to an identified or identifiable individual ("data subject");

"automated data file" means any set of data undergoing automatic processing;

"automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

"controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3 – Scope

The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

that it will not apply this convention to certain categories of automated personal data files, a list of which will be

deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;

that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

that it will also apply this convention to personal data files which are not processed automatically.

Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this convention to such categories by a Party which has not excluded them.

Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

Chapter II – Basic principles for data protection

Article 4 – Duties of the Parties

Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5 – Quality of data

Personal data undergoing automatic processing shall be: obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 – Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7 – Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8 – Additional safeguards for the data subject

Any person shall be enabled:

to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9 – Exceptions and restrictions

No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of: protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; protecting the data subject or the rights and freedoms of others.

Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10 – Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11 – Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

Chapter III – Transborder data flows

Article 12 – Transborder flows of personal data and domestic law

The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

insofar as its legislation includes specific Regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the Regulations of the other Party provide an equivalent protection;

when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

Chapter IV – Mutual assistance

Article 13 – Co-operation between Parties

The Parties agree to render each other mutual assistance in order to implement this convention.

For that purpose:

each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;

each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.

An authority designated by a Party shall at the request of an authority designated by another Party:

furnish information on its law and administrative practice in the field of data protection;

take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14 – Assistance to data subjects resident abroad

Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

The request for assistance shall contain all the necessary particulars, relating *inter alia* to:

the name, address and any other relevant particulars identifying the person making the request;

the automated personal data file to which the request pertains, or its controller;

the purpose of the request.

Article 15 – Safeguards concerning assistance rendered by designated authorities

An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for

purposes other than those specified in the request for assistance.

Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16 – Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless:

the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;

the request does not comply with the provisions of this convention;

compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17 – Costs and procedures of assistance

Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.

Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

Chapter V – Consultative Committee

Article 18 – Composition of the committee

A Consultative Committee shall be set up after the entry into force of this convention.

Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.

The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19 – Functions of the committee

The Consultative Committee:
may make proposals with a view to facilitating or improving the application of the convention;

may make proposals for amendment of this convention in accordance with Article 21;

shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3;

may, at the request of a Party, express an opinion on any question concerning the application of this convention.

Article 20 – Procedure

The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.

A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.

After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention. Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

Chapter VI – Amendments

Article 21 – Amendments

Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.

Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.

Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Chapter VII – Final clauses

Article 22 – Entry into force

This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

Article 23 – Accession by non-member States

After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 24 – Territorial clause

Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25 – Reservations

No reservation may be made in respect of the provisions of this convention.

Article 26 – Denunciation

Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.

Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27 – Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of:

any signature;
the deposit of any instrument of ratification, acceptance, approval or accession;
any date of entry into force of this convention in accordance with Articles 22, 23 and 24;
any other act, notification or communication relating to this convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

Relevant Case-Law on Convention for the Protection of Human Rights and Fundamental Freedoms

- ***CASE OF KLASS AND OTHERS v. GERMANY (Application no. 5029/71) 6 September 1978***
- ***CASE OF MALONE v. THE UNITED KINGDOM (Application no. 8691/79) 2 August 1984***
- ***CASE OF NIEMIETZ v. GERMANY (Application no. 13710/88) 16 December 1992***
- ***CASE OF ROTARU v. ROMANIA (Application no. 28341/95) 4 May 2000***
- ***COPLAND v. THE UNITED KINGDOM (Application no. 62617/00) 3 April 2007***

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,
Having regard to the proposal from the Commission (1),
Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1)

Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2)

Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3)

Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4)

Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5)

Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6)

Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7)

Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, Regulations and administrative provisions;

(8)

Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9)

Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10)

Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11)

Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12)

Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13)

Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14)

Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15)

Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16)

Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17)

Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18)

Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19)

Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20)

Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21)

Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22)

Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23)

Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24)

Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25)

Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26)

Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27)

Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28)

Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29)

Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30)

Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31)

Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32)

Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33)

Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34)

Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35)

Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36)

Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37)

Whereas the processing of personal data for purposes of journalism or for purposes of literary or artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38)

Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39)

Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40)

Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41)

Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42)

Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict

rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43)

Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or Regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44)

Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45)

Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46)

Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47)

Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48)

Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49)

Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights

and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50)

Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51)

Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52)

Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53)

Whereas, however, certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54)

Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55)

Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(56)

Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57)

Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58)

Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or

where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59)

Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60)

Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61)

Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62)

Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63)

Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64)

Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65)

Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66)

Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (4);

(67)

Whereas an agreement on a *modus vivendi* between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68)

Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69)

Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70)

Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71)

Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such Regulation does not concern the protection of individuals with regard to the processing of personal data;

(72)

Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are

determined by national or Community laws or Regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3 Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

— in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

— by a natural person in the course of a purely personal or household activity.

Article 4 National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

— the recipients or categories of recipients of the data,

— whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

— the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

— the categories of data concerned,

— the recipients or categories of recipients,

— the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

— confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

— communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

— knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
- (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
- (g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

- (a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;
- (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

- (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
- (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or

partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.
2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

— where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

— where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

— for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

— for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

— thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or Regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

- (a) the name and address of the controller and of his representative, if any;
- (b) the purpose or purposes of the processing;
- (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
- (d) the recipients or categories of recipient to whom the data might be disclosed;
- (e) proposed transfers of data to third countries;
- (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define

the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or Regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III

JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions

adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or Regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding

rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V

CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority. Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI

SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or Regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

— investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

— effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

— the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

[...]

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

(2) OJ No C 159, 17. 6. 1991, p 38.

(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(4) OJ No L 197, 18. 7. 1987, p. 33.

(5) Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ L 184, 17.7.1999, p. 23).

Amended by:

		Official Journal		
		No	page	date
►M1	Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003	L 284	1	31.10.2003

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Having consulted the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

(1)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2)

This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(3)

Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

(4)

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the

telecommunications sector (5) translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector. Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5)

New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

(6)

The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7)

In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

(8)

Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in

order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.

(9)

The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

(10)

In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.

(11)

Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(12)

Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.

(13)

The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided. Prepaid cards are also considered as a contract.

(14)

Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

(15)

A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission.

Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

(16)

Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However, in cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive.

(17)

For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.

(18)

Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.

(19)

The application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges should not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort. It is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission.

(20)

Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.

(21)

Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to

communications.

(22)

The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

(23)

Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

(24)

Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

(25)

However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

(26)

The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of

natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

(27)

The exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided. For instance for a voice telephony call the transmission will be completed as soon as either of the users terminates the connection. For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.

(28)

The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services.

(29)

The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service.

(30)

Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required.

(31)

Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.

(32)

Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out

in Directive 95/46/EC. Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.

(33)

The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card. To the same end, Member States may ask the operators to offer their subscribers a different type of detailed bill in which a certain number of digits of the called number have been deleted.

(34)

It is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. There is justification for overriding the elimination of calling line identification presentation in specific cases. Certain subscribers, in particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available electronic communications service.

(35)

In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.

(36)

Member States may restrict the users' and subscribers' rights to privacy with regard to calling line identification where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services to carry out their tasks as effectively as possible. For these purposes, Member States may adopt specific provisions to entitle providers of electronic communications services to provide access to calling line identification and location data without the prior consent of the users or subscribers concerned.

(37)

Safeguards should be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others. Moreover, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available electronic communications service.

(38)

Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

(39)

The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.

(40)

Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(41)

Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(42)

Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43)

To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44)

Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.

(45)

This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) (6) are fully applicable.

(46)

The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (7) will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.

(47)

Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

(48)

It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.

(49)

To facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope and aim

1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.
2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.
3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 2

Definitions

Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (8) shall apply.

The following definitions shall also apply:

- (a) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;
- (b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
- (c) 'location data' means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;
- (d) 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;
- (f) 'consent' by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;
- (g) 'value added service' means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;
- (h) 'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient;
- (i) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.

Article 3

Services concerned

This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic

communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.

Article 4 Security of processing

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,
- ensure the implementation of a security policy with respect to the processing of personal data,

1a. Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

3. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

3. Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

3. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

3. The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied

with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so.

4. Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.

5. In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article.

5. Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).

Article 5 Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Article 6 Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such

processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 7

Itemised billing

1. Subscribers shall have the right to receive non-itemised bills.
2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

Article 8

Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications

services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9

Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Article 10

Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

Article 11

Automatic call forwarding

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

Article 12

Directories of subscribers

1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through

directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 13

Unsolicited communications

1. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.

4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member

States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.

Article 14

Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and Regulations and of rules on information society services (9).

3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications (10).

Article 14a

Committee procedure

1. The Commission shall be assisted by the Communications Committee established by Article 22 of Directive 2002/21/EC (Framework Directive).

2. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph, Article 5a(1), (2), (4) and (6) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

Article 15

Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

1b. Providers shall establish internal procedures for responding to requests for access to users' personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector. Article 15a
Implementation and enforcement

1. Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by 25 May 2011, and shall notify it without delay of any subsequent amendment affecting them.

2. Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.

3. Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.

4. The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows.

4. The national regulatory authorities shall provide the Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the measures.

Article 16 Transitional arrangements

1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.

2. Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search

functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.

Article 17 Transposition

1. Before 31 October 2003 Member States shall bring into force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 18 Review

The Commission shall submit to the European Parliament and the Council, not later than three years after the date referred to in Article 17(1), a report on the application of this Directive and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, taking into account the international environment. [...]

Article 19 Repeal

Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1). References made to the repealed Directive shall be construed as being made to this Directive.

Article 20 Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

[...]

(1) OJ C 365 E, 19.12.2000, p. 223.

(2) OJ C 123, 25.4.2001, p. 53.

(3) Opinion of the European Parliament of 13 November 2001 (not yet published in the Official Journal), Council Common Position of 28 January 2002 (OJ C 113 E, 14.5.2002, p. 39) and Decision of the European Parliament of 30 May 2002 (not yet published in the Official Journal). Council Decision of 25 June 2002.

(4) OJ L 281, 23.11.1995, p. 31.

(5) OJ L 24, 30.1.1998, p. 1.

(6) OJ L 178, 17.7.2000, p. 1.

(7) OJ L 91, 7.4.1999, p. 10.

(8) OJ L 108, 24.4.2002, p. 33.

(9) OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

(10) OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

(11) OJ L 105, 13.4.2006, p. 54.

Amended by:

	No	page	date
► M1	<u>Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006</u>	L 105 54	13.4.2006
► M2	<u>Directive 2009/136/EC of the European Parliament and of the Council Text with EEA relevance of 25 November 2009</u>	L 337 11	18.12.2009

Relevant Case Law on the Directives 95/46/EC; 2002/58/EC

C-101/01 Criminal proceedings against Bodil Lindqvist

[...]

The main proceedings and the questions referred

[...]

(1) Is the mention of a person — by name or with name and telephone number — on an internet home page an action which falls within the scope of [Directive 95/46]? Does it constitute the processing of personal data wholly or partly by automatic means to list on a self-made internet home page a number of persons with comments and statements about their jobs and hobbies etc.?

(2) If the answer to the first question is no, can the act of setting up on an internet home page separate pages for about 15 people with links between the pages which make it possible to search by first name be considered to constitute the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system within the meaning of Article 3(1)?

If the answer to either of those questions is yes, the hovrätt also asks the following questions:

(3) Can the act of loading information of the type described about work colleagues onto a private home page which is none the less accessible to anyone who knows its address be regarded as outside the scope of [Directive 95/46] on the ground that it is covered by one of the exceptions in Article 3(2)?

(4) Is information on a home page stating that a named colleague has injured her foot and is on half-time on medical grounds personal data concerning health which, according to Article 8(1), may not be processed?

(5) [Directive 95/46] prohibits the transfer of personal data to third countries in certain cases. If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden — with the result that personal data become accessible to people in third countries — does that constitute a transfer of data to a third country within the meaning of the Directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?

(6) Can the provisions of [Directive 95/46], in a case such as the above, be regarded as bringing about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the EU and are enshrined in inter alia Article 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms?

Finally, the hovrätt asks the following question:

(7) Can a Member State, as regards the issues raised in the above questions, provide more extensive protection for personal data or give it a wider scope than the Directive, even if none of the circumstances described in Article 13 exists?

[...]

[...]

On those grounds,

THE COURT,

in answer to the questions referred to it by the Göta hovrätt by order of 23 February 2001, hereby rules:

1. The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2. Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46.

3. Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.

4. There is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.

5. The provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order.

6. Measures taken by the Member States to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it.

[...]

**C-275/06 Productores de Música de España (Promusicae) v
Telefónica de España SAU**

[...]

'Does Community law, specifically Articles 15(2) and 18 of Directive [2000/31], Article 8(1) and (2) of Directive [2001/29], Article 8 of Directive [2004/48] and Articles 17(2) and 47 of the Charter ... permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service?'

[...]

On those grounds, the Court (Grand Chamber) hereby rules:

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, Community law requires that, when transposing those Directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those Directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those Directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

[...]

**C-557/07 LSG-Gesellschaft zur Wahrnehmung von
Leistungsschutzrechten GmbH v Tele2 Telecommunication
GmbH**

[...]

'(1) Is the term "intermediary" in Article 5(1)(a) and Article 8(3) of Directive [2001/29] to be interpreted as including an access provider who merely provides a user with access to the network by allocating him a dynamic IP address but does not himself provide him with any services such as email, FTP or file-sharing services and does not exercise any control, whether *de iure* or *de facto*, over the services which the user makes use of?

(2) If the first question is answered in the affirmative: Is Article 8(3) of Directive [2004/48], regard being had to Article 6 and Article 15 of Directive [2002/58], to be interpreted (restrictively) as not permitting the disclosure of

personal traffic data to private third parties for the purposes of civil proceedings for alleged infringements of exclusive rights protected by copyright (rights of exploitation and use)?'

[...]

On those grounds, the Court (Eighth Chamber) hereby rules:

1. Community law – in particular, Article 8(3) of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, read in conjunction with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) – does not preclude Member States from imposing an obligation to disclose to private third parties personal data relating to Internet traffic in order to enable them to bring civil proceedings for copyright infringements. Community law nevertheless requires Member States to ensure that, when transposing into national law Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, and Directives 2002/58 and 2004/48, they rely on an interpretation of those Directives which allows a fair balance to be struck between the various fundamental rights involved. Moreover, when applying the measures transposing those Directives, the authorities and courts of Member States must not only interpret their national law in a manner consistent with those Directives but must also make sure that they do not rely on an interpretation of those Directives which would conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

2. Access providers which merely provide users with Internet access, without offering other services such as email, FTP or file-sharing services or exercising any control, whether *de iure* or *de facto*, over the services which users make use of, must be regarded as 'intermediaries' within the meaning of Article 8(3) of Directive 2001/29.

[...]

**C-461/10 Bonnier Audio AB et al. v Perfect Communication
Sweden AB**

[...]

'1. Does [Directive 2006/24], and in particular Articles 3 [to] 5 and 11 thereof, preclude the application of a national provision which is based on Article 8 of [Directive 2004/48] and which permits an internet service provider in civil proceedings, in order to identify a particular subscriber, to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided a specific IP address, which address, it is claimed, was used in the infringement? The question is based on the assumption that the applicant has adduced clear evidence of the infringement of a particular copyright and that the measure is proportionate.

2. Is the answer to Question 1 affected by the fact that the Member State has not implemented [Directive 2006/24] despite the fact that the period prescribed for implementation has expired?'

[...]

On those grounds, the Court (Third Chamber) hereby rules:

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC must be interpreted as not precluding the application of national legislation based on Article 8 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights which, in order to identify an internet subscriber or user, permits an internet service provider in civil proceedings to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided an IP address which was allegedly used in an infringement, since that legislation does not fall within the material scope of Directive 2006/24.

It is irrelevant to the main proceedings that the Member State concerned has not yet transposed Directive 2006/24, despite the period for doing so having expired.

Directives 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and 2004/48 must be interpreted as not precluding national legislation such as that at issue in the main proceedings insofar as that legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality.

[...]

Joined Cases C-293/12 and C-594/12, (Digital Rights Ireland Ltd, Kärntner Landesregierung)

[...]

C-293/12

[...]

‘1. Is the restriction on the rights of the [p]laintiff in respect of its use of mobile telephony arising from the requirements of Articles 3, 4 ... and 6 of Directive 2006/24/EC incompatible with [Article 5(4)] TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims of: (a) Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime? and/or

b) Ensuring the proper functioning of the internal market of the European Union?

2. Specifically,

(i) Is Directive 2006/24 compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TFEU?

(ii) Is Directive 2006/24 compatible with the right to privacy laid down in Article 7 of the [Charter of Fundamental Rights of the European Union (“the Charter”)] and Article 8 ECHR?

(iii) Is Directive 2006/24 compatible with the right to the protection of personal data laid down in Article 8 of the Charter?

(iv) Is Directive 2006/24 compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?

(v) Is Directive 2006/24 compatible with the right to [g]ood [a]dministration laid down in Article 41 of the Charter?

3. To what extent do the Treaties — and specifically the principle of loyal cooperation laid down in [Article 4(3) TEU] — require a national court to inquire into, and assess, the compatibility of the national implementing measures for [Directive 2006/24] with the protections afforded by the

[Charter], including Article 7 thereof (as informed by Article 8 of the ECHR)?’

Case C-594/12

[...]

‘1. Concerning the validity of acts of institutions of the European Union:

Are Articles 3 to 9 of [Directive 2006/24] compatible with Articles 7, 8 and 11 of the [Charter]?’

2. Concerning the interpretation of the Treaties:

(a) In the light of the explanations relating to Article 8 of the Charter, which, according to Article 52(7) of the Charter, were drawn up as a way of providing guidance in the interpretation of the Charter and to which regard must be given by the Verfassungsgerichtshof, must [Directive 95/46] and Regulation (EC) No 45/2001 of the European Parliament and of the Council [of 18 December 2000] on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [O] 2001 L 8, p. 1] be taken into account, for the purposes of assessing the permissibility of interference, as being of equal standing to the conditions under Article 8(2) and Article 52(1) of the Charter?

(b) What is the relationship between “Union law”, as referred to in the final sentence of Article 52(3) of the Charter, and the Directives in the field of the law on data protection?

(c) In view of the fact that [Directive 95/26] and Regulation ... No 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments resulting from subsequent secondary law be taken into account for the purpose of interpreting Article 8 of the Charter?

(d) Having regard to Article 52(4) of the Charter, does it follow from the principle of the preservation of higher levels of protection in Article 53 of the Charter that the limits applicable under the Charter in relation to permissible restrictions must be more narrowly circumscribed by secondary law?

(e) Having regard to Article 52(3) of the Charter, the fifth paragraph in the preamble thereto and the explanations in relation to Article 7 of the Charter, according to which the rights guaranteed in that article correspond to those guaranteed by Article 8 of the [ECHR], can assistance be derived from the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of that latter article?’

[...]

On those grounds, the Court (Grand Chamber) hereby rules: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid.

C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,

1. Article 2(b) and (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the ‘controller’ in respect of that processing, within the meaning of Article 2(d).

2. Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that

provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

3. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

4. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should *inter alia* be examined whether the data subject has a right that the information in question relating

to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

[...]

household activity, for the purposes of that provision

C-212/13, František Ryneš v Úřad pro ochranu osobních údajů,

[...]

18. In those circumstances, the Nejvyšší správní soud decided to stay proceedings and refer the following question to the Court of Justice for a preliminary ruling:

'Can the operation of a camera system installed on a family home for the purposes of the protection of the property, health and life of the owners of the home be classified as the processing of personal data "by a natural person in the course of a purely personal or household activity" for the purposes of Article 3(2) of Directive 95/46 ..., even though such a system also monitors a public space?'

[...]

On those grounds, the Court (Fourth Chamber) hereby rules:

The second indent of Article 3(2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or

C-362/14 - Schrems

1. Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that Directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

2. Decision 2000/520 is invalid.

Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission, After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced. (8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation

does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC (5).

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council (6) applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in

the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council (7). Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council (8), in particular of the liability rules of intermediary

service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern

the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the Regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample

from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (9) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating

personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (10) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the

legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights

including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest,

scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council (11), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including

mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those

considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore

not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the Regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the

controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour,

location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the

processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available

technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing. (85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been

carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this

Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations

may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant

developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council (12) as established under this Regulation, to the European Parliament and to the Council.

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding. (109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(115) Some third countries adopt laws, Regulations and other legal acts which purport to directly regulate the processing

activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, Regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, *inter alia*, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the

government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single

establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority

authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any

supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject

matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council (13) should not prejudice the application of such specific rules.

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of

the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council (14) leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to

erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council (15) should apply.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing.

Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163)The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council (16) provides further specifications on statistical confidentiality for European statistics.

(164)As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(165)This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166)In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(167)In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(168)The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory

authorities, and between supervisory authorities and the Board.

(169)The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170)Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(171)Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(172)The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 (17).

(173)This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council (18), including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

- (a) in the course of an activity which falls outside the scope of Union law;
- (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
- (c) by a natural person in the course of a purely personal or household activity;
- (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) 'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that

the processor is subject to specific obligations under this Regulation;

(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

(22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (19);

(26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not

be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects

concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

- (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
- (d) the possible consequences of the intended further processing for data subjects;
- (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when

those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the

request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in

those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3 Rectification and erasure

Article 16 Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17 Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18 Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20 Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4 Right to object and automated individual decision-making

Article 21 Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
 - (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - (c) is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5 Restrictions

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms

and is a necessary and proportionate measure in a democratic society to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- (f) the protection of judicial independence and judicial proceedings;
- (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- (i) the protection of the data subject or the rights and freedoms of others;
- (j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

- (a) the purposes of the processing or categories of processing;
- (b) the categories of personal data;
- (c) the scope of the restrictions introduced;
- (d) the safeguards to prevent abuse or unlawful access or transfer;
- (e) the specification of the controller or categories of controllers;
- (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- (g) the risks to the rights and freedoms of data subjects; and
- (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and

severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

- (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
- (b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing

will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;
- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- (f) where possible, the envisaged time limits for erasure of the different categories of data;
- (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

- (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is

acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
 - (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - (c) describe the likely consequences of the personal data breach;
 - (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
 - (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
 - (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
 - (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
 - (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
 - (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
 - (c) a systematic monitoring of a publicly accessible area on a large scale.
4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.
5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.
6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.
7. The assessment shall contain at least:
 - (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
 - (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
 - (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.
9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.
10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been

carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36

Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

- (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
- (b) the purposes and means of the intended processing;
- (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
- (d) where applicable, the contact details of the data protection officer;
- (e) the data protection impact assessment provided for in Article 35; and
- (f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4 Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

- (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their

scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code,

amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including

suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42 Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43 Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to

point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (20) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and

recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or

authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

- (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
- (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

- (a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
- (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
- (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

- (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- (c) their legally binding nature, both internally and externally;
- (d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- (e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
- (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;
- (g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;
- (h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding

corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

- (i) the complaint procedures;
- (j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

- (k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
- (l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

- (m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
- (n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of public interest;

- (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

- (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
- (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
- (c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

- (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 52

Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53

General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

- their parliament;
-

their government;

—

their head of State; or

—

an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Section 2

Competence, tasks and powers

Article 55

Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56

Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried

out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) Conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
(l) give advice on the processing operations referred to in Article 36(2);
(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(r) authorise contractual clauses and provisions referred to in Article 46(3);
(s) approve binding corporate rules pursuant to Article 47;
(t) contribute to the activities of the Board;
(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58 Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
(b) to carry out investigations in the form of data protection audits;
(c) to carry out a review on certifications issued pursuant to Article 42(7);
(d) to notify the controller or the processor of an alleged infringement of this Regulation;
(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59 Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as

designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII Cooperation and consistency

Section 1 Cooperation

Article 60

Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.
8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.
9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and

shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

- (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
- (b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the

exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62

Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.
2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.
3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.
4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.
5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.
6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.
7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2 Consistency

Article 63

Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64

Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:
 - (a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);
 - (b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;
 - (c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);
 - (d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);
 - (e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or
 - (f) aims to approve binding corporate rules within the meaning of Article 47.
2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.
3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.
4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.
5. The Chair of the Board shall, without undue, delay inform by electronic means:
 - (a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and
 - (b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.
6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.
7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.
8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7

of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65 Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall be adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66 Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to

in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67 Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3 European data protection board

Article 68 European Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69 Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70
Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

- (a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;
- (b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;
- (c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;
- (d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);
- (e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;
- (f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);
- (g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;
- (h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1);
- (i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;
- (j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);
- (k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;
- (l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);
- (m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);
- (n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;
- (o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);
- (p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

- (q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);
- (r) provide the Commission with an opinion on the icons referred to in Article 12(7);
- (s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.
- (t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;
- (u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;
- (v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;
- (w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.
- (x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and
- (y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71
Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72
Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73
Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.
2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74
Tasks of the Chair

1. The Chair shall have the following tasks:
 - (a) to convene the meetings of the Board and prepare its agenda;
 - (b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;
 - (c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.
2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75
Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.
2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.
3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.
4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.
5. The secretariat shall provide analytical, administrative and logistical support to the Board.
6. The secretariat shall be responsible in particular for:
 - (a) the day-to-day business of the Board;
 - (b) communication between the members of the Board, its Chair and the Commission;
 - (c) communication with other institutions and the public;
 - (d) the use of electronic means for the internal and external communication;
 - (e) the translation of relevant information;
 - (f) the preparation and follow-up of the meetings of the Board;
 - (g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76
Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.
2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council (21).

CHAPTER VIII
Remedies, liability and penalties

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a

complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.
4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.
2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it

considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81

Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.
2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.
3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.
4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.
5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.
6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
 - (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing

- (b) the intentional or negligent character of the infringement;
 - (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
 - (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
 - (e) any relevant previous infringements by the controller or processor;
 - (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
 - (g) the categories of personal data affected by the infringement;
 - (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
 - (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
 - (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
 - (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.
3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.
 4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
 - (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
 - (b) the obligations of the certification body pursuant to Articles 42 and 43;
 - (c) the obligations of the monitoring body pursuant to Article 41(4).
 5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
 - (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
 - (b) the data subjects' rights pursuant to Articles 12 to 22;
 - (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
 - (d) any obligations pursuant to Member State law adopted under Chapter IX;
 - (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).
 6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
 7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.
 8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural

safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84 Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX

Provisions relating to specific processing situations

Article 85 Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86 Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87 Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general

application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88 Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89 Safeguards and derogations relating to processing for archiving purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90 Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X

Delegated acts and implementing acts

Article 92

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

Final provisions

Article 94

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96

Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Article 97

Commission reports

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account developments in information technology and in the light of the state of progress in the information society.

Article 98

Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by

Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

J.A. HENNIS-PLASSCHAERT

(1) OJ C 229, 31.7.2012, p. 90.

(2) OJ C 391, 18.12.2012, p. 127.

(3) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.

(4) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(5) Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

(6) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(7) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

(8) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

(9) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(10) Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

(11) Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

(12) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(13) Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on

jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

(14) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

(15) Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

(16) Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

(17) OJ C 192, 30.6.2012, p. 7.

(18) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

(19) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical Regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(20) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

(21) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

Top

Other sites managed by the Publications Office

EU Bookshop

EU Open Data Portal

Ted

Whoiswho

CORDIS

N-Lex

EU law and publications

Direct access

Official Journal

EU law and related documents

National law

Preparatory acts

More...

Practical information

FAQ

Help

Contact

EuroVoc

My EUR-Lex

Preferences

My searches

My items

My RSS feeds

About this websiteLegal noticeContactTop

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission, After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the Committee of the Regions (1), Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(4) The free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed by strong enforcement.

(5) Directive 95/46/EC of the European Parliament and of the Council (3) applies to all processing of personal data in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities in the areas of judicial cooperation in criminal matters and police cooperation.

(6) Council Framework Decision 2008/977/JHA (4) applies in the areas of judicial cooperation in criminal matters and police cooperation. The scope of application of that Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(7) Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Member States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation. To that end, the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should be equivalent in all Member States. Effective protection of personal data throughout the Union requires the strengthening of the rights of data subjects and of the obligations of those who process personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

(8) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(9) On that basis, Regulation (EU) 2016/679 of the European Parliament and of the Council (5) lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

(10) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.

(11) It is therefore appropriate for those fields to be addressed by a Directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, Regulation (EU) 2016/679 applies. Regulation (EU) 2016/679 therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain

certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of Regulation (EU) 2016/679 remains unaffected for the processing of personal data by the processor outside the scope of this Directive.

(12) The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation (EU) 2016/679.

(13) A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union (the 'Court of Justice').

(14) Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive.

(15) In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, this Directive should provide for harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The approximation of Member States' laws should not result in any lessening of the personal data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

(16) This Directive is without prejudice to the principle of public access to official documents. Under Regulation (EU) 2016/679 personal data in official documents held by a public authority or a public or private body for the performance of a task carried out in the public interest may be disclosed by that authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data.

(17) The protection afforded by this Directive should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

(18) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Directive.

(19) Regulation (EC) No 45/2001 of the European Parliament and of the Council (6) applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in Regulation (EU) 2016/679.

(20) This Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings.

(21) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable.

(22) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the Regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data protection rules according to the purposes of the processing.

(23) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or health of that natural person and which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained. Considering the complexity and sensitivity of genetic information, there is a great risk of misuse and re-use for various purposes by the controller. Any discrimination based on genetic features should in principle be prohibited.

(24) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as

referred to in Directive 2011/24/EU of the European Parliament and of the Council (7) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(25) All Member States are affiliated to the International Criminal Police Organisation (Interpol). To fulfil its mission, Interpol receives, stores and circulates personal data to assist competent authorities in preventing and combating international crime. It is therefore appropriate to strengthen cooperation between the Union and Interpol by promoting an efficient exchange of personal data whilst ensuring respect for fundamental rights and freedoms regarding the automatic processing of personal data. Where personal data are transferred from the Union to Interpol, and to countries which have delegated members to Interpol, this Directive, in particular the provisions on international transfers, should apply. This Directive should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA (8) and Council Decision 2007/533/JHA (9).

(26) Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.

(27) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.

(28) In order to maintain security in relation to processing and to prevent processing in infringement of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, including by preventing unauthorised access to or use of personal data and

the equipment used for the processing, and that takes into account available state of the art and technology, the costs of implementation in relation to the risks and the nature of the personal data to be protected.

(29) Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and should not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. If personal data are processed by the same or another controller for a purpose within the scope of this Directive other than that for which it has been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose.

(30) The principle of accuracy of data should be applied while taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of natural persons and are not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(31) It is inherent to the processing of personal data in the areas of judicial cooperation in criminal matters and police cooperation that personal data relating to different categories of data subjects are processed. Therefore, a clear distinction should, where applicable and as far as possible, be made between personal data of different categories of data subjects such as: suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses; persons possessing relevant information or contacts; and associates of suspects and convicted criminals. This should not prevent the application of the right of presumption of innocence as guaranteed by the Charter and by the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively.

(32) The competent authorities should ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. In order to ensure the protection of natural persons, the accuracy, completeness or the extent to which the personal data are up to date and the reliability of the personal data transmitted or made available, the competent authorities should, as far as possible, add necessary information in all transmissions of personal data.

(33) Where this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

(34) The processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction.

In particular, the rules of this Directive should apply to the transmission of personal data for the purposes of this Directive to a recipient not subject to this Directive. Such a recipient should encompass a natural or legal person, public authority, agency or any other body to which personal data are lawfully disclosed by the competent authority. Where personal data were initially collected by a competent authority for one of the purposes of this Directive, Regulation (EU) 2016/679 should apply to the processing of those data for purposes other than the purposes of this Directive where such processing is authorised by Union or Member State law. In particular, the rules of Regulation (EU) 2016/679 should apply to the transmission of personal data for purposes outside the scope of this Directive. For the processing of personal data by a recipient that is not a competent authority or that is not acting as such within the meaning of this Directive and to which personal data are lawfully disclosed by a competent authority, Regulation (EU) 2016/679 should apply. While implementing this Directive, Member States should also be able to further specify the application of the rules of Regulation (EU) 2016/679, subject to the conditions set out therein.

(35) In order to be lawful, the processing of personal data under this Directive should be necessary for the performance of a task carried out in the public interest by a competent authority based on Union or Member State law for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Those activities should cover the protection of vital interests of the data subject. The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.

(36) Member States should provide that where Union or Member State law applicable to the transmitting competent authority provides for specific conditions applicable in specific circumstances to the processing of personal data, such as the use of handling codes, the transmitting competent authority should inform the recipient of such personal data of those conditions and the requirement to respect them. Such conditions could, for example, include a prohibition against transmitting the personal data further to others, or using them for purposes other than those for which they were transmitted to the recipient, or informing the data subject in the case of a limitation of the right of information without the prior approval of the transmitting competent authority. Those obligations should also apply to transfers by the transmitting competent authority to recipients in third countries or international organisations. Member States should ensure that the transmitting competent authority does not apply such conditions to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar data transmissions within the Member State of that competent authority.

(37) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial

origin' in this Directive does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. Such personal data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; where not already authorised by such a law, the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject. Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data. The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.

(38) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces adverse legal effects concerning, or significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision. Profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited under the conditions laid down in Articles 21 and 52 of the Charter.

(39) In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language. Such information should be adapted to the needs of vulnerable persons such as children.

(40) Modalities should be provided for facilitating the exercise of the data subject's rights under the provisions adopted pursuant to this Directive, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and restriction of processing. The controller should be obliged to respond to requests of the data subject without undue delay, unless the controller applies limitations to data subject rights in accordance with this Directive. Moreover, if requests are manifestly unfounded or excessive, such as where the data subject unreasonably and repetitiously requests information or where the data subject abuses his or her right to receive information, for example, by providing false or misleading information when making the request, the controller should be able to charge a reasonable fee or refuse to act on the request.

(41) Where the controller requests the provision of additional information necessary to confirm the identity of the data subject, that information should be processed only for that specific purpose and should not be stored for longer than needed for that purpose.

(42) At least the following information should be made available to the data subject: the identity of the controller, the existence of the processing operation, the purposes of the processing, the right to lodge a complaint and the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing. This could take place on the website of the competent authority. In addition, in specific cases and in order to enable the exercise of his or her rights, the data subject should be informed of the legal basis for the processing and of how long the data will be stored, in so far as such further information is necessary, taking into account the specific

circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

(43) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know, and obtain communications about, the purposes for which the data are processed, the period during which the data are processed and the recipients of the data, including those in third countries. Where such communications include information as to the origin of the personal data, the information should not reveal the identity of natural persons, in particular confidential sources. For that right to be complied with, it is sufficient that the data subject be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that data subject to become aware of those data and to verify that they are accurate and processed in accordance with this Directive, so that it is possible for him or her to exercise the rights conferred on him or her by this Directive. Such a summary could be provided in the form of a copy of the personal data undergoing processing.

(44) Member States should be able to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others. The controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted.

(45) Any refusal or restriction of access should in principle be set out in writing to the data subject and include the factual or legal reasons on which the decision is based.

(46) Any restriction of the rights of the data subject must comply with the Charter and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms.

(47) A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular where it relates to facts, and the right to erasure where the processing of such data infringes this Directive. However, the right to rectification should not affect, for example, the content of a witness testimony. A natural person should also have the right to restriction of processing where he or she contests the accuracy of personal data and its accuracy or inaccuracy cannot be ascertained or where the personal data have to be maintained for purpose of evidence. In particular, instead of erasing personal data, processing should be restricted if in a specific case there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. In such a case, restricted data should be processed only for the purpose which prevented their erasure. Methods to restrict the processing of personal data could include, inter alia, moving the selected data to another processing system, for example for archiving purposes, or making the selected data unavailable. In automated filing systems the restriction of processing should in principle be ensured by technical means. The fact that the processing of personal data is restricted should be indicated in the system in such a manner that it is clear that the processing of the personal data is restricted. Such rectification or erasure of personal data or restriction of processing should be communicated to recipients to whom the data have been disclosed and to the competent authorities from which the inaccurate data originated. The controllers should also abstain from further dissemination of such data.

(48) Where the controller denies a data subject his or her right to information, access to or rectification or erasure of personal data or restriction of processing, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing. The data subject should be informed of that right. Where the supervisory authority acts on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory authority have taken place. The supervisory authority should also inform the data subject of the right to seek a judicial remedy.

(49) Where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, Member States should be able to provide that the exercise the right to information, access to and rectification or erasure of personal data and restriction of processing is carried out in accordance with national rules on judicial proceedings.

(50) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and should be able to demonstrate that processing activities are in compliance with this Directive. Such measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable natural persons, such as children.

(51) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or where data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed; where personal aspects are evaluated, in particular analysing and predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(52) The likelihood and severity of the risk should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, through which it is established whether data-processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of data subjects.

(53) The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organisational measures are taken, to ensure that the requirements of this Directive are met. The implementation of such measures should not depend solely on economic considerations. In order to be able to demonstrate compliance with this Directive, the controller should adopt internal policies and implement measures which adhere in particular to the principles of data protection by design and data protection by default. Where the controller has carried out a data protection impact assessment pursuant to this Directive, the results should be taken into account when developing those measures and procedures. The measures could consist, inter

alia, of the use of pseudonymisation, as early as possible. The use of pseudonymisation for the purposes of this Directive can serve as a tool that could facilitate, in particular, the free flow of personal data within the area of freedom, security and justice.

(54) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities set out in this Directive, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(55) The carrying-out of processing by a processor should be governed by a legal act including a contract binding the processor to the controller and stipulating, in particular, that the processor should act only on instructions from the controller. The processor should take into account the principle of data protection by design and by default.

(56) In order to demonstrate compliance with this Directive, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records available to it on request, so that they might serve for monitoring those processing operations. The controller or the processor processing personal data in non-automated processing systems should have in place effective methods of demonstrating the lawfulness of the processing, of enabling self-monitoring and of ensuring data integrity and data security, such as logs or other forms of records.

(57) Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged and from that identification it should be possible to establish the justification for the processing operations. The logs should solely be used for the verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.

(58) A data protection impact assessment should be carried out by the controller where the processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes, which should include, in particular, the measures, safeguards and mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with this Directive. Impact assessments should cover relevant systems and processes of processing operations, but not individual cases.

(59) In order to ensure effective protection of the rights and freedoms of data subjects, the controller or processor should consult the supervisory authority, in certain cases, prior to the processing.

(60) In order to maintain security and to prevent processing that infringes this Directive, the controller or processor should evaluate the risks inherent in the processing and should implement measures to mitigate those risks, such as encryption. Such measures should ensure an appropriate level of security, including confidentiality and take into account the state of the art, the costs of implementation in relation to the risk and the nature of the personal data to be protected. In assessing data security risks, consideration should be given to the risks that are presented by data processing, such as the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed, which may, in particular, lead to physical, material or non-material damage. The controller and processor should ensure that the processing of personal data is not carried out by unauthorised persons.

(61) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights,

discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(62) Natural persons should be informed without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, in order to allow them to take the necessary precautions. The communication should describe the nature of the personal data breach and include recommendations for the natural person concerned to mitigate potential adverse effects. Communication to data subjects should be made as soon as reasonably feasible, in close cooperation with the supervisory authority, and respecting guidance provided by it or other relevant authorities. For example, the need to mitigate an immediate risk of damage would call for a prompt communication to data subjects, whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for the communication. Where avoiding obstruction of official or legal inquiries, investigations or procedures, avoiding prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protecting public security, protecting national security or protecting the rights and freedoms of others cannot be achieved by delaying or restricting the communication of a personal data breach to the natural person concerned, such communication could, in exceptional circumstances, be omitted.

(63) The controller should designate a person who would assist it in monitoring internal compliance with the provisions adopted pursuant to this Directive, except where a Member State decides to exempt courts and other independent judicial authorities when acting in their judicial capacity. That person could be a member of the existing staff of the controller who received special training in data protection law and practice in order to acquire expert knowledge in that field. The necessary level of expert knowledge should be determined, in particular, according to the data processing carried out and the protection required for the personal data processed by the controller. His or her task could be carried out on a part-time or full-time basis. A data protection officer may be appointed jointly by several controllers, taking into account their organisational structure and size, for example in the case of shared resources in central units. That person can also be appointed to different positions within the structure of the relevant controllers. That person should help the controller and the employees processing personal data by informing and advising them on compliance with their relevant data protection obligations. Such data protection officers should be in a position to perform their duties and tasks in an independent manner in accordance with Member State law.

(64) Member States should ensure that a transfer to a third country or to an international organisation takes place only if necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and that the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer should be carried out only by competent authorities acting as controllers, except where processors are explicitly instructed to transfer on behalf of controllers. Such a transfer

may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level of protection, where appropriate safeguards have been provided, or where derogations for specific situations apply. Where personal data are transferred from the Union to controllers, to processors or to other recipients in third countries or international organisations, the level of protection of natural persons provided for in the Union by this Directive should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same or in another third country or international organisation.

(65) Where personal data are transferred from a Member State to third countries or international organisations, such a transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law-enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Member State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such a prior authorisation. Member States should provide that any specific conditions concerning the transfer should be communicated to third countries or international organisations. Onward transfers of personal data should be subject to prior authorisation by the competent authority that carried out the original transfer. When deciding on a request for the authorisation of an onward transfer, the competent authority that carried out the original transfer should take due account of all relevant factors, including the seriousness of the criminal offence, the specific conditions subject to which, and the purpose for which, the data was originally transferred, the nature and conditions of the execution of the criminal penalty, and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred. The competent authority that carried out the original transfer should also be able to subject the onward transfer to specific conditions. Such specific conditions can be described, for example, in handling codes.

(66) The Commission should be able to decide with effect for the entire Union that certain third countries, a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such a level of protection. In such cases, transfers of personal data to those countries should be able to take place without the need to obtain any specific authorisation, except where another Member State from which the data were obtained has to give its authorisation to the transfer.

(67) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security, as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and provide for cooperation mechanisms with the Member States' data protection

authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(68) Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult with the European Data Protection Board established by Regulation (EU) 2016/679 (the 'Board') when assessing the level of protection in third countries or international organisations. The Commission should also take into account any relevant Commission adequacy decision adopted in accordance with Article 45 of Regulation (EU) 2016/679.

(69) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or a specified sector within a third country, or an international organisation. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be undertaken in consultation with the third country or international organisation in question and should take into account all relevant developments in the third country or international organisation.

(70) The Commission should also be able to recognise that a third country, a territory or a specified sector within a third country, or an international organisation, no longer ensures an adequate level of data protection. Consequently, the transfer of personal data to that third country or international organisation should be prohibited unless the requirements in this Directive relating to transfers subject to appropriate safeguards and derogations for specific situations are fulfilled. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(71) Transfers not based on such an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist. Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. The controller should be able to take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, the controller should be able to require additional safeguards.

(72) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could take place only

in specific situations, if necessary to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; for the prevention of an immediate and serious threat to the public security of a Member State or a third country; in an individual case for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or in an individual case for the establishment, exercise or defence of legal claims. Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data, or large-scale transfers of data, but should be limited to data strictly necessary. Such transfers should be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.

(73) Competent authorities of Member States apply bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial cooperation in criminal matters and police cooperation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through, or at least with, the cooperation of the authorities competent in the third countries concerned for the purposes of this Directive, sometimes even in the absence of a bilateral or multilateral international agreement. However, in specific individual cases, the regular procedures requiring contacting such an authority in the third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards, so that competent authorities of Member States could decide to transfer personal data directly to recipients established in those third countries. This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism. Even if such a transfer between competent authorities and recipients established in third countries should take place only in specific individual cases, this Directive should provide for conditions to regulate such cases. Those provisions should not be considered to be derogations from any existing bilateral or multilateral international agreements in the field of judicial cooperation in criminal matters and police cooperation. Those rules should apply in addition to the other rules of this Directive, in particular those on the lawfulness of processing and Chapter V.

(74) Where personal data move across borders it may put at increased risk the ability of natural persons to exercise data protection rights to protect themselves from the unlawful use or disclosure of those data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers and inconsistent legal regimes. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information with their foreign counterparts.

(75) The establishment in Member States of supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and should contribute to their consistent application throughout the Union in order to protect natural persons with regard to the processing of their personal data. To that end, the supervisory authorities should cooperate with each other and with the Commission.

(76) Member States may entrust a supervisory authority already established under Regulation (EU) 2016/679 with the

responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(77) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with the financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(78) Supervisory authorities should be subject to independent control or monitoring mechanisms regarding their financial expenditure, provided that such financial control does not affect their independence.

(79) The general conditions for the member or members of the supervisory authority should be laid down by Member State law and should in particular provide that those members should be either appointed by the parliament or the government or the head of State of the Member State based on a proposal from the government or a member of the government, or the parliament or its chamber, or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, should refrain from any action incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. In order to ensure the independence of the supervisory authority, the staff should be chosen by the supervisory authority which may include an intervention by an independent body entrusted by Member State law.

(80) While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data where courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. That exemption should be limited to judicial activities in court cases and not apply to other activities where judges might be involved in accordance with Member State law. Member States should also be able to provide that the competence of the supervisory authority does not cover the processing of personal data of other independent judicial authorities when acting in their judicial capacity, for example public prosecutor's office. In any event, the compliance with the rules of this Directive by the courts and other independent judicial authorities is always subject to independent supervision in accordance with Article 8(3) of the Charter.

(81) Each supervisory authority should handle complaints lodged by any data subject and should investigate the matter or transmit it to the competent supervisory authority. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be provided to the data subject.

(82) In order to ensure effective, reliable and consistent monitoring of compliance with and enforcement of this Directive throughout the Union pursuant to the TFEU as interpreted by the Court of Justice, the supervisory authorities should have in each Member State the same tasks and effective powers, including investigative, corrective, and advisory powers which constitute necessary means to perform their tasks. However, their powers should not interfere with specific rules for criminal proceedings, including investigation and prosecution of criminal offences, or the independence of the judiciary. Without prejudice to the powers of prosecutorial

authorities under Member State law, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities or to engage in legal proceedings. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards laid down by Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Directive, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure that would adversely affect the person concerned is taken, and avoiding superfluous costs and excessive inconvenience to the person concerned. Investigative powers as regards access to premises should be exercised in accordance with specific requirements in Member State law, such as the requirement to obtain a prior judicial authorisation. The adoption of a legally binding decision should be subject to judicial review in the Member State of the supervisory authority that adopted the decision.

(83)The supervisory authorities should assist one another in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(84)The Board should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the cooperation of the supervisory authorities throughout the Union.

(85)Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The competent supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be provided to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(86)Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, that right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with Member State law. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.

(87)Where a data subject considers that his or her rights under this Directive are infringed, he or she should have the right to mandate a body which aims to protect the rights and interests of data subjects in relation to the protection of their personal data and is constituted according to Member State law to lodge a complaint on his or her behalf with a supervisory authority and to exercise the right to a judicial remedy. The right of representation of data subjects should be without prejudice to Member State procedural law which may require mandatory

representation of data subjects by a lawyer, as defined in Council Directive 77/249/EEC (10), before national courts.

(88)Any damage which a person may suffer as a result of processing that infringes the provisions adopted pursuant to this Directive should be compensated by the controller or any other authority competent under Member State law. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Directive. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. When reference is made to processing that is unlawful or that infringes the provisions adopted pursuant to this Directive it also covers processing that infringes implementing acts adopted pursuant to this Directive. Data subjects should receive full and effective compensation for the damage that they have suffered.

(89)Penalties should be imposed on any natural or legal person, whether governed by private or public law, who infringes this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and should take all measures to implement the penalties.

(90)In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission with regard to the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (11).

(91)The examination procedure should be used for the adoption of implementing acts on the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and on the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, given that those acts are of a general scope.

(92)The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country, a territory or a specified sector within a third country, or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.

(93)Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the TEU. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives

(94)Specific provisions of acts of the Union adopted in the field of judicial cooperation in criminal matters and police cooperation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected, such as, for example, the specific provisions concerning the protection of personal data applied pursuant to Council Decision 2008/615/JHA (12), or Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (13). Since Article 8 of the Charter and Article 16 TFEU require that the fundamental right to the protection of personal data be ensured in a consistent manner

throughout the Union, the Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of those specific provisions with this Directive. Where appropriate, the Commission should make proposals with a view to ensuring consistent legal rules relating to the processing of personal data.

(95) In order to ensure a comprehensive and consistent protection of personal data in the Union, international agreements which were concluded by Member States prior to the date of entry into force of this Directive and which comply with the relevant Union law applicable prior to that date should remain in force until amended, replaced or revoked.

(96) Member States should be allowed a period of not more than two years from the date of entry into force of this Directive to transpose it. Processing already under way on that date should be brought into conformity with this Directive within the period of two years after which this Directive enters into force. However, where such processing complies with the Union law applicable prior to the date of entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way on that date given that those requirements, by their very nature, are to be met prior to the processing. Where Member States use the longer implementation period expiring seven years after the date of entry into force of this Directive for meeting the logging obligations for automated processing systems set up prior to that date, the controller or the processor should have in place effective methods for demonstrating the lawfulness of the data processing, for enabling self-monitoring and for ensuring data integrity and data security, such as logs or other forms of records.

(97) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93/EU of the European Parliament and of the Council (14).

(98) Framework Decision 2008/977/JHA should therefore be repealed.

(99) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, the United Kingdom and Ireland are not bound by the rules laid down in this Directive which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU.

(100) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, as annexed to the TEU and to the TFEU, Denmark is not bound by the rules laid down in this Directive or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the TFEU, Denmark, in accordance with Article 4 of that Protocol, is to decide within six months after adoption of this Directive whether it will implement it in its national law.

(101) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis (15).

(102) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis (16).

(103) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (17).

(104) This Directive respects the fundamental rights and observes the principles recognised in the Charter as enshrined in the TFEU, in particular the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on those rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(105) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a Directive and the corresponding parts of national transposition measures. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(106) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 (18).

(107) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access to and rectification or erasure of personal data and restriction of processing in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I General provisions

Article 1 Subject-matter and objectives

1. This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

2. In accordance with this Directive, Member States shall:
(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and
(b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

3. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

Article 2

Scope

1. This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).
2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
3. This Directive does not apply to the processing of personal data:
 - (a) in the course of an activity which falls outside the scope of Union law;
 - (b) by the Union institutions, bodies, offices and agencies.

Article 3

Definitions

For the purposes of this Directive:

- (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
- (4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- (5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- (6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- (7) 'competent authority' means:
 - (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or
 - (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (8) 'controller' means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- (9) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- (10) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- (11) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (12) 'genetic data' means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- (13) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- (14) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- (15) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 41;
- (16) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II Principles

Article 4

Principles relating to processing of personal data

1. Member States shall provide for personal data to be:
 - (a) processed lawfully and fairly;
 - (b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
 - (c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
 - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
 - (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
2. Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:
 - (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and
 - (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.
3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or

historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.

4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

Article 5

Time-limits for storage and review

Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.

Article 6

Distinction between different categories of data subject

Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:

- (a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
- (b) persons convicted of a criminal offence;
- (c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and
- (d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).

Article 7

Distinction between personal data and verification of quality of personal data

1. Member States shall provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments.
2. Member States shall provide for the competent authorities to take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.
3. If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with Article 16.

Article 8

Lawfulness of processing

1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.
2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.

Article 9

Specific processing conditions

1. Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.

2. Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law.

3. Member States shall, where Union or Member State law applicable to the transmitting competent authority provides specific conditions for processing, provide for the transmitting competent authority to inform the recipient of such personal data of those conditions and the requirement to comply with them.

4. Member States shall provide for the transmitting competent authority not to apply conditions pursuant to paragraph 3 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.

Article 10

Processing of special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

- (a) where authorised by Union or Member State law;
- (b) to protect the vital interests of the data subject or of another natural person; or
- (c) where such processing relates to data which are manifestly made public by the data subject.

Article 11

Automated individual decision-making

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

CHAPTER III Rights of the data subject

Article 12

Communication and modalities for exercising the rights of the data subject

1. Member States shall provide for the controller to take reasonable steps to provide any information referred to in Article 13 and make any communication with regard to Articles 11, 14 to 18 and 31 relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.

2. Member States shall provide for the controller to facilitate the exercise of the rights of the data subject under Articles 11 and 14 to 18.

3. Member States shall provide for the controller to inform the data subject in writing about the follow up to his or her request without undue delay.

4. Member States shall provide for the information provided under Article 13 and any communication made or action taken pursuant to Articles 11, 14 to 18 and 31 to be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

5. Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 14 or 16, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 13

Information to be made available or given to the data subject

1. Member States shall provide for the controller to make available to the data subject at least the following information:

(a) the identity and the contact details of the controller;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended;

(d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;

(e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

2. In addition to the information referred to in paragraph 1, Member States shall provide by law for the controller to give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:

(a) the legal basis for the processing;

(b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;

(c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;

(d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

4. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of the points listed in paragraph 3.

Article 14

Right of access by the data subject

Subject to Article 15, Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of and legal basis for the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;

(f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;

(g) communication of the personal data undergoing processing and of any available information as to their origin.

Article 15

Limitations to the right of access

1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

2. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under points (a) to (e) of paragraph 1.

3. In the cases referred to in paragraphs 1 and 2, Member States shall provide for the controller to inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

4. Member States shall provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.

Article 16

Right to rectification or erasure of personal data and restriction of processing

1. Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her. Taking into account the purposes of the processing, Member States shall provide for the data subject to have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

2. Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.

3. Instead of erasure, the controller shall restrict processing where:

(a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or

(b) the personal data must be maintained for the purposes of evidence.

Where processing is restricted pursuant to point (a) of the first subparagraph, the controller shall inform the data subject before lifting the restriction of processing.

4. Member States shall provide for the controller to inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

5. Member States shall provide for the controller to communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

6. Member States shall, where personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 and 3, provide for the controller to notify the recipients and that the recipients shall rectify or erase the personal data or restrict processing of the personal data under their responsibility.

Article 17

Exercise of rights by the data subject and verification by the supervisory authority

1. In the cases referred to in Article 13(3), Article 15(3) and Article 16(4) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.

2. Member States shall provide for the controller to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1.

3. Where the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

Article 18

Rights of the data subject in criminal investigations and proceedings

Member States may provide for the exercise of the rights referred to in Articles 13, 14 and 16 to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 19

Obligations of the controller

1. Member States shall provide for the controller, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Directive. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Article 20

Data protection by design and by default

1. Member States shall provide for the controller, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Directive and protect the rights of data subjects.

2. Member States shall provide for the controller to implement appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Article 21

Joint controllers

1. Member States shall, where two or more controllers jointly determine the purposes and means of processing, provide for them to be joint controllers. They shall, in a transparent manner, determine their respective responsibilities for compliance with this Directive, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 13, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate the

contact point for data subjects. Member States may designate which of the joint controllers can act as a single contact point for data subjects to exercise their rights.

2. Irrespective of the terms of the arrangement referred to in paragraph 1, Member States may provide for the data subject to exercise his or her rights under the provisions adopted pursuant to this Directive in respect of and against each of the controllers.

Article 22

Processor

1. Member States shall, where processing is to be carried out on behalf of a controller, provide for the controller to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Directive and ensure the protection of the rights of the data subject.

2. Member States shall provide for the processor not to engage another processor without prior specific or general written authorisation by the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Member States shall provide for the processing by a processor to be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

- (a) acts only on instructions from the controller;
- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;
- (d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- (e) makes available to the controller all information necessary to demonstrate compliance with this Article;
- (f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.

4. The contract or the other legal act referred to in paragraph 3 shall be in writing, including in an electronic form.

5. If a processor determines, in infringement of this Directive, the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing.

Article 23

Processing under the authority of the controller or processor

Member States shall provide for the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, not to process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 24

Records of processing activities

1. Member States shall provide for controllers to maintain a record of all categories of processing activities under their responsibility. That record shall contain all of the following information:

- (a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;

(b) the purposes of the processing;

(c) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(d) a description of the categories of data subject and of the categories of personal data;

(e) where applicable, the use of profiling;

(f) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(g) an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;

(h) where possible, the envisaged time limits for erasure of the different categories of personal data;

(i) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

2. Member States shall provide for each processor to maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

The controller and the processor shall make those records available to the supervisory authority on request.

Article 25

Logging

1. Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

2. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

3. The controller and the processor shall make the logs available to the supervisory authority on request.

Article 26

Cooperation with the supervisory authority

Member States shall provide for the controller and the processor to cooperate, on request, with the supervisory authority in the performance of its tasks on request.

Article 27

Data protection impact assessment

1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address

those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Article 28

Prior consultation of the supervisory authority

1. Member States shall provide for the controller or processor to consult the supervisory authority prior to processing which will form part of a new filing system to be created, where:

(a) a data protection impact assessment as provided for in Article 27 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

(b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

2. Member States shall provide for the supervisory authority to be consulted during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to processing.

3. Member States shall provide that the supervisory authority may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

4. Member States shall provide for the controller to provide the supervisory authority with the data protection impact assessment pursuant to Article 27 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

5. Member States shall, where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 of this Article would infringe the provisions adopted pursuant to this Directive, in particular where the controller has insufficiently identified or mitigated the risk, provide for the supervisory authority to provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, and may use any of its powers referred to in Article 47. That period may be extended by a month, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay.

Section 2 Security of personal data

Article 29

Security of processing

1. Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10.

2. In respect of automated processing, each Member State shall provide for the controller or processor, following an evaluation of the risks, to implement measures designed to:

(a) deny unauthorised persons access to processing equipment used for processing ('equipment access control');

(b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');

(c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');

(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');

(e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');

(f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');

(i) ensure that installed systems may, in the case of interruption, be restored ('recovery');

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

(k) security provision editors remark

Article 30

Notification of a personal data breach to the supervisory authority

1. Member States shall, in the case of a personal data breach, provide for the controller to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. Member States shall provide for the controller to document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

6. Member States shall, where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, provide for the information referred to in paragraph 3 to be communicated to the controller of that Member State without undue delay.

Article 31

Communication of a personal data breach to the data subject

1. Member States shall, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, provide for the controller to communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in points (b), (c) and (d) of Article 30(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph 3 are met.

5. The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 13(3).

Section 3

Data protection officer

Article 32

Designation of the data protection officer

1. Member States shall provide for the controller to designate a data protection officer. Member States may exempt courts and other independent judicial authorities when acting in their judicial capacity from that obligation.

2. The data protection officer shall be designated on the basis of his or her professional qualities and, in particular, his or her expert knowledge of data protection law and practice and ability to fulfil the tasks referred to in Article 34.

3. A single data protection officer may be designated for several competent authorities, taking account of their organisational structure and size.

4. Member States shall provide for the controller to publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 33

Position of the data protection officer

1. Member States shall provide for the controller to ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller shall support the data protection officer in performing the tasks referred to in Article 34 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

Article 34

Tasks of the data protection officer

Member States shall provide for the controller to entrust the data protection officer at least with the following tasks:

(a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to this Directive and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Directive, with other Union or Member State data protection provisions and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 27;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 28, and to consult, where appropriate, with regard to any other matter.

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 35

General principles for transfers of personal data

1. Member States shall provide for any transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation to take place, subject to compliance with the national provisions adopted pursuant to other provisions of this Directive, only where the conditions laid down in this Chapter are met, namely:

(a) the transfer is necessary for the purposes set out in Article 1(1);

(b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1);

(c) where personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in accordance with its national law;

(d) the Commission has adopted an adequacy decision pursuant to Article 36, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37, or, in the absence of an adequacy decision pursuant to Article 36 and of appropriate safeguards in accordance with Article 37, derogations for specific situations apply pursuant to Article 38; and

(e) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

2. Member States shall provide for transfers without the prior authorisation by another Member State in accordance with point (c) of paragraph 1 to be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

3. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Directive is not undermined.

Article 36

Transfers on the basis of an adequacy decision

1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide a mechanism for periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 58(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing

acts in accordance with the procedure referred to in Article 58(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. Member States shall provide for a decision pursuant to paragraph 5 to be without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 37 and 38.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

Article 37

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 36(3), Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where:

(a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

(b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

2. The controller shall inform the supervisory authority about categories of transfers under point (b) of paragraph 1.

3. When a transfer is based on point (b) of paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

Article 38

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 36, or of appropriate safeguards pursuant to Article 37, Member States shall provide that a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the condition that the transfer is necessary:

(a) in order to protect the vital interests of the data subject or another person;

(b) to safeguard legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides;

(c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;

(d) in individual cases for the purposes set out in Article 1(1); or

(e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1(1).

2. Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1.

3. Where a transfer is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

Article 39

Transfers of personal data to recipients established in third countries

1. By way of derogation from point (b) of Article 35(1) and without prejudice to any international agreement referred to in paragraph 2 of this Article, Union or Member State law may provide for the competent authorities referred to in point (7)(a) of Article 3, in individual and specific cases, to transfer personal data directly to recipients established in third countries only if the other provisions of this Directive are complied with and all of the following conditions are fulfilled:

(a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1);

(b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

(c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

(d) the authority that is competent for the purposes referred to in Article 1(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;

(e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation.

3. The transferring competent authority shall inform the supervisory authority about transfers under this Article.

4. Where a transfer is based on paragraph 1, such a transfer shall be documented.

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation.

3. The transferring competent authority shall inform the supervisory authority about transfers under this Article.

4. Where a transfer is based on paragraph 1, such a transfer shall be documented.

5. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Directive, in order to protect

the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and with the Commission in accordance with Chapter VII.

3. Member States may provide for a supervisory authority established under Regulation (EU) 2016/679 to be the supervisory authority referred to in this Directive and to assume responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

4. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which are to represent those authorities in the Board referred to in Article 51.

Article 40
International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Article 41
Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Directive, in order to protect

the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and with the Commission in accordance with Chapter VII.

3. Member States may provide for a supervisory authority established under Regulation (EU) 2016/679 to be the supervisory authority referred to in this Directive and to assume responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

4. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which are to represent those authorities in the Board referred to in Article 51.

Article 42
Independence

1. Each Member State shall provide for each supervisory authority to act with complete independence in performing its tasks and exercising its powers in accordance with this Directive.

2. Member States shall provide for the member or members of their supervisory authorities in the performance of their tasks and exercise of their powers in accordance with this Directive, to remain free from external influence, whether direct or indirect, and that they shall neither seek nor take instructions from anybody.

3. Members of Member States' supervisory authorities shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 43
General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

— their parliament;

— their government;

— their head of State; or

— an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform their duties and exercise their powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Section 1
Independent status

Article 41
Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Directive, in order to protect

the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and with the Commission in accordance with Chapter VII.

3. Member States may provide for a supervisory authority established under Regulation (EU) 2016/679 to be the supervisory authority referred to in this Directive and to assume responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

4. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which are to represent those authorities in the Board referred to in Article 51.

Article 44

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

- (a) the establishment of each supervisory authority;
- (b) the qualifications and eligibility conditions required to be appointed as a member of each supervisory authority;
- (c) the rules and procedures for the appointment of the member or members of each supervisory authority;
- (d) the duration of the term of the member or members of each supervisory authority of not less than four years, except for the first appointment after 6 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;
- (e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;
- (f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or the exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Directive.

Section 2

Competence, tasks and powers

Article 45

Competence

1. Each Member State shall provide for each supervisory authority to be competent for the performance of the tasks assigned to, and for the exercise of the powers conferred on, it in accordance with this Directive on the territory of its own Member State.

2. Each Member State shall provide for each supervisory authority not to be competent for the supervision of processing operations of courts when acting in their judicial capacity. Member States may provide for their supervisory authority not to be competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.

Article 46

Tasks

1. Each Member State shall provide, on its territory, for each supervisory authority to:

- (a) monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;
- (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;
- (c) Advise, in accordance with Member State law, the national parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
- (d) promote the awareness of controllers and processors of their obligations under this Directive;
- (e) upon request, provide information to any data subject concerning the exercise of their rights under this Directive and,

if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 55, and investigate, to the extent appropriate, the subject-matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;

(h) cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, with a view to ensuring the consistency of application and enforcement of this Directive;

(i) conduct investigations on the application of this Directive, including on the basis of information received from another supervisory authority or other public authority;

(j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(k) provide advice on the processing operations referred to in Article 28; and

(l) contribute to the activities of the Board.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer.

4. Where a request is manifestly unfounded or excessive, in particular because it is repetitive, the supervisory authority may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating that the request is manifestly unfounded or excessive.

Article 47

Powers

1. Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.

2. Each Member State shall provide by law for each supervisory authority to have effective corrective powers such as, for example:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions adopted pursuant to this Directive;

(b) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing pursuant to Article 16;

(c) to impose a temporary or definitive limitation, including a ban, on processing.

3. Each Member State shall provide by law for each supervisory authority to have effective advisory powers to advise the controller in accordance with the prior consultation procedure referred to in Article 28 and to issue, on its own initiative or on request, opinions to its national parliament and its government or, in accordance with its national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to

appropriate safeguards, including effective judicial remedy and due process, as set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law for each supervisory authority to have the power to bring infringements of provisions adopted pursuant to this Directive to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings, in order to enforce the provisions adopted pursuant to this Directive.

Article 48 Reporting of infringements

Member States shall provide for competent authorities to put in place effective mechanisms to encourage confidential reporting of infringements of this Directive.

Article 49 Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of penalties imposed. Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, the Commission and the Board.

CHAPTER VII Cooperation

Article 50 Mutual assistance

1. Each Member State shall provide for their supervisory authorities to provide each other with relevant information and mutual assistance in order to implement and apply this Directive in a consistent manner, and to put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.

2. Each Member States shall provide for each supervisory authority to take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Directive or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

Article 51 Tasks of the Board

1. The Board established by Regulation (EU) 2016/679 shall perform all of the following tasks in relation to processing within the scope of this Directive:

(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;

(b) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Directive and issue guidelines, recommendations and best practices in order to encourage consistent application of this Directive;

(c) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 47(1) and (3);

(d) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph for establishing personal data breaches and determining the undue delay referred to in Article 30(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(e) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons as referred to in Article 31(1);

(f) review the practical application of the guidelines, recommendations and best practices referred to in points (b) and (c);

(g) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country, a territory or one or more specified sectors within a third country, or an international organisation, including for the assessment whether such a third country, territory, specified sector, or international organisation no longer ensures an adequate level of protection;

(h) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(i) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(j) promote the exchange of knowledge and documentation on data protection law and practice with data protection supervisory authorities worldwide.

With regard to point (g) of the first subparagraph, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with the territory or specified sector within that third country, or with the international organisation.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations and best practices to the Commission and to the committee referred to in Article 58(1) and make them public.

4. The Commission shall inform the Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the Board.

CHAPTER VIII

Remedies, liability and penalties

Article 52

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.
2. Member States shall provide for the supervisory authority with which the complaint has been lodged to transmit it to the competent supervisory authority, without undue delay if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 45(1). The data subject shall be informed about the transmission.
3. Member States shall provide for the supervisory authority with which the complaint has been lodged to provide further assistance on request of the data subject.
4. The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 53.

Article 53

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Article 45(1) does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged pursuant to Article 52.
3. Member States shall provide for proceedings against a supervisory authority to be brought before the courts of the Member State where the supervisory authority is established.

Article 54

Right to an effective judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.

Article 55

Representation of data subjects

Member States shall, in accordance with Member State procedural law, provide for the data subject to have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Member State law, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 52, 53 and 54 on his or her behalf.

Article 56

Right to compensation

Member States shall provide for any person who has suffered material or non-material damage as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive to have the right to receive compensation for the damage suffered from the controller or any other authority competent under Member State law.

Article 57

Penalties

Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

CHAPTER IX
Implementing acts

Article 58

Committee procedure

1. The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER X
Final provisions

Article 59

Repeal of Framework Decision 2008/977/JHA

1. Framework Decision 2008/977/JHA is repealed with effect from 6 May 2018.
2. References to the repealed Decision referred to in paragraph 1 shall be construed as references to this Directive.

Article 60

Union legal acts already in force

The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected.

Article 61

Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force until amended, replaced or revoked.

Article 62

Commission reports

1. By 6 May 2022, and every four years thereafter, the Commission shall submit a report on the evaluation and review

of this Directive to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 36(3) and Article 39.

3. For the purposes of paragraphs 1 and 2, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Directive, in particular taking account of developments in information technology and in the light of the state of progress in the information society.

6. By 6 May 2019, the Commission shall review other legal acts adopted by the Union which regulate processing by the competent authorities for the purposes set out in Article 1(1) including those referred to in Article 60, in order to assess the need to align them with this Directive and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of this Directive.

Article 63

Transposition

1. Member States shall adopt and publish, by 6 May 2018, the laws, Regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from 6 May 2018.

When Member States adopt those provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. By way of derogation from paragraph 1, a Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.

3. By way of derogation from paragraphs 1 and 2 of this Article, a Member State may, in exceptional circumstances, bring an automated processing system as referred to in paragraph 2 of this Article into conformity with Article 25(1) within a specified period after the period referred to in paragraph 2 of this Article, if it would otherwise cause serious difficulties for the operation of that particular automated processing system. The Member State concerned shall notify the Commission of the grounds for those serious difficulties and the grounds for the specified period within which it shall bring that particular automated processing system into conformity with Article 25(1). The specified period shall in any event not be later than 6 May 2026.

4. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 64

Entry into force

This Directive shall enter into force on the day following that of its publication in the Official Journal of the European Union.

Article 65

Addressees

This Directive is addressed to the Member States.

Done at Brussels, 27 April 2016.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

J.A. HENNIS-PLASSCHAERT

(1) OJ C 391, 18.12.2012, p. 127.

(2) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.

(3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(4) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

(5) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (see page 1 of this Official Journal).

(6) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(7) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(8) Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).

(9) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

(10) Council Directive 77/249/EEC of 22 March 1977 to facilitate the effective exercise by lawyers of freedom to provide services (OJ L 78, 26.3.1977, p. 17).

(11) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(12) Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).

(13) Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, 12.7.2000, p. 1).

(14) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

(15) OJ L 176, 10.7.1999, p. 36.

(16) OJ L 53, 27.2.2008, p. 52.

(17) OJ L 160, 18.6.2011, p. 21.

(18) OJ C 192, 30.6.2012, p. 7.

X.E-Finance

Treaty on the Functioning of the European Union (relevant provisions connected with E-Finance)

[...]

TITLE V AREA OF FREEDOM, SECURITY AND JUSTICE

CHAPTER 4 JUDICIAL COOPERATION IN CRIMINAL MATTERS

Article 83

1. The European Parliament and the Council may, by means of Directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.

These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

[...]

CHAPTER 4 PROVISIONS SPECIFIC TO MEMBER STATES WHOSE CURRENCY IS THE EURO

Article 136

1. In order to ensure the proper functioning of economic and monetary union, and in accordance with the relevant provisions of the Treaties, the Council shall, in accordance with the relevant procedure from among those referred to in Articles 121 and 126, with the exception of the procedure set out in Article 126(14), adopt measures specific to those Member States whose currency is the euro:

(a) to strengthen the coordination and surveillance of their budgetary discipline;

(b) to set out economic policy guidelines for them, while ensuring that they are compatible with those adopted for the whole of the Union and are kept under surveillance.

2. For those measures set out in paragraph 1, only members of the Council representing Member States whose currency is the euro shall take part in the vote.

A qualified majority of the said members shall be defined in accordance with Article 238(3)(a).

[...]

Article 138

1. In order to secure the euro's place in the international monetary system, the Council, on a proposal from the Commission, shall adopt a decision establishing common

positions on matters of particular interest for economic and monetary union within the competent international financial institutions and conferences. The Council shall act after consulting the European Central Bank.

2. The Council, on a proposal from the Commission, may adopt appropriate measures to ensure unified representation within the international financial institutions and conferences. The Council shall act after consulting the European Central Bank.

3. For the measures referred to in paragraphs 1 and 2, only members of the Council representing Member States whose currency is the euro shall take part in the vote.

A qualified majority of the said members shall be defined in accordance with Article 238(3)(a).

CHAPTER 5 TRANSITIONAL PROVISIONS

Article 139

1. Member States in respect of which the Council has not decided that they fulfil the necessary conditions for the adoption of the euro shall hereinafter be referred to as 'Member States with a derogation'.

2. The following provisions of the Treaties shall not apply to Member States with a derogation:

(a) adoption of the parts of the broad economic policy guidelines which concern the euro area generally (Article 121(2));

(b) coercive means of remedying excessive deficits (Article 126(9) and (11));

(c) the objectives and tasks of the ESCB (Article 127(1) to (3) and (5));

(d) issue of the euro (Article 128);

(e) acts of the European Central Bank (Article 132);

(f) measures governing the use of the euro (Article 133);

(g) monetary agreements and other measures relating to exchange-rate policy (Article 219);

(h) appointment of members of the Executive Board of the European Central Bank (Article 283(2));

(i) decisions establishing common positions on issues of particular relevance for economic and monetary union within the competent international financial institutions and conferences (Article 138(1));

(j) measures to ensure unified representation within the international financial institutions and conferences (Article 138(2)).

In the Articles referred to in points (a) to (j), 'Member States' shall therefore mean Member States whose currency is the euro.

3. Under Chapter IX of the Statute of the ESCB and of the ECB, Member States with a derogation and their national central banks are excluded from rights and obligations within the ESCB.

4. The voting rights of members of the Council representing Member States with a derogation shall be suspended for the adoption by the Council of the measures referred to in the Articles listed in paragraph 2, and in the following instances:

(a) recommendations made to those Member States whose currency is the euro in the framework of multilateral

surveillance, including on stability programmes and warnings (Article 121(4));
(b) measures relating to excessive deficits concerning those Member States whose currency is the euro (Article 126(6), (7), (8), (12) and (13)).

A qualified majority of the other members of the Council shall be defined in accordance with Article 238(3)(a).

Article 140

1. At least once every two years, or at the request of a Member State with a derogation, the Commission and the European Central Bank shall report to the Council on the progress made by the Member States with a derogation in fulfilling their obligations regarding the achievement of economic and monetary union. These reports shall include an examination of the compatibility between the national legislation of each of these Member States, including the statutes of its national central bank, and Articles 130 and 131 and the Statute of the ESCB and of the ECB. The reports shall also examine the achievement of a high degree of sustainable convergence by reference to the fulfilment by each Member State of the following criteria:

— the achievement of a high degree of price stability; this will be apparent from a rate of inflation which is close to that of, at most, the three best performing Member States in terms of price stability,

— the sustainability of the government financial position; this will be apparent from having achieved a government budgetary position without a deficit that is excessive as determined in accordance with Article 126(6),

— the observance of the normal fluctuation margins provided for by the exchange-rate mechanism of the European Monetary System, for at least two years, without devaluing against the euro,

— the durability of convergence achieved by the Member State with a derogation and of its participation in the exchange-rate mechanism being reflected in the long-term interest-rate levels. The four criteria mentioned in this paragraph and the relevant periods over which they are to be respected are developed further in a Protocol annexed to the Treaties. The reports of the Commission and the European Central Bank shall also take account of the results of the integration of markets, the situation and development of the balances of payments on current account and an examination of the development of unit labour costs and other price indices.

2. After consulting the European Parliament and after discussion in the European Council, the Council shall, on a proposal from the Commission, decide which Member States with a derogation fulfil the necessary conditions on the basis of the criteria set out in paragraph 1, and abrogate the derogations of the Member States concerned.

The Council shall act having received a recommendation of a qualified majority of those among its members representing Member States whose currency is the euro. These members shall act within six months of the Council receiving the Commission's proposal.

The qualified majority of the said members, as referred to in the second subparagraph, shall be defined in accordance with Article 238(3)(a).

3. If it is decided, in accordance with the procedure set out in paragraph 2, to abrogate a derogation, the Council shall, acting with the unanimity of the Member States whose currency is the euro and the Member State concerned, on a proposal from the Commission and after consulting the European Central Bank, irrevocably fix the rate at which the euro shall be substituted for the currency of the Member State concerned, and take the other measures necessary for the introduction of the euro as the single currency in the Member State concerned.

Article 141

1. If and as long as there are Member States with a derogation, and without prejudice to Article 129(1), the General Council of the European Central Bank referred to in Article 44 of the Statute of the ESCB and of the ECB shall be constituted as a third decision-making body of the European Central Bank.

2. If and as long as there are Member States with a derogation, the European Central Bank shall, as regards those Member States:

— strengthen cooperation between the national central banks,

— strengthen the coordination of the monetary policies of the Member States, with the aim of ensuring price stability,

— monitor the functioning of the exchange-rate mechanism,

— hold consultations concerning issues falling within the competence of the national central banks and affecting the stability of financial institutions and markets,

— carry out the former tasks of the European Monetary Cooperation Fund which had subsequently been taken over by the European Monetary Institute.

Article 142

Each Member State with a derogation shall treat its exchange-rate policy as a matter of common interest. In so doing, Member States shall take account of the experience acquired in cooperation within the framework of the exchange-rate mechanism.

(Editorial note: More articles of this treaty may be found in the part I. E-Commerce.)

Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services (“DMFS” Directive)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 47(2), Article 55 and Article 95 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

(1) It is important, in the context of achieving the aims of the single market, to adopt measures designed to consolidate progressively this market and those measures must contribute to attaining a high level of consumer protection, in accordance with Articles 95 and 153 of the Treaty.

(2) Both for consumers and suppliers of financial services, the distance marketing of financial services will constitute one of

the main tangible results of the completion of the internal market.

(3) Within the framework of the internal market, it is in the interest of consumers to have access without discrimination to the widest possible range of financial services available in the Community so that they can choose those that are best suited to their needs. In order to safeguard freedom of choice, which is an essential consumer right, a high degree of consumer protection is required in order to enhance consumer confidence in distance selling.

(4) It is essential to the smooth operation of the internal market for consumers to be able to negotiate and conclude contracts with a supplier established in other Member States, regardless of whether the supplier is also established in the Member State in which the consumer resides.

(5) Because of their intangible nature, financial services are particularly suited to distance selling and the establishment of a legal framework governing the distance marketing of financial services should increase consumer confidence in the use of new techniques for the distance marketing of financial services, such as electronic commerce.

(6) This Directive should be applied in conformity with the Treaty and with secondary law, including Directive 2000/31/EC (4) on electronic commerce, the latter being applicable solely to the transactions which it covers.

(7) This Directive aims to achieve the objectives set forth above without prejudice to Community or national law governing freedom to provide services or, where applicable, host Member State control and/or authorisation or supervision systems in the Member States where this is compatible with Community legislation.

(8) Moreover, this Directive, and in particular its provisions relating to information about any contractual clause on law applicable to the contract and/or on the competent court does not affect the applicability to the distance marketing of consumer financial services of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters (5) or of the 1980 Rome Convention on the law applicable to contractual obligations.

(9) The achievement of the objectives of the Financial Services Action Plan requires a higher level of consumer protection in certain areas. This implies a greater convergence, in particular, in non harmonised collective investment funds, rules of conduct applicable to investment services and consumer credits. Pending the achievement of the above convergence, a high level of consumer protection should be maintained.

(10) Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (6), lays down the main rules applicable to distance contracts for goods or services concluded between a supplier and a consumer. However, that Directive does not cover financial services.

(11) In the context of the analysis conducted by the Commission with a view to ascertaining the need for specific measures in the field of financial services, the Commission invited all the interested parties to transmit their comments, notably in connection with the preparation of its Green Paper entitled 'Financial Services — Meeting Consumers' Expectations'. The consultations in this context showed that there is a need to strengthen consumer protection in this area. The Commission therefore decided to present a specific proposal concerning the distance marketing of financial services.

(12) The adoption by the Member States of conflicting or different consumer protection rules governing the distance marketing of consumer financial services could impede the functioning of the internal market and competition between firms in the market. It is therefore necessary to enact common rules at Community level in this area, consistent with no reduction in overall consumer protection in the Member States.

(13) A high level of consumer protection should be guaranteed by this Directive, with a view to ensuring the free movement of financial services. Member States should not be able to adopt provisions other than those laid down in this Directive in the fields it harmonises, unless otherwise specifically indicated in it.

[...]

(15) Contracts negotiated at a distance involve the use of means of distance communication which are used as part of a distance sales or service-provision scheme not involving the simultaneous presence of the supplier and the consumer. The constant development of those means of communication requires principles to be defined that are valid even for those means which are not yet in widespread use. Therefore, distance contracts are those the offer, negotiation and conclusion of which are carried out at a distance.

(16) A single contract involving successive operations or separate operations of the same nature performed over time may be subject to different legal treatment in the different Member States, but it is important that this Directive be applied in the same way in all the Member States. To that end, it is appropriate that this Directive should be considered to apply to the first of a series of successive operations or separate operations of the same nature performed over time which may be considered as forming a whole, irrespective of whether that operation or series of operations is the subject of a single contract or several successive contracts.

(17) An 'initial service agreement' may be considered to be for example the opening of a bank account, acquiring a credit card, concluding a portfolio management contract, and 'operations' may be considered to be for example the deposit or withdrawal of funds to or from the bank account, payment by credit card, transactions made within the framework of a portfolio management contract. Adding new elements to an initial service agreement, such as a possibility to use an electronic payment instrument together with one's existing bank account, does not constitute an 'operation' but an additional contract to which this Directive applies. The subscription to new units of the same collective investment fund is considered to be one of 'successive operations of the same nature'.

[...]

(19) The supplier is the person providing services at a distance. This Directive should however also apply when one of the marketing stages involves an intermediary. Having regard to the nature and degree of that involvement, the pertinent provisions of this Directive should apply to such an intermediary, irrespective of his or her legal status.

(20) Durable mediums include in particular floppy discs, CD-ROMs, DVDs and the hard drive of the consumer's computer on which the electronic mail is stored, but they do not include Internet websites unless they fulfil the criteria contained in the definition of a durable medium.

(21) The use of means of distance communications should not lead to an unwarranted restriction on the information provided to the client. In the interests of transparency this Directive lays down the requirements needed to ensure that an appropriate level of information is provided to the consumer both before and after conclusion of the contract. The consumer should receive, before conclusion of the contract, the prior information needed so as to properly appraise the financial service offered to him and hence make a well-informed choice. The supplier should specify how long his offer applies as it stands.

(22) Information items listed in this Directive cover information of a general nature applicable to all kinds of financial services. Other information requirements concerning a given financial service, such as the coverage of an insurance policy, are not solely specified in this Directive. This kind of information should be provided in accordance, where applicable, with relevant Community legislation or national legislation in conformity with Community law.

(23) With a view to optimum protection of the consumer, it is important that the consumer is adequately informed of the

provisions of this Directive and of any codes of conduct existing in this area and that he has a right of withdrawal.

(24) When the right of withdrawal does not apply because the consumer has expressly requested the performance of a contract, the supplier should inform the consumer of this fact.

(25) Consumers should be protected against unsolicited services. Consumers should be exempt from any obligation in the case of unsolicited services, the absence of a reply not being construed as signifying consent on their part. However, this rule should be without prejudice to the tacit renewal of contracts validly concluded between the parties whenever the law of the Member States permits such tacit renewal.

(26) Member States should take appropriate measures to protect effectively consumers who do not wish to be contacted through certain means of communication or at certain times. This Directive should be without prejudice to the particular safeguards available to consumers under Community legislation concerning the protection of personal data and privacy.

(27) With a view to protecting consumers, there is a need for suitable and effective complaint and redress procedures in the Member States with a view to settling potential disputes between suppliers and consumers, by using, where appropriate, existing procedures.

(28) Member States should encourage public or private bodies established with a view to settling disputes out of court to cooperate in resolving cross-border disputes. Such cooperation could in particular entail allowing consumers to submit to extra-judicial bodies in the Member State of their residence complaints concerning suppliers established in other Member States. The establishment of FIN-NET offers increased assistance to consumers when using cross-border services.

(29) This Directive is without prejudice to extension by Member States, in accordance with Community law, of the protection provided by this Directive to non-profit organisations and persons making use of financial services in order to become entrepreneurs.

(30) This Directive should also cover cases where the national legislation includes the concept of a consumer making a binding contractual statement.

[...]

(32) The Community and the Member States have entered into commitments in the context of the General Agreement on Trade in Services (GATS) concerning the possibility for consumers to purchase banking and investment services abroad. The GATS entitles Member States to adopt measures for prudential reasons, including measures to protect investors, depositors, policy-holders and persons to whom a financial service is owed by the supplier of the financial service. Such measures should not impose restrictions going beyond what is required to ensure the protection of consumers.

(33) In view of the adoption of this Directive, the scope of Directive 97/7/EC and Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests (7) and the scope of the cancellation period in Council Directive 90/619/EEC of 8 November 1990 on the coordination of laws, Regulations and administrative provisions relating to direct life assurance, laying down provisions to facilitate the effective exercise of freedom to provide services (8) should be adapted.

(34) Since the objectives of this Directive, namely the establishment of common rules on the distance marketing of consumer financial services cannot be sufficiently achieved by the Member States and can therefore be better achieved at Community level, the Community may adopt measures, in accordance with the principles of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary to achieve that objective,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Object and scope

1. The object of this Directive is to approximate the laws, Regulations and administrative provisions of the Member States concerning the distance marketing of consumer financial services.

2. In the case of contracts for financial services comprising an initial service agreement followed by successive operations or a series of separate operations of the same nature performed over time, the provisions of this Directive shall apply only to the initial agreement.

In case there is no initial service agreement but the successive operations or the separate operations of the same nature performed over time are performed between the same contractual parties, Articles 3 and 4 apply only when the first operation is performed. Where, however, no operation of the same nature is performed for more than one year, the next operation will be deemed to be the first in a new series of operations and, accordingly, Articles 3 and 4 shall apply.

Article 2

Definitions

For the purposes of this Directive:

(a) 'distance contract' means any contract concerning financial services concluded between a supplier and a consumer under an organised distance sales or service-provision scheme run by the supplier, who, for the purpose of that contract, makes exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded;

(b) 'financial service' means any service of a banking, credit, insurance, personal pension, investment or payment nature;

(c) 'supplier' means any natural or legal person, public or private, who, acting in his commercial or professional capacity, is the contractual provider of services subject to distance contracts;

(d) 'consumer' means any natural person who, in distance contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession;

(e) 'means of distance communication' refers to any means which, without the simultaneous physical presence of the supplier and the consumer, may be used for the distance marketing of a service between those parties;

(f) 'durable medium' means any instrument which enables the consumer to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;

(g) 'operator or supplier of a means of distance communication' means any public or private, natural or legal person whose trade, business or profession involves making one or more means of distance communication available to suppliers.

Article 3

Information to the consumer prior to the conclusion of the distance contract

1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning:

(1) the supplier

(a) the identity and the main business of the supplier, the geographical address at which the supplier is established and any other geographical address relevant for the customer's relations with the supplier;

(b) the identity of the representative of the supplier established in the consumer's Member State of residence and the geographical address relevant for the customer's relations with the representative, if such a representative exists;

(c) when the consumer's dealings are with any professional other than the supplier, the identity of this professional, the capacity in which he is acting vis-à-vis the consumer, and the geographical address relevant for the customer's relations with this professional;

(d) where the supplier is registered in a trade or similar public register, the trade register in which the supplier is entered and his registration number or an equivalent means of identification in that register;

(e) where the supplier's activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;

(2) the financial service

(a) a description of the main characteristics of the financial service;

(b) the total price to be paid by the consumer to the supplier for the financial service, including all related fees, charges and expenses, and all taxes paid via the supplier or, when an exact price cannot be indicated, the basis for the calculation of the price enabling the consumer to verify it;

(c) where relevant notice indicating that the financial service is related to instruments involving special risks related to their specific features or the operations to be executed or whose price depends on fluctuations in the financial markets outside the supplier's control and that historical performances are no indicators for future performances;

(d) notice of the possibility that other taxes and/or costs may exist that are not paid via the supplier or imposed by him;

(e) any limitations of the period for which the information provided is valid;

(f) the arrangements for payment and for performance;

(g) any specific additional cost for the consumer of using the means of distance communication, if such additional cost is charged;

(3) the distance contract

(a) the existence or absence of a right of withdrawal in accordance with Article 6 and, where the right of withdrawal exists, its duration and the conditions for exercising it, including information on the amount which the consumer may be required to pay on the basis of Article 7(1), as well as the consequences of non-exercise of that right;

(b) the minimum duration of the distance contract in the case of financial services to be performed permanently or recurrently;

(c) information on any rights the parties may have to terminate the contract early or unilaterally by virtue of the terms of the distance contract, including any penalties imposed by the contract in such cases;

(d) practical instructions for exercising the right of withdrawal indicating, inter alia, the address to which the notification of a withdrawal should be sent;

(e) the Member State or States whose laws are taken by the supplier as a basis for the establishment of relations with the consumer prior to the conclusion of the distance contract;

(f) any contractual clause on law applicable to the distance contract and/or on competent court;

(g) in which language, or languages, the contractual terms and conditions, and the prior information referred to in this Article are supplied, and furthermore in which language, or languages, the supplier, with the agreement of the consumer, undertakes to communicate during the duration of this distance contract;

(4) redress

(a) whether or not there is an out-of-court complaint and redress mechanism for the consumer that is party to the distance contract and, if so, the methods for having access to it;

(b) the existence of guarantee funds or other compensation arrangements, not covered by Directive 94/19/EC of the European Parliament and of the Council of 30 May 1994 on deposit guarantee schemes (9) and Directive 97/9/EC of the European Parliament and of the Council of 3 March 1997 on investor compensation schemes (10).

2. The information referred to in paragraph 1, the commercial purpose of which must be made clear, shall be provided in a clear and comprehensible manner in any way appropriate to the means of distance communication used, with due regard, in particular, to the principles of good faith in commercial transactions, and the principles governing the protection of

those who are unable, pursuant to the legislation of the Member States, to give their consent, such as minors.

3. In the case of voice telephony communications

(a) the identity of the supplier and the commercial purpose of the call initiated by the supplier shall be made explicitly clear at the beginning of any conversation with the consumer;

(b) subject to the explicit consent of the consumer only the following information needs to be given:

— the identity of the person in contact with the consumer and his link with the supplier,

— a description of the main characteristics of the financial service,

— the total price to be paid by the consumer to the supplier for the financial service including all taxes paid via the supplier or, when an exact price cannot be indicated, the basis for the calculation of the price enabling the consumer to verify it,

— notice of the possibility that other taxes and/or costs may exist that are not paid via the supplier or imposed by him,

— the existence or absence of a right of withdrawal in accordance with Article 6 and, where the right of withdrawal exists, its duration and the conditions for exercising it, including information on the amount which the consumer may be required to pay on the basis of Article 7(1).

The supplier shall inform the consumer that other information is available on request and of what nature this information is. In any case the supplier shall provide the full information when he fulfils his obligations under Article 5.

4. Information on contractual obligations, to be communicated to the consumer during the pre-contractual phase, shall be in conformity with the contractual obligations which would result from the law presumed to be applicable to the distance contract if the latter were concluded.

Article 4

Additional information requirements

1. Where there are provisions in the Community legislation governing financial services which contain prior information requirements additional to those listed in Article 3(1), these requirements shall continue to apply.

2. Pending further harmonisation, Member States may maintain or introduce more stringent provisions on prior information requirements when the provisions are in conformity with Community law.

3. Member States shall communicate to the Commission national provisions on prior information requirements under paragraphs 1 and 2 of this Article when these requirements are additional to those listed in Article 3(1). The Commission shall take account of the communicated national provisions when drawing up the report referred to in Article 20(2).

4. The Commission shall, with a view to creating a high level of transparency by all appropriate means, ensure that information, on the national provisions communicated to it, is made available to consumers and suppliers.

▼M2

5. Where Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market (11) is also applicable, the information provisions under Article 3(1) of this Directive, with the exception of paragraphs (2)(c) to (g), (3)(a), (d) and (e), and (4)(b), shall be replaced with Articles 36, 37, 41 and 42 of that Directive.

▼B

Article 5

Communication of the contractual terms and conditions and of the prior information

1. The supplier shall communicate to the consumer all the contractual terms and conditions and the information referred to in Article 3(1) and Article 4 on paper or on another durable medium available and accessible to the consumer in good time before the consumer is bound by any distance contract or offer.

2. The supplier shall fulfil his obligation under paragraph 1 immediately after the conclusion of the contract, if the

contract has been concluded at the consumer's request using a means of distance communication which does not enable providing the contractual terms and conditions and the information in conformity with paragraph 1.

3. At any time during the contractual relationship the consumer is entitled, at his request, to receive the contractual terms and conditions on paper. In addition, the consumer is entitled to change the means of distance communication used, unless this is incompatible with the contract concluded or the nature of the financial service provided.

Article 6

Right of withdrawal

1. The Member States shall ensure that the consumer shall have a period of 14 calendar days to withdraw from the contract without penalty and without giving any reason. However, this period shall be extended to 30 calendar days in distance contracts relating to life insurance covered by Directive 90/619/EEC and personal pension operations.

The period for withdrawal shall begin:

- either from the day of the conclusion of the distance contract, except in respect of the said life assurance, where the time limit will begin from the time when the consumer is informed that the distance contract has been concluded, or
- from the day on which the consumer receives the contractual terms and conditions and the information in accordance with Article 5(1) or (2), if that is later than the date referred to in the first indent.

Member States, in addition to the right of withdrawal, may provide that the enforceability of contracts relating to investment services is suspended for the same period provided for in this paragraph.

2. The right of withdrawal shall not apply to:

(a) financial services whose price depends on fluctuations in the financial market outside the suppliers control, which may occur during the withdrawal period, such as services related to:

- foreign exchange,
 - money market instruments,
 - transferable securities,
 - units in collective investment undertakings,
 - financial-futures contracts, including equivalent cash-settled instruments,
 - forward interest-rate agreements (FRAs),
 - interest-rate, currency and equity swaps,
 - options to acquire or dispose of any instruments referred to in this point including equivalent cash-settled instruments.
- This category includes in particular options on currency and on interest rates;

(b) travel and baggage insurance policies or similar short-term insurance policies of less than one month's duration;

(c) contracts whose performance has been fully completed by both parties at the consumer's express request before the consumer exercises his right of withdrawal.

3. Member States may provide that the right of withdrawal shall not apply to:

(a) any credit intended primarily for the purpose of acquiring or retaining property rights in land or in an existing or projected building, or for the purpose of renovating or improving a building, or

(b) any credit secured either by mortgage on immovable property or by a right related to immovable property, or

(c) declarations by consumers using the services of an official, provided that the official confirms that the consumer is guaranteed the rights under Article 5(1).

This paragraph shall be without prejudice to the right to a reflection time to the benefit of the consumers that are resident in those Member States where it exists, at the time of the adoption of this Directive.

4. Member States making use of the possibility set out in paragraph 3 shall communicate it to the Commission.

5. The Commission shall make available the information communicated by Member States to the European Parliament and the Council and shall ensure that it is also available to consumers and suppliers who request it.

6. If the consumer exercises his right of withdrawal he shall, before the expiry of the relevant deadline, notify this following the practical instructions given to him in accordance with Article 3(1)(3)(d) by means which can be proved in accordance with national law. The deadline shall be deemed to have been observed if the notification, if it is on paper or on another durable medium available and accessible to the recipient, is dispatched before the deadline expires.

7. This Article does not apply to credit agreements cancelled under the conditions of Article 6(4) of Directive 97/7/EC or Article 7 of Directive 94/47/EC of the European Parliament and of the Council of 26 October 1994 on the protection of purchasers in respect of certain aspects of contracts relating to the purchase of the right to use immovable properties on a timeshare basis (12).

If to a distance contract of a given financial service another distance contract has been attached concerning services provided by the supplier or by a third party on the basis of an agreement between the third party and the supplier, this additional distance contract shall be cancelled, without any penalty, if the consumer exercises his right of withdrawal as provided for in Article 6(1).

8. The provisions of this Article are without prejudice to the Member States' laws and Regulations governing the cancellation or termination or non-enforceability of a distance contract or the right of a consumer to fulfil his contractual obligations before the time fixed in the distance contract. This applies irrespective of the conditions for and the legal effects of the winding-up of the contract.

Article 7

Payment of the service provided before withdrawal

1. When the consumer exercises his right of withdrawal under Article 6(1) he may only be required to pay, without any undue delay, for the service actually provided by the supplier in accordance with the contract. The performance of the contract may only begin after the consumer has given his approval. The amount payable shall not:

- exceed an amount which is in proportion to the extent of the service already provided in comparison with the full coverage of the contract,
- in any case be such that it could be construed as a penalty.

2. Member States may provide that the consumer cannot be required to pay any amount when withdrawing from an insurance contract.

3. The supplier may not require the consumer to pay any amount on the basis of paragraph 1 unless he can prove that the consumer was duly informed about the amount payable, in conformity with Article 3(1)(3)(a). However, in no case may he require such payment if he has commenced the performance of the contract before the expiry of the withdrawal period provided for in Article 6(1) without the consumer's prior request.

4. The supplier shall, without any undue delay and no later than within 30 calendar days, return to the consumer any sums he has received from him in accordance with the distance contract, except for the amount referred to in paragraph 1. This period shall begin from the day on which the supplier receives the notification of withdrawal.

5. The consumer shall return to the supplier any sums and/or property he has received from the supplier without any undue delay and no later than within 30 calendar days. This period shall begin from the day on which the consumer dispatches the notification of withdrawal.

▼M2 —————

▼M1

Article 9

Given the prohibition of inertia selling practices laid down in Directive 2005/29/EC of 11 May 2005 of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (13) and without prejudice to the provisions of Member States' legislation on the tacit renewal of distance contracts, when such rules permit tacit renewal, Member States shall take

measures to exempt the consumer from any obligation in the event of unsolicited supplies, the absence of a reply not constituting consent.

▼B

Article 10

Unsolicited communications

1. The use by a supplier of the following distance communication techniques shall require the consumer's prior consent:

(a) automated calling systems without human intervention (automatic calling machines);
(b) fax machines.

2. Member States shall ensure that means of distance communication other than those referred to in paragraph 1, when they allow individual communications:

(a) shall not be authorised unless the consent of the consumers concerned has been obtained, or
(b) may only be used if the consumer has not expressed his manifest objection.

3. The measures referred to in paragraphs 1 and 2 shall not entail costs for consumers.

Article 11

Sanctions

Member States shall provide for appropriate sanctions in the event of the supplier's failure to comply with national provisions adopted pursuant to this Directive.

They may provide for this purpose in particular that the consumer may cancel the contract at any time, free of charge and without penalty.

These sanctions must be effective, proportional and dissuasive.

Article 12

Imperative nature of this Directive's provisions

1. Consumers may not waive the rights conferred on them by this Directive.

2. Member States shall take the measures needed to ensure that the consumer does not lose the protection granted by this Directive by virtue of the choice of the law of a non-member country as the law applicable to the contract, if this contract has a close link with the territory of one or more Member States.

Article 13

Judicial and administrative redress

1. Member States shall ensure that adequate and effective means exist to ensure compliance with this Directive in the interests of consumers.

2. The means referred to in paragraph 1 shall include provisions whereby one or more of the following bodies, as determined by national law, may take action in accordance

with national law before the courts or competent administrative bodies to ensure that the national provisions for the implementation of this Directive are applied:

(a) public bodies or their representatives;

(b) consumer organisations having a legitimate interest in protecting consumers;

(c) professional organisations having a legitimate interest in acting.

3. Member States shall take the measures necessary to ensure that operators and suppliers of means of distance communication put an end to practices that have been declared to be contrary to this Directive, on the basis of a judicial decision, an administrative decision or a decision issued by a supervisory authority notified to them, where those operators or suppliers are in a position to do so.

Article 14

Out-of-court redress

1. Member States shall promote the setting up or development of adequate and effective out-of-court complaints and redress procedures for the settlement of consumer disputes concerning financial services provided at distance.

2. Member States shall, in particular, encourage the bodies responsible for out-of-court settlement of disputes to cooperate in the resolution of cross-border disputes concerning financial services provided at distance.

Article 15

Burden of proof

Without prejudice to Article 7(3), Member States may stipulate that the burden of proof in respect of the supplier's obligations to inform the consumer and the consumer's consent to conclusion of the contract and, where appropriate, its performance, can be placed on the supplier.

Any contractual term or condition providing that the burden of proof of the respect by the supplier of all or part of the obligations incumbent on him pursuant to this Directive should lie with the consumer shall be an unfair term within the meaning of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (14).

[...]

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 23

Addressees

This Directive is addressed to the Member States.

Amended by:

		Official Journal		
		No	page	date
►M1	Directive 2005/29/EC of the European Parliament and of the Council Text with EEA relevance of 11 May 2005	L 149	22	11.6.2005
►M2	Directive 2007/64/EC of the European Parliament and of the Council Text with EEA relevance of 13 November 2007	L 319	1	5.12.2007

Relevant Case Law on Durable Medium and Information Providing in e-Finance

**E-4/09 Inconsult Anstalt vs the Financial Market
Authority (Finanzmarktaufsicht, Liechtenstein)**

1 By a decision dated 27 March 2009, the Appeals Commission of the Financial Market Authority (hereinafter "the Appeals Commission") made a request for an Advisory Opinion, registered at the Court on 14 April 2009 on a question concerning the interpretation of Article 2(12) in Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation, hereinafter "the Directive".

2 This question has arisen in a case pending before the Appeals Commission between Inconsult Anstalt (hereinafter "the Appellant") and the Financial Market Authority of Liechtenstein (hereinafter "the Defendant"). The case concerns a dispute on whether the Appellant has complied with certain information obligations as stated in Articles 13 and 15 of the Act of 17 May 2006 on Insurance Mediation (Gesetz vom 17. Mai 2006 über die Versicherungsvermittlung, hereinafter "the VersVermG") and the Regulation of 27 June 2006 on Insurance Mediation (Verordnung vom 27. Juni 2006 über die Versicherungsvermittlung, hereinafter "the VersVermV").

3 The Appellant, a private entity incorporated under Liechtenstein law, received on 29 May 2007 a licence from the Defendant to operate as an insurance intermediary in the form of a broker.

4 On 25 November 2008, following an on-site audit on the premises of the Appellant, the Defendant issued an order requiring the Appellant to comply with information obligations laid down in Articles 13 and 15 of the VersVermG.

5 The Appellant brought an action before the Appeals Commission on 6 February 2009, in which it contested the order of the Defendant in its entirety and submitted that it had satisfied the information obligations under Articles 13 and 15 of the VersVermG by means of operating a website.

6 According to Article 15(1) of the VersVermG, an insurance intermediary is required to provide a customer with the information described, *inter alia*, in Article 13 of the VersVermG, in writing on paper or on another "durable medium". What constitutes a durable medium is defined in Article 12 of the VersVermV, which implements Article 2(12) of the Directive.

7 The request of the Appeals Commission concerns the following question: What are the criteria by which an Internet site may be regarded as constituting a "durable medium", as it is to be understood under Article 2(12) of Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation?

The Appeals Commission particularly highlights the following points:

- Do the criteria in the first paragraph of Article 2(12) of the Directive entail that only password-protected Internet sites are covered by the term "durable medium" or that the customer must be sent a link to a particular Internet address?

- Is it necessary that the relevant Internet site is "personally" addressed to a particular person in such a way that only that person can access the Internet site?

- Is it necessary for the customer to have expressly consented (in writing) to the information being provided via the Internet?

- What are the criteria to be applied in order to establish that particular information was accessible unchanged over a particular period of time?

- What is an "adequate" period of time and how can it be established/proved that the information was accessible unchanged over such an adequate period of time?

8 In answer to a written question from the Court, the Financial Market Authority, whose order is the subject of the dispute in the case at hand, confirmed that it is headed by Mr René H. Melliger who, since 2002, has also served as a member of the EFTA Board of Auditors, the body responsible for auditing the

Court's financial statement. This relation between one of the parties to the case before the national court and the Court could cause concerns as to the neutrality of the judges required under Article 15 of the Court's Statute.

9 At the hearing, the agent of the Principality of Liechtenstein stated that the mandate of Mr Melliger as a member of the EFTA Board of Auditors would terminate at the end of 2009 and would not be renewed. The Court's Financial Statements for 2008 have been approved by the EFTA Board of Auditors. As Mr Melliger will not participate in the audit of the Court's financial statement for 2009, the Court has come to the conclusion that there are no sufficient grounds for the judges to recuse themselves *en banc* from the case pursuant to Article 15 of the Court's Statute.

II Legal Background

National law

[...]

EEA law

17 Directive 2002/92/EC was incorporated in to the EEA Agreement as point 13b of Annex IX thereto by Decision No 115/2003 of the EEA Joint Committee, which entered into force on 1 May 2004.

18 In Articles 12 and 13, the Directive sets out certain information requirements for insurance intermediaries which apply prior to the conclusion of insurance contracts, as well as up on their amendment and renewal. Article 12 of the Directive reads:

Information provided by the insurance intermediary

1. Prior to the conclusion of any initial insurance contract, and, if necessary, upon amendment or renewal thereof, an insurance intermediary shall provide the customer with at least the following information:

(a) his identity and address;

(b) the register in which he has been included and the means for verifying that he has been registered;

(c) whether he has a holding, direct or indirect, representing more than 10 % of the voting rights or of the capital in a given insurance undertaking;

(d) whether a given insurance undertaking or parent undertaking of a given insurance undertaking has a holding, direct or indirect, representing more than 10 % of the voting rights or of the capital in the insurance intermediary;

(e) the procedures referred to in Article 10 allowing customers and other interested parties to register complaints about insurance and reinsurance intermediaries and, if appropriate, about the out-of-court complaint and redress procedures referred to in Article 11.

...

19 Article 13 of the Directive reads:

1. All information to be provided to customers in accordance with Article 12 shall be communicated:

(a) on paper or on any other durable medium available and accessible to the customer;

(b) in a clear and accurate manner, comprehensible to the customer;

(c) in an official language of the Member State of the commitment or in any other language agreed by the parties.

2. By way of derogation from paragraph 1(a), the information referred to in Article 12 may be provided orally where the customer requests it, or where immediate cover is necessary. In those cases, the information shall be provided to the customer in accordance with paragraph 1 immediately after the conclusion of the insurance contract.

3. In the case of telephone selling, the prior information given to the customer shall be in accordance with Community rules applicable to the distance marketing of consumer financial services. Moreover, information shall be provided to the customer in accordance with paragraph 1 immediately after the conclusion of the insurance contract.

20 The term "durable medium" is defined in Article 2(12) of the Directive which reads: 'durable medium' means any instrument which enables the customer to store information

addressed personally to him in a way accessible for future reference for a period of time adequate to the purposes of the information and which allows the unchanged reproduction of the information stored. In particular, durable medium covers floppy disks, CD-ROMs, DVDs and hard drives of personal computers on which electronic mail is stored, but it excludes Internet sites, unless such sites meet the criteria specified in the first paragraph.

21 Reference is made to the Report for the Hearing for a fuller account of the legal framework, the facts, the procedure and the written observations submitted to the Court, which are mentioned or discussed hereinafter only insofar as is necessary for the reasoning of the Court.

III

Findings of the Court

Admissibility

22 Under Article 34 of the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice (hereinafter “the SCA”), any court or tribunal in an EFTA State may refer questions on the interpretation of the EEA Agreement to the Court, if it considers it necessary to enable it to give judgment.

23 In order to determine whether a referring body qualifies as a court or tribunal within the meaning of Article 34 SCA the Court takes account of a number of factors. These include whether the referring body is established by law, has a permanent existence, exercises binding jurisdiction, applies rules of law, is independent and, as the case may be, whether its procedure is *inter partes* and similar to the procedure in court, see Case E-1/94 Restamark [1994–95] EFTA Ct. Rep. 15, at paragraph 24 et seq. and Joined Cases E-8/94 and E-9/94 Mattel and Lego [1994–95] EFTA Ct. Rep. 113, at paragraph 15. For comparison, see also C-54/96 Dorsch Consult [1997] ECR I-4961, at paragraph 23 and C-178/99 Salzmann [2001] ECR I-4421, at paragraph 13.

24 The composition and powers of the Appeals Commission are defined in the legislative provisions described at paragraphs 11–13 above. According to those provisions, the Appeals Commission is established by law and has a permanent character. As regards its independence, the provisions of the Liechtenstein Constitution mentioned at paragraph 11 and the provisions of the FMAG mentioned at paragraphs 12–13 demonstrate that the Appeals Commission gives rulings, without receiving any instructions and in total impartiality, on decisions adopted by the Financial Market Authority. In this respect the Appeals Commission has a status separate from the authority which adopted the decision under appeal. As is apparent from the documents of the case, the procedure before the Appeals Commission is *inter partes*. Thus, the Court finds that the Appeals Commission exercises a judicial function and qualifies as a court or tribunal within the meaning of Article 34 SCA.

General remarks

25 The request of the referring court contains an adequate description of the facts in order for the Court to give a reply. However, the order for reference does not contain specific information on the nature and function of the Internet site by which the Appellant claims to have fulfilled the requirements of the VersVermG to provide the customer with information on a “durable medium”.

26 The Appellant simply claims that all the requisite statutory information is to be found on its website, from which every customer can download the relevant documents and/or print these out and file them away for their own information needs. The Appellant argues furthermore that all files printed from the website are automatically marked with the date of printing. In the Appellant’s view, the storage and/or provision of the relevant information on the website fulfils the requirement of providing information on a “durable medium”.

27 By its question, the referring court essentially asks under what conditions an Internet site can constitute a “durable medium” within the meaning of Article 2(12) of the Directive.

28 According to Recital 8 of the preamble to the Directive, the coordination of national provisions on professional requirements and registration of persons taking up and pursuing the activity of insurance mediation can contribute both to the completion of the single market for financial services and to the enhancement of customer protection in this field.

29 For the purposes of consumer protection, the Directive sets out certain minimum obligations on the information which insurance intermediaries must provide to their customers (see Article 12 of the Directive). Article 13(1)(a) of the Directive requires that all information provided to customers in accordance with Article 12 must be communicated on “paper or on any other durable medium available and accessible to the customer”.

30 By requiring information provided under Article 12 of the Directive to be communicated in a certain form, Article 13(1)(a) facilitates the subsequent verification of the information which an intermediary has provided to his customer. Furthermore, such a requirement enables the customer to access the information at a later stage and resort to it, if needed in order to protect his interests.

31 According to the second subparagraph of Article 2(12) of the Directive, in principle, an Internet site may constitute a “durable medium” within the meaning of that Article, provided that the conditions laid down in the first subparagraph of the Article are met.

32 In view of the question referred to the Court and the manner in which the case has been argued, it seems appropriate to address those conditions as follows: The Internet site in question must constitute an instrument which (a) enables the customer to store information addressed personally to him, (b) enables him to store such information in a way accessible for future reference for a period of time adequate to the purposes of the information, and (c) allows for the unchanged reproduction of the information stored.

33 In this respect, the instruments listed as examples of durable media in the second subparagraph of Article 2(12) provide guidance as to the substance of those conditions. The second subparagraph of Article 2(12) of the Directive specifically defines floppy disks, CD-ROMs, DVDs and hard drives of personal computers on which electronic mail is stored as durable media. The instrument must enable the customer to store information addressed personally to him.

34 The first criterion under Article 2(12) of the Directive is that the instrument in question must enable a customer to store information which is addressed personally to that customer.

35 The parties submitting observations to the Court on that point have commented upon the notion of “information addressed personally” to the customer. The Federal Republic of Germany, ESA and the European Commission address this mainly from the perspective of content, raising the question whether that phrase means that the information must be of personal relevance to the customer and not of such a general character that it concerns all customers. The Czech Republic and the Republic of Estonia approach the issue primarily from the perspective of accessibility, that is, whether or not information on an Internet site freely accessible to the general public may qualify as “addressed personally” to a particular customer. In that respect, the Czech Republic argues that information may be considered personally addressed even if freely accessible to the public, whereas the Republic of Estonia argues that this requirement may be met if a customer has his own personal account on a webpage, accessible via a secure personal password.

36 The Court notes that the case before the Appeals Commission concerns the alleged failure by the Appellant to provide on a “durable medium” the information listed in Article 13 of the VersVermG, which corresponds to Article 12(1) of Directive 2002/92/EC. Under Article 15 of the VersVermG, an insurance intermediary is required to provide this information to his customers either in writing or on another “durable medium”. Article 12 VersVermV defines

“durable medium” in the same way as Article 2(12) of the Directive. Thus, within the framework of the present case, it is clear what kind of information must be provided either in writing or on a “durable medium”. It is clear, furthermore, that this includes information, such as the address of the insurance intermediary, which has the same content regardless of whether published on a website as information freely accessible to the general public or as a message accessible only to a specific customer.

37 The issue whether information published on a website freely accessible to the general public may qualify as information “personally addressed” to that customer, is linked to the obligation, also included under Article 12(1) of the Directive, to “provide the customer with” the information required. In relation to the present Directive, the notion of “information addressed personally” to the customer in Article 2(12) refers, in effect, to the information which must be provided to a customer under Article 12.

38 This question is linked also to another element of Article 2(12), that is, that the customer himself must be able to store this information. This requirement, in turn, is functionally linked to the third criterion, concerning unchanged reproduction. Based on the information which the Court has received, it appears difficult to conceive of a website which allows such unchanged reproduction without there having been first some kind of personalised message to the customer containing or referring to the information in question. In this respect, the Court refers to its observations at paragraphs 61–67 below.

39 In the light of the above, in relation to the first criterion under Article 2(12), it suffices to conclude that in order to qualify as a “durable medium” within the meaning of Article 2(12) of Directive 2002/92/EC, a website must enable the customer to store the information listed in Article 12 of the Directive. Accessibility for a period of time adequate to the purposes of the information

40 The second criterion is that the instrument in question enables the customer to store the information provided to him in a way accessible for future reference for a period of time adequate to the purposes of the information.

41 The Czech Republic, the Republic of Estonia, the Federal Republic of Germany and ESA are all of the view that this period must cover the duration of the legal relationship between the customer and the service provider.

42 As regards the accessibility of information supplied prior to the conclusion of a contract, the Czech Republic submits that the period must cover the time from when negotiations on the future contract begin until the moment when no doubt remains that no contract will be concluded with the customer concerned. In a similar vein, the Federal Republic of Germany argues that this period covers, at any rate, the duration of contractual negotiations.

43 In relation to the accessibility of information after the termination of a contract, the Czech Republic, the Republic of Estonia, the Federal Republic of Germany and ESA all agree that for purposes of customer protection and the purpose of informing the customer of redress possibilities in case of a dispute, such information should also be accessible after the termination of the contract. The Republic of Estonia submits that account must be taken of the period during which a dispute might arise between the parties, which may depend on national provisions on time limits for bringing legal action.

44 With regard to the question of what period of accessibility is adequate to the purposes of the information, the Court finds that the information must be accessible for as long as it is relevant to the customer in order to protect his interests stemming from his relations with the insurance intermediary. The length of this period will depend upon the content of the information, the contractual relationship and the circumstances of the case. Thus, the period of accessibility may cover both the time during which contractual negotiations were conducted, even if not resulting in the conclusion of an insurance contract, and the period during which an insurance contract concluded is in force.

Furthermore, in order to allow a customer, where necessary, to seek redress, the adequate period of accessibility may also cover the period after such a contract has lapsed.

45 The Court further notes that, as is clear from Article 12(5) of the Directive and Recital 19 of the preamble, the Directive establishes only minimum requirements regarding the information to be provided to customers. Thus, the content to be provided under the national provisions on information, which may differ from one EEA State to another, may affect the length of the adequate period of accessibility.

46 Consequently, the second criterion under Article 2(12) must be understood to mean that in order to qualify as a “durable medium”, an Internet site must enable the customer to store the information required under Article 12 of the Directive in a way which makes it accessible for a period of time adequate to the purposes of the information, that is, for as long as it is relevant for the customer in order to protect his interests stemming from his relations with the insurance intermediary. This may cover the time during which contractual negotiations were conducted even if not resulting in the conclusion of an insurance contract, the period during which an insurance contract is in force and, to the extent necessary, the period after such a contract has lapsed. Unchanged reproduction of the information stored

47 The third criterion is that the instrument must allow for the unchanged reproduction of the information stored.

48 The Czech Republic argues in this regard that an intermediary who intends to use his website as a durable medium for the purposes of the Directive must ensure that he stores the original version of the information and makes such accessible to the customer. If he changes the information, he must indicate clearly when exactly the change took place.

49 The Republic of Estonia argues that it is important that the stored information on the durable medium does not change to the disadvantage of the customer, generally considered to be the weaker party to a contractual relationship. It notes that while, in principle, it is possible to store the information on a website unchanged, for a customer it is difficult to ascertain whether or not the administrator controlling the website has amended the information. In view of the difficulties to obtain evidence in that respect, the Republic of Estonia suggests that customers be required to print out the information or store it on their personal hard drives in order to prove the content of the original information. In that situation, the website itself may not constitute a durable medium but a means through which information is stored on another durable medium.

50 The Republic of Estonia further remarks that as a result of technological progress it may become feasible to prove the unchanged nature of information on a webpage. In that case, the website itself would constitute a durable medium, although it remains for the competent court to assess this in an individual case. Moreover, in order for a website to constitute a durable medium, the relevant information must be in a form which enables the customer to reproduce it independently later, regardless of the actions of third parties. Consequently, this criterion is not met when the web administrator reproduces the information for the customer.

51 The Federal Republic of Germany argues that it follows from a schematic consideration of Article 2(12) and Article 13(1) of the Directive that the customer has to be able to reproduce the information unchanged. This is because the provision of information required by Article 13(1) aims to ensure that the customer may access this information as a contracting partner of the insurance intermediary. In the view of the Federal Republic of Germany, the unchanged reproduction of the information stored is generally not guaranteed in the case of an insurance intermediary’s Internet site, since the intermediary may change the information or amend its content at any time.

52 The Federal Republic of Germany argues that since it must be possible to reproduce the information for a period of time adequate to the purposes of the information, one cannot be guided by whether the information was provided on an Internet site for an adequate period of time in an unchanged

form in an individual case. In line with the argument presented by the Republic of Estonia, the Federal Republic of Germany argues that this would lead to considerable difficulties of proof, both for the insurance intermediary and the customer. In particular, a customer wishing to read the information on the Internet during the period of time regarded as adequate could never be sure that the information is unchanged and complete because he is neither informed of any amendment to the information nor has the possibility to make a comparison.

53 The Federal Republic of Germany submits further that the possibility of unchanged reproduction would exist in the case of an intermediary's corporate Internet site only if a mandatory framework was present guaranteeing that the customer could reproduce unchanged the information provided on the Internet site. This could take the form, for example, of an undertaking by the intermediary to provide information on his Internet site in a form that cannot be changed by the intermediary himself, which the customer may access at any time for a period adequate to the purposes of the information. To the knowledge of the Federal Republic of Germany, this cannot currently be ensured, neither legally nor technically. It notes that the Appeals Commission gives no indication of any special legal or technical obligations on the insurance intermediary concerned.

54 Nevertheless, in the view of the Federal Republic of Germany, an insurance intermediary's Internet site is not completely unsuitable for the provision of information within the meaning of Article 13 of the Directive. While it does not in itself fulfil the requirements of a durable medium within the meaning of Article 2(12), an Internet site can provide the customer with the possibility of storing information from the site on a medium in the customer's domain. If this medium allows the customer to make an unchanged reproduction of the information stored for a period of time adequate to the purposes of the information, the information is available to the customer on a durable medium.

55 ESA submits that from examining the elements that make up the definition of a durable medium, it is clear that the purpose of providing information on such a medium is to ensure that the customer can easily document the information which he has been provided, and that the insurance intermediary cannot alter it without the customer's consent. ESA argues that it follows from this that "ordinary" websites (see paragraph 56 below) cannot be regarded as durable media, since such websites normally may be changed by those who operate them, whereas the purpose of storing information on a durable medium is to ensure that it cannot be changed unilaterally.

56 ESA observes that the European Securities Markets Expert Group (hereinafter "ESME") issued a report on the concept of a "durable medium" in 2007 (Report of 11 July 2007 on Durable Medium - Distance Marketing Directive and Markets in Financial Instruments Directive). In that report, ESME concluded that ordinary websites, which are frequently changed and from which the user cannot necessarily save or print pages, cannot be regarded as durable media. ESA notes that the report examined the concept of durable medium as used in certain provisions of Directive 2002/65/EC concerning the distance marketing of consumer financial services and Directive 2004/39/EC on markets in financial instruments. Both those Directives contain the same definition of durable medium as the Directive at issue in the present case. In ESA's view, the concept should be interpreted uniformly in all these instruments.

57 ESA points out that the ESME report considers that "sophisticated" websites may constitute durable media. This category of websites can be divided into two sub-categories: (i) those that act as portals for the provision of information in another durable medium, and (ii) those that may actually constitute durable media themselves. The first type of sophisticated website allows users to access information which can be either printed off or copied and stored on an external drive. The information may be reproduced,

therefore, on a durable medium, either paper or movable disk, even if the website itself does not constitute a durable medium.

58 According to ESA, the ESME report describes the second type of sophisticated website as containing secure storage areas for individual users which are accessed by a user code and password. This type of storage can be compared to a user's own hard disk, except that in this case he can access the information remotely via the Internet.

59 ESA shares the opinion presented in the ESME report that a website that provides secure and individual personal storage areas continuously available to users could be considered to constitute a durable medium within the meaning of Article 2(12) of the Directive. ESA considers that it would be incumbent on the insurance intermediary to demonstrate that the technical solutions used by him ensure that his website fulfils the conditions for constituting a durable medium.

60 The European Commission concurs with the views expressed in the ESME report. It adds that other technological solutions may be found in the future which will similarly enable a website to comply with the requirements laid down in Article 2(12) of Directive 2002/92/EC and thus constitute a durable medium.

61 The Court notes that according to Recital 8 of the preamble to the Directive, one of the key objectives of the Directive is to enhance protection for consumers concluding insurance contracts via insurance intermediaries.

This means, *inter alia*, that it must be possible for consumers to make an informed decision prior to the conclusion of an initial insurance contract or upon its amendment or renewal, and thereby to protect their interests in case of a conflict with the intermediary. To that end, consumers must be able to reproduce the information unchanged, which in the Court's view means that the information provided must be stored in a way that makes it impossible for the insurance intermediary to change it unilaterally.

62 There may be several technical methods available for guaranteeing unchanged reproduction. It is for the insurance intermediary in each case to ensure that the methods of electronic communication he employs permit this kind of reproduction.

63 As pointed out by ESA and the European Commission, a distinction may be made between "ordinary" websites on the one hand and "sophisticated" websites on the other. An ordinary website serves as a dynamic electronic host or portal for the provision of information which, generally, may freely be changed by the website proprietor. The Court finds that a website which exhibits these characteristics, including freedom for the proprietor to change the content, does not meet the requirements laid down in the first subparagraph of Article 2(12) of the Directive with respect to guaranteeing unchanged reproduction. Therefore, it cannot be regarded as durable medium within the meaning of that Article.

64 With regard to sophisticated websites, a further distinction must be made between those sophisticated websites that act as a portal for the provision of information on another instrument which can qualify as a durable medium and those sophisticated websites that may actually constitute durable media themselves.

65 The first type of sophisticated website in essence allows the user to access information, for example in the form of an e-mail with an attachment, which he can copy and store on his own computer. For this method to constitute the communication to the customer of information on a durable medium, as required under Article 13(1)(a) of the Directive, the website must contain features which will lead the customer almost certainly to either secure the information on paper or to store it on another durable medium.

66 The second type of sophisticated website contains a secure storage area for individual users which is accessed by a user code and password. Provided that this method of storing information excludes any possibility of the insurance

intermediary changing the information, this kind of storage can be compared to the user's own hard drive. The only difference is that the customer can access the information remotely via the Internet. The Court finds that this type of sophisticated website fulfils the requirement of guaranteeing unchanged reproduction necessary to qualify as a durable medium within the meaning of Article 2(12) of the Directive. 67 It cannot be ruled out that other technological solutions may similarly enable a website to comply with requirements laid down in Article 2(12) of the Directive, including the condition of securing unchanged reproduction of information. This is an assessment which must be made based on the characteristics of the technology in question. It is not for the Court, within the framework of the present case, to specify which particular technological solutions may be acceptable in that regard. The Court therefore limits itself to concluding that in order to qualify as a "durable medium", an Internet site must allow for the unchanged reproduction of the information stored, that is, the information must be stored in a way that makes it impossible for the insurance intermediary to change it unilaterally.

No requirement for consent

68 Concerning the referring court's question on the relevance of the customer consenting to receive the information via the Internet, the Court notes that Article 13(1)(a) of the Directive grants an insurance intermediary the option to choose whether to provide the required information to the customer "on paper or on any other durable medium". By contrast, Article 3(1) of Directive 2006/73/EC implementing Directive 2004/39/EC as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive makes the communication of information on a durable medium other than paper dependent upon satisfying specific conditions, inter alia, that "... (b) the person to whom the information is to be provided, when offered the choice between information on paper or in that other durable medium, specifically chooses the provision of the information in that other medium". Therefore, in relation to the question raised in the case at hand, it is irrelevant whether the customer has expressly consented to the provision of information through the Internet.

IV Costs

69 The costs incurred by the Principality of Liechtenstein, the Czech Republic, the Republic of Estonia, the Federal Republic of Germany, ESA and the European Commission, which have submitted observations to the Court, are not recoverable. Since these proceedings are a step in the proceedings before the Financial Appeals Commission, any decision on costs for the parties to those proceedings is a matter for that court.

On those grounds,

THE COURT

in answer to the question referred to it by the Financial Appeals Commission hereby gives the following Advisory Opinion:

1. In order for an Internet site to qualify as a "durable medium" within the meaning of Article 2(12) of Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation, it must enable the customer to store the information listed in Article 12 of the Directive.
2. In order to qualify as a "durable medium", an Internet site must enable the customer to store the information required under Article 12 of the Directive in a way which makes it accessible for a period of time adequate to the purposes of the information, that is, for as long as it is relevant for the customer in order to protect his interests stemming from his relations with the insurance intermediary. This may cover the time during which contractual negotiations were conducted even if not resulting in the conclusion of an insurance contract, the period during which an insurance contract is in force and, to the extent necessary, the period after such a contract has lapsed.
3. In order to qualify as a "durable medium", an Internet site must allow for the unchanged reproduction of the information stored, that is, the information must be stored in a way that makes it impossible for the insurance intermediary to change it unilaterally.
4. In order for an Internet site to qualify as a "durable medium", it is irrelevant whether the customer has expressly consented to the provision of information through the Internet.

Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC ("PSD2" Directive)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Central Bank (1),
Having regard to the opinion of the European Economic and Social Committee (2),
Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) In recent years, significant progress has been achieved in integrating retail payments in the Union, in particular in the context of the Union acts on payments, in particular through Directive 2007/64/EC of the European Parliament and of the Council (4), Regulation (EC) No 924/2009 of the European Parliament and of the Council (5), Directive 2009/110/EC of the European Parliament and of the Council (6), and Regulation (EU) No 260/2012 of the European Parliament and of the Council (7). Directive 2011/83/EU of the European Parliament and of the Council (8) has further complemented the legal framework for payment services by setting a specific limit on the ability of retailers to surcharge their customers for the use of a given means of payment.

(2) The revised Union legal framework on payment services is complemented by Regulation (EU) 2015/751 of the European

Parliament and of the Council (9). That Regulation introduces, in particular, rules on the charging of interchange fees for card-based transactions and aims to further accelerate the achievement of an effective integrated market for card-based payments.

(3) Directive 2007/64/EC was adopted in December 2007 on the basis of a Commission proposal of December 2005. Since then, the retail payments market has experienced significant technical innovation, with rapid growth in the number of electronic and mobile payments and the emergence of new types of payment services in the market place, which challenges the current framework.

[...]

(5) The continued development of an integrated internal market for safe electronic payments is crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market.

(6) New rules should be established to close the regulatory gaps while at the same time providing more legal clarity and ensuring consistent application of the legislative framework across the Union. Equivalent operating conditions should be guaranteed, to existing and new players on the market, enabling new means of payment to reach a broader market, and ensuring a high level of consumer protection in the use of those payment services across the Union as a whole. This should generate efficiencies in the payment system as a whole and lead to more choice and more transparency of payment services while strengthening the trust of consumers in a harmonised payments market.

(7) In recent years, the security risks relating to electronic payments have increased. This is due to the growing technical complexity of electronic payments, the continuously growing volumes of electronic payments worldwide and emerging types of payment services. Safe and secure payment services constitute a vital condition for a well-functioning payment services market. Users of payment services should therefore be adequately protected against such risks. Payment services are essential for the functioning of vital economic and social activities.

[...]

(10) This Directive introduces a neutral definition of acquiring of payment transactions in order to capture not only the traditional acquiring models structured around the use of payment cards, but also different business models, including those where more than one acquirer is involved. This should ensure that merchants receive the same protection, regardless of the payment instrument used, where the activity is the same as the acquiring of card transactions. Technical services provided to payment service providers, such as the mere processing and storage of data or the operation of terminals, should not be considered to constitute acquiring. Moreover, some acquiring models do not provide for an actual transfer of funds by the acquirer to the payee because the parties may agree upon other forms of settlement.

[...]

(16) The exclusion relating to certain payment transactions by means of telecom or information technology devices should focus specifically on micro-payments for digital content and voice-based services. A clear reference to payment transactions for the purchase of electronic tickets should be introduced to take into account the development in payments where, in particular, customers can order, pay for, obtain and validate electronic tickets from any location and at any time using mobile phones or other devices. Electronic tickets allow and facilitate the delivery of services that consumers could otherwise purchase in paper ticket form and include transport, entertainment, car parking, and entry to venues, but exclude physical goods. They thus reduce the production and distribution costs connected with traditional paper-based ticketing channels and increase customer convenience by providing new and simple ways to purchase tickets. In order to ease the burden on entities that collect charitable donations,

payment transactions in relation to such donations should also be excluded.

[...]

(24) It is necessary to specify the categories of payment service providers which may legitimately provide payment services throughout the Union, namely, credit institutions which take deposits from users that can be used to fund payment transactions and which should continue to be subject to the prudential requirements laid down in Directive 2013/36/EU of the European Parliament and of the Council (10), electronic money institutions which issue electronic money that can be used to fund payment transactions and which should continue to be subject to the prudential requirements laid down in Directive 2009/110/EC, payment institutions and post office giro institutions which are so entitled under national law. The application of that legal framework should be confined to service providers who provide payment services as a regular occupation or business activity in accordance with this Directive.

(25) This Directive lays down rules on the execution of payment transactions where the funds are electronic money as defined in Directive 2009/110/EC. This Directive does not, however, regulate the issuance of electronic money as provided for in Directive 2009/110/EC. Therefore, payment institutions should not be allowed to issue electronic money.

[...]

(27) Since the adoption of Directive 2007/64/EC new types of payment services have emerged, especially in the area of internet payments. In particular, payment initiation services in the field of e-commerce have evolved. Those payment services play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's account servicing payment service provider in order to initiate internet payments on the basis of a credit transfer.

(28) Moreover, technological developments have given rise to the emergence of a range of complementary services in recent years, such as account information services. Those services provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider. The payment service user is thus able to have an overall view of its financial situation immediately at any given moment. Those services should also be covered by this Directive in order to provide consumers with adequate protection for their payment and account data as well as legal certainty about the status of account information service providers.

(29) Payment initiation services enable the payment initiation service provider to provide comfort to a payee that the payment has been initiated in order to provide an incentive to the payee to release the goods or to deliver the service without undue delay. Such services offer a low-cost solution for both merchants and consumers and provide consumers with a possibility to shop online even if they do not possess payment cards. Since payment initiation services are currently not subject to Directive 2007/64/EC, they are not necessarily supervised by a competent authority and are not required to comply with Directive 2007/64/EC. This raises a series of legal issues, such as consumer protection, security and liability as well as competition and data protection issues, in particular regarding protection of the payment service users' data in accordance with Union data protection rules. The new rules should therefore respond to those issues.

(30) The personalised security credentials used for secure customer authentication by the payment service user or by the payment initiation service provider are usually those issued by the account servicing payment service providers. Payment initiation service providers do not necessarily enter into a contractual relationship with the account servicing payment service providers and, regardless of the business model used by the payment initiation service providers, the account servicing payment service providers should make it possible for payment initiation service providers to rely on the authentication

procedures provided by the account servicing payments service providers to initiate a specific payment on behalf of the payer.

(31) When exclusively providing payment initiation services, the payment initiation service provider does not at any stage of the payment chain hold the user's funds. When a payment initiation service provider intends to provide payment services in relation to which it holds user funds, it should obtain full authorisation for those services.

(32) Payment initiation services are based on direct or indirect access for the payment initiation service provider to the payer's account. An account servicing payment service provider which provides a mechanism for indirect access should also allow direct access for the payment initiation service providers.

[...]

(35) Payment initiation service providers and account information service providers, when exclusively providing those services, do not hold client funds. Accordingly, it would be disproportionate to impose own funds requirements on those new market players. Nevertheless, it is important that they be able to meet their liabilities in relation to their activities. They should therefore be required to hold either professional indemnity insurance or a comparable guarantee. EBA should develop guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 on the criteria to be used by Member States to establish the minimum monetary amount of professional indemnity insurance or comparable guarantee. EBA should not differentiate between professional indemnity insurance and a comparable guarantee, as they should be interchangeable.

[...]

(37) Provision should be made for payment service user funds to be kept separate from the payment institution's funds. Safeguarding requirements are necessary when a payment institution is in possession of payment service user funds. Where the same payment institution executes a payment transaction for both the payer and the payee and a credit line is provided to the payer, it might be appropriate to safeguard the funds in favour of the payee once they represent the payee's claim towards the payment institution. Payment institutions should also be subject to effective anti-money laundering and anti-terrorist financing requirements.

[...]

(48) In view of the specific nature of the activity performed and the risks connected to the provision of account information services, it is appropriate to provide for a specific prudential regime for account information service providers. Account information service providers should be allowed to provide services on a cross-border basis, benefiting from the 'passporting' rules.

[...]

(57) In practice, framework contracts and the payment transactions covered by them are far more common and economically significant than single payment transactions. If there is a payment account or a specific payment instrument, a framework contract is required. Therefore, the requirements for prior information on framework contracts should be comprehensive and information should always be provided on paper or on another durable medium, such as printouts by account printers, CD-ROMs, DVDs, the hard drives of personal computers on which electronic mail can be stored, and internet sites, provided that such sites are accessible for future reference, for a sufficient period of time for the purposes of accessing the information and provided that these sites allow the reproduction of the information stored there in an unaltered form. However, it should be possible for the payment service provider and the payment service user to agree in the framework contract on the manner in which subsequent information on executed payment transactions is to be given, for instance, that in internet banking, all information on the payment account be made available online.

[...]

(60) The way in which the required information is to be given by the payment service provider to the payment service user

should take into account the needs of the latter as well as practical technical aspects and cost-efficiency depending on the situation with regard to the agreement in the respective payment service contract. This Directive should therefore distinguish between two ways in which information is to be given by the payment service provider: either the information should be provided, i.e. actively communicated by the payment service provider at the appropriate time as required by this Directive without any prompting by the payment service user, or the information should be made available to the payment service user on the basis of a request for further information. In the second situation, the payment service user should take active steps in order to obtain the information, such as requesting it explicitly from the payment service provider, logging into a bank account mail box or inserting a bank card into a printer for account statements. For such purposes the payment service provider should ensure that access to the information is possible and that the information is available to the payment service user.

(61) The consumer should receive basic information on executed payment transactions at no additional charge. In the case of a single payment transaction the payment service provider should not charge separately for that information. Similarly, subsequent information on payment transactions under a framework contract should also be provided on a monthly basis free of charge. However, taking into account the importance of transparency in pricing and differing customer needs, the parties should be able to agree on charges for more frequent or additional information. In order to take into account different national practices, Member States should be able to require that monthly statements of payment accounts on paper or in another durable medium are always to be given free of charge.

(62) In order to facilitate customer mobility, it should be possible for consumers to terminate a framework contract without incurring charges. However, for contracts terminated by the consumer less than 6 months after their entry into force, payment service providers should be allowed to apply charges in line with the costs incurred due to the termination of the framework contract by the consumer. For consumers, the period of notice agreed should be no longer than 1 month, and for payment service providers no shorter than 2 months. This Directive should be without prejudice to the payment service provider's obligation to terminate the payment service contract in exceptional circumstances under other relevant Union or national law, such as that on money laundering or terrorist financing, any action targeting the freezing of funds, or any specific measure linked to the prevention and investigation of crimes.

(63) In order to ensure a high level of consumer protection, Member States should, in the interests of the consumer, be able to maintain or introduce restrictions or prohibitions on unilateral changes in the conditions of a framework contract, for instance if there is no justified reason for such a change.

[...]

(68) The use of a card or card-based payment instrument for making a payment often triggers the generation of a message confirming availability of funds and two resulting payment transactions. The first transaction takes place between the issuer and the merchant's account servicing payment service provider, while the second, usually a direct debit, takes place between the payer's account servicing payment service provider and the issuer. Both transactions should be treated in the same way as any other equivalent transactions. Payment service providers issuing card-based payment instruments should enjoy the same rights and should be subject to the same obligations under this Directive, regardless of whether or not they are the account servicing payment service provider of the payer, in particular in terms of responsibility (e.g. authentication) and liability vis-à-vis the different actors in the payment chain. Since the payment service provider's request and the confirmation on the availability of the funds can be made through existing secure communication channels, technical procedures and infrastructure for communication

between payment initiation service providers or account information service providers and account servicing payment service providers, while respecting the necessary security measures, there should be no additional costs for payment services providers or cardholders. Furthermore, whether the payment transaction takes place in an internet environment (the merchant's website), or in retail premises, the account servicing payment service provider should be obliged to provide the confirmation requested by the issuer only where accounts held by the account servicing payment service providers are electronically accessible for that confirmation at least online. Given the specific nature of electronic money, it should not be possible to apply that mechanism to payment transactions initiated through card-based payment instruments on which electronic money, as defined in Directive 2009/110/EC, is stored.

(69) The obligation to keep personalised security credentials safe is of the utmost importance to protect the funds of the payment service user and to limit the risks relating to fraud and unauthorised access to the payment account. However, terms and conditions or other obligations imposed by payment service providers on payment service users in relation to keeping personalised security credentials safe should not be drafted in a way that prevents payment service users from taking advantage of services offered by other payment service providers, including payment initiation services and account information services. Furthermore, such terms and conditions should not contain any provisions that would make it more difficult, in any way, to use the payment services of other payment service providers authorised or registered pursuant to this Directive.

(70) In order to reduce the risks and consequences of unauthorised or incorrectly executed payment transactions, the payment service user should inform the payment service provider as soon as possible about any contestations concerning allegedly unauthorised or incorrectly executed payment transactions, provided that the payment service provider has fulfilled its information obligations under this Directive. If the notification deadline is met by the payment service user, the payment service user should be able to pursue those claims subject to national limitation periods. This Directive should not affect other claims between payment service users and payment service providers.

(71) In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer. In order to protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount has been debited. In order to provide an incentive for the payment service user to notify, without undue delay, the payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a very limited amount, unless the payment service user has acted fraudulently or with gross negligence. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not in a position to become aware of the loss, theft or misappropriation of the payment instrument. Moreover, once users have notified a payment service provider that their payment instrument may have been compromised, payment service users should not be required to cover any further losses stemming from unauthorised use of that instrument. This Directive should be without prejudice to payment service providers' responsibility for technical security of their own products.

(72) In order to assess possible negligence or gross negligence on the part of the payment service user, account should be

taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered to be null and void. Moreover, in specific situations and in particular where the payment instrument is not present at the point of sale, such as in the case of online payments, it is appropriate that the payment service provider be required to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases.

(73) Provision should be made for the allocation of losses in the case of unauthorised payment transactions. Different provisions may apply to payment service users who are not consumers, since such users are normally in a better position to assess the risk of fraud and take countervailing measures. In order to ensure a high level of consumer protection, payers should always be entitled to address their claim to a refund to their account servicing payment service provider, even where a payment initiation service provider is involved in the payment transaction. This is without prejudice to the allocation of liability between the payment service providers.

(74) In the case of payment initiation services, rights and obligations of the payment service users and of the payment service providers involved should be appropriate to the service provided. Specifically, the allocation of liability between the payment service provider servicing the account and the payment initiation service provider involved in the transaction should compel them to take responsibility for the respective parts of the transaction that are under their control.

(75) This Directive aims to increase consumer protection in cases of card-based payment transactions where the exact transaction amount is not known at the moment when the payer gives consent to execute the payment transaction, for example at automatic fuelling stations, in car rental contracts or when making hotel reservations. The payer's payment service provider should be able to block funds on the payer's payment account only if the payer has given consent to the exact amount of the funds to be blocked and those funds should be released without undue delay after receipt of the information concerning the exact amount of the payment transaction and at the latest immediately after receipt of the payment order.

[...]

(80) It is essential, for the fully integrated straight-through processing of payments and for legal certainty with respect to the fulfilment of any underlying obligation between payment service users, that the full amount transferred by the payer should be credited to the account of the payee. Accordingly, it should not be possible for any of the intermediaries involved in the execution of payment transactions to make deductions from the amount transferred. However, it should be possible for payees to enter into an agreement with their payment service provider which allows the latter to deduct its own charges. Nevertheless, in order to enable the payee to verify that the amount due is correctly paid, subsequent information provided on the payment transaction should indicate not only the full amount of funds transferred, but also the amount of any charges that have been deducted.

(81) Low-value payment instruments should be a cheap and easy-to-use alternative in the case of low-priced goods and services and should not be overburdened by excessive requirements. The relevant information requirements and rules on their execution should therefore be limited to essential information, also taking into account the technical capabilities that can justifiably be expected from instruments dedicated to low-value payments. Despite the lighter regime, payment service users should have adequate protection, having regard

to the limited risks posed by those payment instruments, especially with regard to prepaid payment instruments.

(82) In order to improve the efficiency of payments throughout the Union, all payment orders initiated by the payer and denominated in euro or the currency of a Member State whose currency is not the euro, including credit transfers and money remittances, should be subject to a maximum 1-day execution time. For all other payments, such as payments initiated by or through a payee, including direct debits and card payments, in the absence of an explicit agreement between the payment service provider and the payer setting a longer execution time, the same 1-day execution time should apply. It should be possible to extend those periods by 1 additional business day, if a payment order is given on paper, to allow the continued provision of payment services to consumers who are used only to paper documents. When a direct debit scheme is used the payee's payment service provider should transmit the collection order within the time limits agreed between the payee and the payment service provider, enabling settlement on the agreed due date. In view of the fact that payment infrastructures are often highly efficient and in order to prevent any deterioration in current service levels, Member States should be allowed to maintain or establish rules specifying an execution time shorter than 1 business day, where appropriate.

(83) The provisions on execution for the full amount and execution time should constitute good practice where one of the payment service providers is not located in the Union.

(84) In order to strengthen the trust of consumers in a harmonised payment market, it is essential for payment service users to know the real costs and charges of payment services in order to make their choice. Accordingly, the use of non-transparent pricing methods should be prohibited, since it is commonly accepted that those methods make it extremely difficult for users to establish the real price of the payment service. Specifically, the use of value dating to the disadvantage of the user should not be permitted.

[...]

(89) Provision of payment services by the payment services providers may entail processing of personal data. Directive 95/46/EC of the European Parliament and of the Council (22), the national rules which transpose Directive 95/46/EC and Regulation (EC) No 45/2001 of the European Parliament and of the Council (23) are applicable to the processing of personal data for the purposes of this Directive. In particular, where personal data is processed for the purposes of this Directive, the precise purpose should be specified, the relevant legal basis referred to, the relevant security requirements laid down in Directive 95/46/EC complied with, and the principles of necessity, proportionality, purpose limitation and proportionate data retention period respected. Also, data protection by design and data protection by default should be embedded in all data processing systems developed and used within the framework of this Directive.

(90) This Directive respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, including the right to respect for private and family life, the right to protection of personal data, the freedom to conduct a business, the right to an effective remedy and the right not to be tried or punished twice in criminal proceedings for the same offence. This Directive must be implemented in accordance with those rights and principles.

(91) Payment service providers are responsible for security measures. Those measures need to be proportionate to the security risks concerned. Payment service providers should establish a framework to mitigate risks and maintain effective incident management procedures. A regular reporting mechanism should be established, to ensure that payment service providers provide the competent authorities, on a regular basis, with an updated assessment of their security risks and the measures that they have taken in response to those risks. Furthermore, in order to ensure that damage to users, other payment service providers or payment systems, such as a substantial disruption of a payment system, is kept to

a minimum, it is essential that payment service providers be required to report major security incidents without undue delay to the competent authorities. A coordination role by EBA should be established.

(92) The security incidents reporting obligations should be without prejudice to other incident reporting obligations laid down in other legal acts of the Union and any requirements laid down in this Directive should be aligned with, and proportionate to, the reporting obligations imposed by other Union law.

[...]

(95) Security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. There does not seem to be a need to guarantee the same level of protection to payment transactions initiated and executed with modalities other than the use of electronic platforms or devices, such as paper-based payment transactions, mail orders or telephone orders. A solid growth of internet payments and mobile payments should be accompanied by a generalised enhancement of security measures. Payment services offered via internet or via other at-distance channels, the functioning of which does not depend on where the device used to initiate the payment transaction or the payment instrument used are physically located, should therefore include the authentication of transactions through dynamic codes, in order to make the user aware, at all times, of the amount and the payee of the transaction that the user is authorising.

(96) The security measures should be compatible with the level of risk involved in the payment service. In order to allow the development of user-friendly and accessible means of payment for low-risk payments, such as low value contactless payments at the point of sale, whether or not they are based on mobile phone, the exemptions to the application of security requirements should be specified in regulatory technical standards. Safe use of personalised security credentials is needed to limit the risks relating to phishing and other fraudulent activities. In that respect, the user should be able to rely on the adoption of measures that protect the confidentiality and integrity of personalised security credentials. Those measures typically include encryption systems based on personal devices of the payer, including card readers or mobile phones, or provided to the payer by its account servicing payment service provider via a different channel, such as by SMS or email. The measures, typically including encryption systems, which may result in authentication codes such as one-time passwords, are able to enhance the security of payment transactions. The use of such authentication codes by payment service users should be considered to be compatible with their obligations in relation to payment instruments and personalised security credentials also when payment initiation service providers or account information service providers are involved.

[...]

(101) It is important that consumers be informed in a clear and comprehensible way of their rights and obligations under this Directive. The Commission should therefore produce a leaflet about those rights and obligations.

(102) This Directive is without prejudice to provisions of national law relating to the consequences as regards liability of inaccuracy in the expression or transmission of a statement.

[...]

(109) Since the objective of this Directive, namely the further integration of an internal market in payment services, cannot be sufficiently achieved by the Member States because it requires the harmonisation of a multitude of different rules currently existing in the legal systems of the various Member States but can rather, because of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in

Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.
[...]

HAVE ADOPTED THIS DIRECTIVE:

TITLE I

SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

Subject matter

1. This Directive establishes the rules in accordance with which Member States shall distinguish between the following categories of payment service provider:

(a) credit institutions as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council (28), including branches thereof within the meaning of point (17) Article 4(1) of that Regulation where such branches are located in the Union, whether the head offices of those branches are located within the Union or, in accordance with Article 47 of Directive 2013/36/EU and with national law, outside the Union;

(b) electronic money institutions within the meaning of point (1) of Article 2 of Directive 2009/110/EC, including, in accordance with Article 8 of that Directive and with national law, branches thereof, where such branches are located within the Union and their head offices are located outside the Union, in as far as the payment services provided by those branches are linked to the issuance of electronic money;

(c) post office giro institutions which are entitled under national law to provide payment services;

(d) payment institutions;

(e) the ECB and national central banks when not acting in their capacity as monetary authority or other public authorities;

(f) Member States or their regional or local authorities when not acting in their capacity as public authorities.

2. This Directive also establishes rules concerning:

(a) the transparency of conditions and information requirements for payment services; and

(b) the respective rights and obligations of payment service users and payment service providers in relation to the provision of payment services as a regular occupation or business activity.

Article 2

Scope

1. This Directive applies to payment services provided within the Union.

2. Titles III and IV apply to payment transactions in the currency of a Member State where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union.

3. Title III, except for point (b) of Article 45(1), point (2)(e) of Article 52 and point (a) of Article 56, and Title IV, except for Articles 81 to 86, apply to payment transactions in a currency that is not the currency of a Member State where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union, in respect to those parts of the payments transaction which are carried out in the Union.

4. Title III, except for point (b) of Article 45(1), point (2)(e) of Article 52, point (5)(g) of Article 52 and point (a) of Article 56, and Title IV, except for Article 62(2) and (4), Articles 76, 77, 81, 83(1), 89 and 92, apply to payment transactions in all currencies where only one of the payment service providers is located within the Union, in respect to those parts of the payments transaction which are carried out in the Union.

5. Member States may exempt institutions referred to in points (4) to (23) of Article 2(5) of Directive 2013/36/EU from the application of all or part of the provisions of this Directive.

Article 3

Exclusions

This Directive does not apply to the following:

(a) payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention;

(b) payment transactions from the payer to the payee through a commercial agent authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee;

(c) professional physical transport of banknotes and coins, including their collection, processing and delivery;

(d) payment transactions consisting of the non-professional cash collection and delivery within the framework of a non-profit or charitable activity;

(e) services where cash is provided by the payee to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services;

(f) cash-to-cash currency exchange operations where the funds are not held on a payment account;

(g) payment transactions based on any of the following documents drawn on the payment service provider with a view to placing funds at the disposal of the payee:

(i) paper cheques governed by the Geneva Convention of 19 March 1931 providing a uniform law for cheques;

(ii) paper cheques similar to those referred to in point (i) and governed by the laws of Member States which are not party to the Geneva Convention of 19 March 1931 providing a uniform law for cheques;

(iii) paper-based drafts in accordance with the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(iv) paper-based drafts similar to those referred to in point (iii) and governed by the laws of Member States which are not party to the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(v) paper-based vouchers;

(vi) paper-based traveller's cheques;

(vii) paper-based postal money orders as defined by the Universal Postal Union;

(h) payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and other participants of the system, and payment service providers, without prejudice to Article 35;

(i) payment transactions related to securities asset servicing, including dividends, income or other distributions, or redemption or sale, carried out by persons referred to in point (h) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services and any other entities allowed to have the custody of financial instruments;

(j) services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services, with the exclusion of payment initiation services and account information services;

(k) services based on specific payment instruments that can be used only in a limited way, that meet one of the following conditions:

(i) instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a limited network of service providers under direct commercial agreement with a professional issuer;

(ii) instruments which can be used only to acquire a very limited range of goods or services;

(iii) instruments valid only in a single Member State provided at the request of an undertaking or a public sector entity and

regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer;

(l) payment transactions by a provider of electronic communications networks or services provided in addition to electronic communications services for a subscriber to the network or service;

(i) for purchase of digital content and voice-based services, regardless of the device used for the purchase or consumption of the digital content and charged to the related bill; or

(ii) performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets;

provided that the value of any single payment transaction referred to in points (i) and (ii) does not exceed EUR 50 and:

—
the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month, or

—
where a subscriber pre-funds its account with the provider of the electronic communications network or service, the cumulative value of payment transactions does not exceed EUR 300 per month;

(m) payment transactions carried out between payment service providers, their agents or branches for their own account;

(n) payment transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group;
[...]

Article 4

Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'home Member State' means either of the following:

(a) the Member State in which the registered office of the payment service provider is situated; or

(b) if the payment service provider has, under its national law, no registered office, the Member State in which its head office is situated;

(2) 'host Member State' means the Member State other than the home Member State in which a payment service provider has an agent or a branch or provides payment services;

(3) 'payment service' means any business activity set out in Annex I;

(4) 'payment institution' means a legal person that has been granted authorisation in accordance with Article 11 to provide and execute payment services throughout the Union;

(5) 'payment transaction' means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

(6) 'remote payment transaction' means a payment transaction initiated via internet or through a device that can be used for distance communication;

(7) 'payment system' means a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions;

(8) 'payer' means a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order;

(9) 'payee' means a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction;

(10) 'payment service user' means a natural or legal person making use of a payment service in the capacity of payer, payee, or both;

(11) 'payment service provider' means a body referred to in Article 1(1) or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33;

(12) 'payment account' means an account held in the name of one or more payment service users which is used for the execution of payment transactions;

(13) 'payment order' means an instruction by a payer or payee to its payment service provider requesting the execution of a payment transaction;

(14) 'payment instrument' means a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order;

(15) 'payment initiation service' means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;

(16) 'account information service' means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider;

(17) 'account servicing payment service provider' means a payment service provider providing and maintaining a payment account for a payer;

(18) 'payment initiation service provider' means a payment service provider pursuing business activities as referred to in point (7) of Annex I;

(19) 'account information service provider' means a payment service provider pursuing business activities as referred to in point (8) of Annex I;

(20) 'consumer' means a natural person who, in payment service contracts covered by this Directive, is acting for purposes other than his or her trade, business or profession;

(21) 'framework contract' means a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account;

(22) 'money remittance' means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee;

(23) 'direct debit' means a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider;

(24) 'credit transfer' means a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the payment service provider which holds the payer's payment account, based on an instruction given by the payer;

(25) 'funds' means banknotes and coins, scriptural money or electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC;

(26) 'value date' means a reference time used by a payment service provider for the calculation of interest on the funds debited from or credited to a payment account;

(27) 'reference exchange rate' means the exchange rate which is used as the basis to calculate any currency exchange and which is made available by the payment service provider or comes from a publicly available source;

(28) 'reference interest rate' means the interest rate which is used as the basis for calculating any interest to be applied and which comes from a publicly available source which can be verified by both parties to a payment service contract;

(29) 'authentication' means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials;

(30) 'strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

(31) 'personalised security credentials' means personalised features provided by the payment service provider to a payment service user for the purposes of authentication;

(32) 'sensitive payment data' means data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data;

(33) 'unique identifier' means a combination of letters, numbers or symbols specified to the payment service user by the payment service provider and to be provided by the payment service user to identify unambiguously another payment service user and/or the payment account of that other payment service user for a payment transaction;

(34) 'means of distance communication' means a method which, without the simultaneous physical presence of the payment service provider and the payment service user, may be used for the conclusion of a payment services contract;

(35) 'durable medium' means any instrument which enables the payment service user to store information addressed personally to that payment service user in a way accessible for future reference for a period of time adequate to the purposes of the information and which allows the unchanged reproduction of the information stored;

(36) 'microenterprise' means an enterprise, which at the time of conclusion of the payment service contract, is an enterprise as defined in Article 1 and Article 2(1) and (3) of the Annex to Recommendation 2003/361/EC;

(37) 'business day' means a day on which the relevant payment service provider of the payer or the payment service provider of the payee involved in the execution of a payment transaction is open for business as required for the execution of a payment transaction;

(38) 'agent' means a natural or legal person who acts on behalf of a payment institution in providing payment services;

(39) 'branch' means a place of business other than the head office which is a part of a payment institution, which has no legal personality and which carries out directly some or all of the transactions inherent in the business of a payment institution; all of the places of business set up in the same Member State by a payment institution with a head office in another Member State shall be regarded as a single branch; [...]

(41) 'electronic communications network' means a network as defined in point (a) of Article 2 of Directive 2002/21/EC of the European Parliament and of the Council (30);

(42) 'electronic communications service' means a service as defined in point (c) of Article 2 of Directive 2002/21/EC;

(43) 'digital content' means goods or services which are produced and supplied in digital form, the use or consumption of which is restricted to a technical device and which do not include in any way the use or consumption of physical goods or services;

(44) 'acquiring of payment transactions' means a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee;

(45) 'issuing of payment instruments' means a payment service by a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions; [...]

(47) 'payment brand' means any material or digital name, term, sign, symbol or combination of them, capable of denoting under

which payment card scheme card-based payment transactions are carried out;

(48) 'co-badging' means the inclusion of two or more payment brands or payment applications of the same payment brand on the same payment instrument.

TITLE II PAYMENT SERVICE PROVIDERS

CHAPTER 1 Payment institutions [...]

TITLE III TRANSPARENCY OF CONDITIONS AND INFORMATION REQUIREMENTS FOR PAYMENT SERVICES

CHAPTER 1 General rules

Article 38

Scope

1. This Title applies to single payment transactions, framework contracts and payment transactions covered by them. The parties may agree that it shall not apply in whole or in part when the payment service user is not a consumer.

2. Member States may apply the provisions in this Title to microenterprises in the same way as to consumers.

3. This Directive shall be without prejudice to Directive 2008/48/EC, other relevant Union law or national measures regarding conditions for granting credit to consumers not harmonised by this Directive that comply with Union law.

Article 39

Other provisions in Union law

The provisions of this Title are without prejudice to any Union law containing additional requirements on prior information.

However, where Directive 2002/65/EC is also applicable, the information requirements set out in Article 3(1) of that Directive, with the exception of points (2)(c) to (g), (3)(a), (d) and (e), and (4)(b) of that paragraph shall be replaced by Articles 44, 45, 51 and 52 of this Directive.

Article 40

Charges for information

1. The payment service provider shall not charge the payment service user for providing information under this Title.

2. The payment service provider and the payment service user may agree on charges for additional or more frequent information, or transmission by means of communication other than those specified in the framework contract, provided that the payment service user's request.

3. Where the payment service provider may impose charges for information in accordance with paragraph 2, they shall be reasonable and in line with the payment service provider's actual costs.

Article 41

Burden of proof on information requirements

Member States shall stipulate that the burden of proof lies with the payment service provider to prove that it has complied with the information requirements set out in this Title.

Article 42

Derogation from information requirements for low-value payment instruments and electronic money

1. In cases of payment instruments which, according to the relevant framework contract, concern only individual payment transactions that do not exceed EUR 30 or that either have a spending limit of EUR 150 or store funds that do not exceed EUR 150 at any time:

(a) by way of derogation from Articles 51, 52 and 56, the payment service provider shall provide the payer only with information on the main characteristics of the payment service, including the way in which the payment instrument can be used, liability, charges levied and other material information needed to take an informed decision as well as an indication of

where any other information and conditions specified in Article 52 are made available in an easily accessible manner;

(b) it may be agreed that, by way of derogation from Article 54, the payment service provider is not required to propose changes to the conditions of the framework contract in the same way as provided for in Article 51(1);

(c) it may be agreed that, by way of derogation from Articles 57 and 58, after the execution of a payment transaction:

(i) the payment service provider provides or makes available only a reference enabling the payment service user to identify the payment transaction, the amount of the payment transaction, any charges and/or, in the case of several payment transactions of the same kind made to the same payee, information on the total amount and charges for those payment transactions;

(ii) the payment service provider is not required to provide or make available information referred to in point (i) if the payment instrument is used anonymously or if the payment service provider is not otherwise technically in a position to provide it. However, the payment service provider shall provide the payer with a possibility to verify the amount of funds stored.

2. For national payment transactions, Member States or their competent authorities may reduce or double the amounts referred to in paragraph 1. For prepaid payment instruments, Member States may increase those amounts up to EUR 500.

[...]

CHAPTER 3

Framework contracts

Article 50

Scope

This Chapter applies to payment transactions covered by a framework contract.

Article 51

Prior general information

1. Member States shall require that, in good time before the payment service user is bound by any framework contract or offer, the payment service provider provide the payment service user on paper or on another durable medium with the information and conditions specified in Article 52. The information and conditions shall be given in easily understandable words and in a clear and comprehensible form, in an official language of the Member State where the payment service is offered or in any other language agreed between the parties.

2. If the framework contract has been concluded at the request of the payment service user using a means of distance communication which does not enable the payment service provider to comply with paragraph 1, the payment service provider shall fulfil its obligations under that paragraph immediately after conclusion of the framework contract.

3. The obligations under paragraph 1 may also be discharged by providing a copy of the draft framework contract including the information and conditions specified in Article 52.

Article 52

Information and conditions

Member States shall ensure that the following information and conditions are provided to the payment service user:

1. on the payment service provider:

(a) the name of the payment service provider, the geographical address of its head office and, where applicable, the geographical address of its agent or branch established in the Member State where the payment service is offered, and any other address, including electronic mail address, relevant for communication with the payment service provider;

(b) the particulars of the relevant supervisory authorities and of the register provided for in Article 14 or of any other relevant public register of authorisation of the payment service provider and the registration number or equivalent means of identification in that register;

2. on use of the payment service:

(a) a description of the main characteristics of the payment service to be provided;

(b) a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly initiated or executed;

(c) the form of and procedure for giving consent to initiate a payment order or execute a payment transaction and withdrawal of such consent in accordance with Articles 64 and 80;

(d) a reference to the time of receipt of a payment order in accordance with Article 78 and the cut-off time, if any, established by the payment service provider;

(e) the maximum execution time for the payment services to be provided;

(f) whether there is a possibility to agree on spending limits for the use of the payment instrument in accordance with Article 68(1);

(g) in the case of co-badged, card-based payment instruments, the payment service user's rights under Article 8 of Regulation (EU) 2015/751;

3. on charges, interest and exchange rates:

(a) all charges payable by the payment service user to the payment service provider including those connected to the manner in and frequency with which information under this Directive is provided or made available and, where applicable, the breakdown of the amounts of such charges;

(b) where applicable, the interest and exchange rates to be applied or, if reference interest and exchange rates are to be used, the method of calculating the actual interest, and the relevant date and index or base for determining such reference interest or exchange rate;

(c) if agreed, the immediate application of changes in reference interest or exchange rate and information requirements relating to the changes in accordance with Article 54(2);

4. on communication:

(a) where applicable, the means of communication, including the technical requirements for the payment service user's equipment and software, agreed between the parties for the transmission of information or notifications under this Directive;

(b) the manner in, and frequency with which, information under this Directive is to be provided or made available;

(c) the language or languages in which the framework contract will be concluded and communication during this contractual relationship undertaken;

(d) the payment service user's right to receive the contractual terms of the framework contract and information and conditions in accordance with Article 53;

5. on safeguards and corrective measures:

(a) where applicable, a description of the steps that the payment service user is to take in order to keep safe a payment instrument and how to notify the payment service provider for the purposes of point (b) of Article 69(1);

(b) the secure procedure for notification of the payment service user by the payment service provider in the event of suspected or actual fraud or security threats;

(c) if agreed, the conditions under which the payment service provider reserves the right to block a payment instrument in accordance with Article 68;

(d) the liability of the payer in accordance with Article 74, including information on the relevant amount;

(e) how and within what period of time the payment service user is to notify the payment service provider of any unauthorised or incorrectly initiated or executed payment transaction in accordance with Article 71 as well as the payment service provider's liability for unauthorised payment transactions in accordance with Article 73;

(f) the liability of the payment service provider for the initiation or execution of payment transactions in accordance with Article 89;

(g) the conditions for refund in accordance with Articles 76 and 77;

6. on changes to, and termination of, the framework contract:

(a) if agreed, information that the payment service user will be deemed to have accepted changes in the conditions in accordance with Article 54, unless the payment service user notifies the payment service provider before the date of their proposed date of entry into force that they are not accepted;

(b) the duration of the framework contract;

(c) the right of the payment service user to terminate the framework contract and any agreements relating to termination in accordance with Article 54(1) and Article 55;

7. on redress:

(a) any contractual clause on the law applicable to the framework contract and/or the competent courts;

(b) the ADR procedures available to the payment service user in accordance with Articles 99 to 102.

Article 53

Accessibility of information and conditions of the framework contract

At any time during the contractual relationship the payment service user shall have a right to receive, on request, the contractual terms of the framework contract as well as the information and conditions specified in Article 52 on paper or on another durable medium.

Article 54

Changes in conditions of the framework contract

1. Any changes in the framework contract or in the information and conditions specified in Article 52 shall be proposed by the payment service provider in the same way as provided for in Article 51(1) and no later than 2 months before their proposed date of application. The payment service user can either accept or reject the changes before the date of their proposed date of entry into force.

Where applicable in accordance with point (6)(a) of Article 52, the payment service provider shall inform the payment service user that it is to be deemed to have accepted those changes if it does not notify the payment service provider before the proposed date of their entry into force that they are not accepted. The payment service provider shall also inform the payment service user that, in the event that the payment service user rejects those changes, the payment service user has the right to terminate the framework contract free of charge and with effect at any time until the date when the changes would have applied.

2. Changes in the interest or exchange rates may be applied immediately and without notice, provided that such a right is agreed upon in the framework contract and that the changes in the interest or exchange rates are based on the reference interest or exchange rates agreed on in accordance with point (3)(b) and (c) of Article 52. The payment service user shall be informed of any change in the interest rate at the earliest opportunity in the same way as provided for in Article 51(1), unless the parties have agreed on a specific frequency or manner in which the information is to be provided or made available. However, changes in interest or exchange rates which are more favourable to the payment service users, may be applied without notice.

3. Changes in the interest or exchange rate used in payment transactions shall be implemented and calculated in a neutral manner that does not discriminate against payment service users.

Article 55

Termination

1. The payment service user may terminate the framework contract at any time, unless the parties have agreed on a period of notice. Such a period shall not exceed 1 month.

2. Termination of the framework contract shall be free of charge for the payment service user except where the contract has been in force for less than 6 months. Charges, if any, for termination of the framework contract shall be appropriate and in line with costs.

3. If agreed in the framework contract, the payment service provider may terminate a framework contract concluded for an

indefinite period by giving at least 2 months' notice in the same way as provided for in Article 51(1).

4. Charges for payment services levied on a regular basis shall be payable by the payment service user only proportionally up to the termination of the contract. If such charges are paid in advance, they shall be reimbursed proportionally.

5. The provisions of this Article are without prejudice to the Member States' laws and Regulations governing the rights of the parties to declare the framework contract unenforceable or void.

6. Member States may provide for more favourable provisions for payment service users.

Article 56

Information before execution of individual payment transactions

In the case of an individual payment transaction under a framework contract initiated by the payer, a payment service provider shall, at the payer's request for this specific payment transaction, provide explicit information on all of the following:

(a) the maximum execution time;

(b) the charges payable by the payer;

(c) where applicable, a breakdown of the amounts of any charges.

Article 57

Information for the payer on individual payment transactions

1. After the amount of an individual payment transaction is debited from the payer's account or, where the payer does not use a payment account, after receipt of the payment order, the payer's payment service provider shall provide the payer, without undue delay and in the same way as laid down in Article 51(1), with all of the following information:

(a) a reference enabling the payer to identify each payment transaction and, where appropriate, information relating to the payee;

(b) the amount of the payment transaction in the currency in which the payer's payment account is debited or in the currency used for the payment order;

(c) the amount of any charges for the payment transaction and, where applicable, a breakdown of the amounts of such charges, or the interest payable by the payer;

(d) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider, and the amount of the payment transaction after that currency conversion;

(e) the debit value date or the date of receipt of the payment order.

2. A framework contract shall include a condition that the payer may require the information referred to in paragraph 1 to be provided or made available periodically, at least once a month, free of charge and in an agreed manner which allows the payer to store and reproduce information unchanged.

3. However, Member States may require payment service providers to provide information on paper or on another durable medium at least once a month, free of charge.

Article 58

Information for the payee on individual payment transactions

1. After the execution of an individual payment transaction, the payee's payment service provider shall provide the payee without undue delay in the same way as laid down in Article 51(1) with all of the following information:

(a) a reference enabling the payee to identify the payment transaction and the payer, and any information transferred with the payment transaction;

(b) the amount of the payment transaction in the currency in which the payee's payment account is credited;

(c) the amount of any charges for the payment transaction and, where applicable, a breakdown of the amounts of such charges, or the interest payable by the payee;

(d) where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the

amount of the payment transaction before that currency conversion;

(e) the credit value date.

2. A framework contract may include a condition that the information referred to in paragraph 1 is to be provided or made available periodically, at least once a month and in an agreed manner which allows the payee to store and reproduce information unchanged.

3. However, Member States may require payment service providers to provide information on paper or on another durable medium at least once a month, free of charge.

CHAPTER 4

Common provisions

Article 59

Currency and currency conversion

1. Payments shall be made in the currency agreed between the parties.

2. Where a currency conversion service is offered prior to the initiation of the payment transaction and where that currency conversion service is offered at an ATM, at the point of sale or by the payee, the party offering the currency conversion service to the payer shall disclose to the payer all charges as well as the exchange rate to be used for converting the payment transaction.

The payer shall agree to the currency conversion service on that basis.

Article 60

Information on additional charges or reductions

1. Where, for the use of a given payment instrument, the payee requests a charge or offers a reduction, the payee shall inform the payer thereof prior to the initiation of the payment transaction.

2. Where, for the use of a given payment instrument, the payment service provider or another party involved in the transaction requests a charge, it shall inform the payment service user thereof prior to the initiation of the payment transaction.

3. The payer shall only be obliged to pay for the charges referred to in paragraphs 1 and 2 if their full amount was made known prior to the initiation of the payment transaction.

TITLE IV

RIGHTS AND OBLIGATIONS IN RELATION TO THE PROVISION AND USE OF PAYMENT SERVICES

CHAPTER 1

Common provisions

Article 61

Scope

1. Where the payment service user is not a consumer, the payment service user and the payment service provider may agree that Article 62(1), Article 64(3), and Articles 72, 74, 76, 77, 80 and 89 do not apply in whole or in part. The payment service user and the payment service provider may also agree on time limits that are different from those laid down in Article 71.

2. Member States may provide that Article 102 does not apply where the payment service user is not a consumer.

3. Member States may provide that provisions in this Title are applied to microenterprises in the same way as to consumers.

4. This Directive shall be without prejudice to Directive 2008/48/EC, other relevant Union law or national measures regarding conditions for granting credit to consumers not harmonised by this Directive that comply with Union law.

Article 62

Charges applicable

1. The payment service provider shall not charge the payment service user for fulfilment of its information obligations or corrective and preventive measures under this Title, unless otherwise specified in Article 79(1), Article 80(5) and Article 88(2). Those charges shall be agreed between the payment service user and the payment service provider and shall be

appropriate and in line with the payment service provider's actual costs.

2. Member States shall require that for payment transactions provided within the Union, where both the payer's and the payee's payment service providers are, or the sole payment service provider in the payment transaction is, located therein, the payee pays the charges levied by his payment service provider, and the payer pays the charges levied by his payment service provider.

3. The payment service provider shall not prevent the payee from requesting from the payer a charge, offering him a reduction or otherwise steering him towards the use of a given payment instrument. Any charges applied shall not exceed the direct costs borne by the payee for the use of the specific payment instrument.

4. In any case, Member States shall ensure that the payee shall not request charges for the use of payment instruments for which interchange fees are regulated under Chapter II of Regulation (EU) 2015/751 and for those payment services to which Regulation (EU) No 260/2012 applies.

5. Member States may prohibit or limit the right of the payee to request charges taking into account the need to encourage competition and promote the use of efficient payment instruments.

Article 63

Derogation for low value payment instruments and electronic money

1. In the case of payment instruments which, according to the framework contract, solely concern individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150, or store funds which do not exceed EUR 150 at any time, payment service providers may agree with their payment service users that:

(a) point (b) of Article 69(1), points (c) and (d) of Article 70(1), and Article 74(3) do not apply if the payment instrument does not allow its blocking or prevention of its further use;

(b) Articles 72 and 73, and Article 74(1) and (3), do not apply if the payment instrument is used anonymously or the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised;

(c) by way of derogation from Article 79(1), the payment service provider is not required to notify the payment service user of the refusal of a payment order, if the non-execution is apparent from the context;

(d) by way of derogation from Article 80, the payer may not revoke the payment order after transmitting the payment order or giving consent to execute the payment transaction to the payee;

(e) by way of derogation from Articles 83 and 84, other execution periods apply.

2. For national payment transactions, Member States or their competent authorities may reduce or double the amounts referred to in paragraph 1. They may increase them for prepaid payment instruments up to EUR 500.

3. Articles 73 and 74 of this Directive shall apply also to electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC, except where the payer's payment service provider does not have the ability to freeze the payment account on which the electronic money is stored or block the payment instrument. Member States may limit that derogation to payment accounts on which the electronic money is stored or to payment instruments of a certain value.

CHAPTER 2

Authorisation of payment transactions

Article 64

Consent and withdrawal of consent

1. Member States shall ensure that a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the

payer and the payment service provider, after the execution of the payment transaction.

2. Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the payment service provider. Consent to execute a payment transaction may also be given via the payee or the payment initiation service provider.

In the absence of consent, a payment transaction shall be considered to be unauthorised.

3. Consent may be withdrawn by the payer at any time, but no later than at the moment of irrevocability in accordance with Article 80. Consent to execute a series of payment transactions may also be withdrawn, in which case any future payment transaction shall be considered to be unauthorised.

4. The procedure for giving consent shall be agreed between the payer and the relevant payment service provider(s).

Article 65

Confirmation on the availability of funds

1. Member States shall ensure that an account servicing payment service provider shall, upon the request of a payment service provider issuing card-based payment instruments, immediately confirm whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer, provided that all of the following conditions are met:

(a) the payment account of the payer is accessible online at the time of the request;

(b) the payer has given explicit consent to the account servicing payment service provider to respond to requests from a specific payment service provider to confirm that the amount corresponding to a certain card-based payment transaction is available on the payer's payment account;

(c) the consent referred to in point (b) has been given before the first request for confirmation is made.

2. The payment service provider may request the confirmation referred to in paragraph 1 where all of the following conditions are met:

(a) the payer has given explicit consent to the payment service provider to request the confirmation referred to in paragraph 1;

(b) the payer has initiated the card-based payment transaction for the amount in question using a card based payment instrument issued by the payment service provider;

(c) the payment service provider authenticates itself towards the account servicing payment service provider before each confirmation request, and securely communicates with the account servicing payment service provider in accordance with point (d) of Article 98(1).

3. In accordance with Directive 95/46/EC, the confirmation referred to in paragraph 1 shall consist only in a simple 'yes' or 'no' answer and not in a statement of the account balance. That answer shall not be stored or used for purposes other than for the execution of the card-based payment transaction.

4. The confirmation referred to in paragraph 1 shall not allow for the account servicing payment service provider to block funds on the payer's payment account.

5. The payer may request the account servicing payment service provider to communicate to the payer the identification of the payment service provider and the answer provided.

6. This Article does not apply to payment transactions initiated through card-based payment instruments on which electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC is stored.

Article 66

Rules on access to payment account in the case of payment initiation services

1. Member States shall ensure that a payer has the right to make use of a payment initiation service provider to obtain payment services as referred to in point (7) of Annex I. The right to make use of a payment initiation service provider shall not apply where the payment account is not accessible online.

2. When the payer gives its explicit consent for a payment to be executed in accordance with Article 64, the account servicing payment service provider shall perform the actions specified in paragraph 4 of this Article in order to ensure the payer's right to use the payment initiation service.

3. The payment initiation service provider shall:

(a) not hold at any time the payer's funds in connection with the provision of the payment initiation service;

(b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;

(c) ensure that any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's explicit consent;

(d) every time a payment is initiated, identify itself towards the account servicing payment service provider of the payer and communicate with the account servicing payment service provider, the payer and the payee in a secure way, in accordance with point (d) of Article 98(1);

(e) not store sensitive payment data of the payment service user;

(f) not request from the payment service user any data other than those necessary to provide the payment initiation service;

(g) not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer;

(h) not modify the amount, the payee or any other feature of the transaction.

4. The account servicing payment service provider shall:

(a) communicate securely with payment initiation service providers in accordance with point (d) of Article 98(1);

(b) immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider;

(c) treat payment orders transmitted through the services of a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer.

5. The provision of payment initiation services shall not be dependent on the existence of a contractual relationship between the payment initiation service providers and the account servicing payment service providers for that purpose.

Article 67

Rules on access to and use of payment account information in the case of account information services

1. Member States shall ensure that a payment service user has the right to make use of services enabling access to account information as referred to in point (8) of Annex I. That right shall not apply where the payment account is not accessible online.

2. The account information service provider shall:

(a) provide services only where based on the payment service user's explicit consent;

(b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels;

(c) for each communication session, identify itself towards the account servicing payment service provider(s) of the payment service user and securely communicate with the account servicing payment service provider(s) and the payment service user, in accordance with point (d) of Article 98(1);

(d) access only the information from designated payment accounts and associated payment transactions;

(e) not request sensitive payment data linked to the payment accounts;

(f) not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.

3. In relation to payment accounts, the account servicing payment service provider shall:

(a) communicate securely with the account information service providers in accordance with point (d) of Article 98(1); and

(b) treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons.

4. The provision of account information services shall not be dependent on the existence of a contractual relationship between the account information service providers and the account servicing payment service providers for that purpose.

Article 68

Limits of the use of the payment instrument and of the access to payment accounts by payment service providers

1. Where a specific payment instrument is used for the purposes of giving consent, the payer and the payer's payment service provider may agree on spending limits for payment transactions executed through that payment instrument.

2. If agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil its liability to pay.

3. In such cases the payment service provider shall inform the payer of the blocking of the payment instrument and the reasons for it in an agreed manner, where possible, before the payment instrument is blocked and at the latest immediately thereafter, unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant Union or national law.

4. The payment service provider shall unblock the payment instrument or replace it with a new payment instrument once the reasons for blocking no longer exist.

5. An account servicing payment service provider may deny an account information service provider or a payment initiation service provider access to a payment account for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that account information service provider or that payment initiation service provider, including the unauthorised or fraudulent initiation of a payment transaction. In such cases the account servicing payment service provider shall inform the payer that access to the payment account is denied and the reasons therefor in the form agreed. That information shall, where possible, be given to the payer before access is denied and at the latest immediately thereafter, unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant Union or national law.

The account servicing payment service provider shall allow access to the payment account once the reasons for denying access no longer exist.

6. In the cases referred to in paragraph 5, the account servicing payment service provider shall immediately report the incident relating to the account information service provider or the payment initiation service provider to the competent authority. The information shall include the relevant details of the case and the reasons for taking action. The competent authority shall assess the case and shall, if necessary, take appropriate measures.

Article 69

Obligations of the payment service user in relation to payment instruments and personalised security credentials

1. The payment service user entitled to use a payment instrument shall:

(a) use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate;

(b) notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

2. For the purposes of point (a) of paragraph 1, the payment service user shall, in particular, as soon as in receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe.

Article 70

Obligations of the payment service provider in relation to payment instruments

1. The payment service provider issuing a payment instrument shall:

(a) make sure that the personalised security credentials are not accessible to parties other than the payment service user that is entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in Article 69;

(b) refrain from sending an unsolicited payment instrument, except where a payment instrument already given to the payment service user is to be replaced;

(c) ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to point (b) of Article 69(1) or to request unblocking of the payment instrument pursuant to Article 68(4); on request, the payment service provider shall provide the payment service user with the means to prove, for 18 months after notification, that the payment service user made such a notification;

(d) provide the payment service user with an option to make a notification pursuant to point (b) of Article 69(1) free of charge and to charge, if at all, only replacement costs directly attributed to the payment instrument;

(e) prevent all use of the payment instrument once notification pursuant to point (b) of Article 69(1) has been made.

2. The payment service provider shall bear the risk of sending a payment instrument or any personalised security credentials relating to it to the payment service user.

Article 71

Notification and rectification of unauthorised or incorrectly executed payment transactions

1. The payment service user shall obtain rectification of an unauthorised or incorrectly executed payment transaction from the payment service provider only if the payment service user notifies the payment service provider without undue delay on becoming aware of any such transaction giving rise to a claim, including that under Article 89, and no later than 13 months after the debit date.

The time limits for notification laid down in the first subparagraph do not apply where the payment service provider has failed to provide or make available the information on the payment transaction in accordance with Title III.

2. Where a payment initiation service provider is involved, the payment service user shall obtain rectification from the account servicing payment service provider pursuant to paragraph 1 of this Article, without prejudice to Article 73(2) and Article 89(1).

Article 72

Evidence on authentication and execution of payment transactions

1. Member States shall require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated,

accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.

If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

2. Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 69. The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user.

Article 73

Payment service provider's liability for unauthorised payment transactions

1. Member States shall ensure that, without prejudice to Article 71, in the case of an unauthorised payment transaction, the payer's payment service provider refunds the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing. Where applicable, the payer's payment service provider shall restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. This shall also ensure that the credit value date for the payer's payment account shall be no later than the date the amount had been debited.

2. Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund immediately, and in any event no later than by the end of the following business day the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.

If the payment initiation service provider is liable for the unauthorised payment transaction, it shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer, including the amount of the unauthorised payment transaction. In accordance with Article 72(1), the burden shall be on the payment initiation service provider to prove that, within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

3. Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the payer and the payment service provider or the contract concluded between the payer and the payment initiation service provider if applicable.

Article 74

Payer's liability for unauthorised payment transactions

1. By way of derogation from Article 73, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.

The first subparagraph shall not apply if:

(a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or

(b) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.

The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 69 with intent or gross negligence. In such cases, the maximum amount referred to in the first subparagraph shall not apply.

Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 69, Member States may reduce the liability referred to in this paragraph, taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated.

2. Where the payer's payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. Where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider.

3. The payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with point (b) of Article 69(1), except where the payer has acted fraudulently.

If the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as required under point (c) of Article 70(1), the payer shall not be liable for the financial consequences resulting from use of that payment instrument, except where the payer has acted fraudulently.

Article 75

Payment transactions where the transaction amount is not known in advance

1. Where a payment transaction is initiated by or through the payee in the context of a card-based payment transaction and the exact amount is not known at the moment when the payer gives consent to execute the payment transaction, the payer's payment service provider may block funds on the payer's payment account only if the payer has given consent to the exact amount of the funds to be blocked.

2. The payer's payment service provider shall release the funds blocked on the payer's payment account under paragraph 1 without undue delay after receipt of the information about the exact amount of the payment transaction and at the latest immediately after receipt of the payment order.

Article 76

Refunds for payment transactions initiated by or through a payee

1. Member States shall ensure that a payer is entitled to a refund from the payment service provider of an authorised payment transaction which was initiated by or through a payee and which has already been executed, if both of the following conditions are met:

(a) the authorisation did not specify the exact amount of the payment transaction when the authorisation was made;

(b) the amount of the payment transaction exceeded the amount the payer could reasonably have expected taking into account the previous spending pattern, the conditions in the framework contract and relevant circumstances of the case.

At the payment service provider's request, the payer shall bear the burden of proving such conditions are met.

The refund shall consist of the full amount of the executed payment transaction. The credit value date for the payer's payment account shall be no later than the date the amount was debited.

Without prejudice to paragraph 3, Member States shall ensure that, in addition to the right referred to in this paragraph, for direct debits as referred to in Article 1 of Regulation (EU) No 260/2012, the payer has an unconditional right to a refund within the time limits laid down in Article 77 of this Directive.

2. However, for the purposes of point (b) of the first subparagraph of paragraph 1, the payer shall not rely on currency exchange reasons if the reference exchange rate agreed with its payment service provider in accordance with point (d) of Article 45(1) and point (3)(b) of Article 52 was applied.

3. It may be agreed in a framework contract between the payer and the payment service provider that the payer has no right to a refund where:

(a) the payer has given consent to execute the payment transaction directly to the payment service provider; and

(b) where applicable, information on the future payment transaction was provided or made available in an agreed manner to the payer for at least 4 weeks before the due date by the payment service provider or by the payee.

4. For direct debits in currencies other than euro, Member States may require their payment service providers to offer more favourable refund rights in accordance with their direct debit schemes provided that they are more advantageous to the payer.

Article 77

Requests for refunds for payment transactions initiated by or through a payee

1. Member States shall ensure that the payer can request the refund referred to in Article 76 of an authorised payment transaction initiated by or through a payee for a period of 8 weeks from the date on which the funds were debited.

2. Within 10 business days of receiving a request for a refund, the payment service provider shall either refund the full amount of the payment transaction or provide a justification for refusing the refund and indicate the bodies to which the payer may refer the matter in accordance with Articles 99 to 102 if the payer does not accept the reasons provided.

The payment service provider's right under the first subparagraph of this paragraph to refuse the refund shall not apply in the case set out in the fourth subparagraph of Article 76(1).

CHAPTER 3

Execution of payment transactions

Section 1

Payment orders and amounts transferred

Article 78

Receipt of payment orders

1. Member States shall ensure that the time of receipt is when the payment order is received by the payer's payment service provider.

The payer's account shall not be debited before receipt of the payment order. If the time of receipt is not on a business day for the payer's payment service provider, the payment order shall be deemed to have been received on the following business day. The payment service provider may establish a cut-off time near the end of a business day beyond which any payment order received shall be deemed to have been received on the following business day.

2. If the payment service user initiating a payment order and the payment service provider agree that execution of the payment order shall start on a specific day or at the end of a certain period or on the day on which the payer has put funds at the payment service provider's disposal, the time of receipt for the purposes of Article 83 is deemed to be the agreed day. If the agreed day is not a business day for the payment service provider, the payment order received shall be deemed to have been received on the following business day.

Article 79

Refusal of payment orders

1. Where the payment service provider refuses to execute a payment order or to initiate a payment transaction, the refusal and, if possible, the reasons for it and the procedure for correcting any factual mistakes that led to the refusal shall be notified to the payment service user, unless prohibited by other relevant Union or national law.

The payment service provider shall provide or make available the notification in an agreed manner at the earliest opportunity, and in any case, within the periods specified in Article 83.

The framework contract may include a condition that the payment service provider may charge a reasonable fee for such a refusal if the refusal is objectively justified.

2. Where all of the conditions set out in the payer's framework contract are met, the payer's account servicing payment service provider shall not refuse to execute an authorised payment order irrespective of whether the payment order is initiated by a payer, including through a payment initiation service provider, or by or through a payee, unless prohibited by other relevant Union or national law.

3. For the purposes of Articles 83 and 89 a payment order for which execution has been refused shall be deemed not to have been received.

[...]

Article 81

Amounts transferred and amounts received

1. Member States shall require the payment service provider(s) of the payer, the payment service provider(s) of the payee and any intermediaries of the payment service providers to transfer the full amount of the payment transaction and refrain from deducting charges from the amount transferred.

2. However, the payee and the payment service provider may agree that the relevant payment service provider deduct its charges from the amount transferred before crediting it to the payee. In such a case, the full amount of the payment transaction and charges shall be separated in the information given to the payee.

3. If any charges other than those referred to in paragraph 2 are deducted from the amount transferred, the payment service provider of the payer shall ensure that the payee receives the full amount of the payment transaction initiated by the payer. Where the payment transaction is initiated by or through the payee, the payment service provider of the payee shall ensure that the full amount of the payment transaction is received by the payee.

[...]

Article 89

Payment service providers' liability for non-execution, defective or late execution of payment transactions

1. Where a payment order is initiated directly by the payer, the payer's payment service provider shall, without prejudice to Article 71, Article 88(2) and (3), and Article 93, be liable to the payer for correct execution of the payment transaction, unless it can prove to the payer and, where relevant, to the payee's payment service provider that the payee's payment service provider received the amount of the payment transaction in accordance with Article 83(1). In that case, the payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction.

Where the payer's payment service provider is liable under the first subparagraph, it shall, without undue delay, refund to the payer the amount of the non-executed or defective payment transaction, and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.

The credit value date for the payer's payment account shall be no later than the date on which the amount was debited.

Where the payee's payment service provider is liable under the first subparagraph, it shall immediately place the amount of the payment transaction at the payee's disposal and, where applicable, credit the corresponding amount to the payee's payment account.

The credit value date for the payee's payment account shall be no later than the date on which the amount would have been value dated, had the transaction been correctly executed in accordance with Article 87.

Where a payment transaction is executed late, the payee's payment service provider shall ensure, upon the request of the payer's payment service provider acting on behalf of the payer, that the credit value date for the payee's payment account is no later than the date the amount would have been value dated had the transaction been correctly executed.

In the case of a non-executed or defectively executed payment transaction where the payment order is initiated by the payer, the payer's payment service provider shall, regardless of liability under this paragraph, on request, make immediate efforts to trace the payment transaction and notify the payer of the outcome. This shall be free of charge for the payer.

2. Where a payment order is initiated by or through the payee, the payee's payment service provider shall, without prejudice to Article 71, Article 88(2) and (3), and Article 93, be liable to the payee for correct transmission of the payment order to the payment service provider of the payer in accordance with Article 83(3). Where the payee's payment service provider is liable under this subparagraph, it shall immediately re-transmit the payment order in question to the payment service provider of the payer.

In the case of a late transmission of the payment order, the amount shall be value dated on the payee's payment account no later than the date the amount would have been value dated had the transaction been correctly executed.

In addition, the payment service provider of the payee shall, without prejudice to Article 71, Article 88(2) and (3), and Article 93, be liable to the payee for handling the payment transaction in accordance with its obligations under Article 87.

Where the payee's payment service provider is liable under this subparagraph, it shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account. The amount shall be value dated on the payee's payment account no later than the date the amount would have been value dated had the transaction been correctly executed.

In the case of a non-executed or defectively executed payment transaction for which the payee's payment service provider is not liable under the first and second subparagraphs, the payer's payment service provider shall be liable to the payer. Where the payer's payment service provider is so liable he shall, as appropriate and without undue delay, refund to the payer the amount of the non-executed or defective payment transaction and restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place. The credit value date for the payer's payment account shall be no later than the date the amount was debited. The obligation under the fourth subparagraph shall not apply to the payer's payment service provider where the payer's payment service provider proves that the payee's payment service provider has received the amount of the payment transaction, even if execution of payment transaction is merely delayed. If so, the payee's payment service provider shall value date the amount on the payee's payment account no later than the date the amount would have been value dated had it been executed correctly.

In the case of a non-executed or defectively executed payment transaction where the payment order is initiated by or through the payee, the payee's payment service provider shall, regardless of liability under this paragraph, on request, make immediate efforts to trace the payment transaction and notify the payee of the outcome. This shall be free of charge for the payee.

3. In addition, payment service providers shall be liable to their respective payment service users for any charges for which they are responsible, and for any interest to which the payment service user is subject as a consequence of non-execution or defective, including late, execution of the payment transaction.

Article 90

Liability in the case of payment initiation services for non-execution, defective or late execution of payment transactions

1. Where a payment order is initiated by the payer through a payment initiation service provider, the account servicing payment service provider shall, without prejudice to Article 71 and Article 88(2) and (3), refund to the payer the amount of the non-executed or defective payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.

The burden shall be on the payment initiation service provider to prove that the payment order was received by the payer's account servicing payment service provider in accordance with Article 78 and that within its sphere of competence the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the non-execution, defective or late execution of the transaction.

2. If the payment initiation service provider is liable for the non-execution, defective or late execution of the payment transaction, it shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer.

Article 91

Additional financial compensation

Any financial compensation additional to that provided for under this Section may be determined in accordance with the law applicable to the contract concluded between the payment service user and the payment service provider.

Article 92

Right of recourse

1. Where the liability of a payment service provider under Articles 73 and 89 is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary shall compensate the first payment service provider for any losses incurred or sums paid under Articles 73 and 89. That shall include compensation where any of the payment service providers fail to use strong customer authentication.

2. Further financial compensation may be determined in accordance with agreements between payment service providers and/or intermediaries and the law applicable to the agreement concluded between them.

Article 93

Abnormal and unforeseeable circumstances

No liability shall arise under Chapter 2 or 3 in cases of abnormal and unforeseeable circumstances beyond the control of the party pleading for the application of those circumstances, the consequences of which would have been unavoidable despite all efforts to the contrary, or where a payment service provider is bound by other legal obligations covered by Union or national law.

CHAPTER 4

Data protection

Article 94

Data protection

1. Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. The provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive 95/46/EC and with Regulation (EC) No 45/2001.

2. Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.

CHAPTER 5

Operational and security risks and authentication [...]

Article 97

Authentication

1. Member States shall ensure that a payment service provider applies strong customer authentication where the payer:

- (a) accesses its payment account online;
- (b) initiates an electronic payment transaction;
- (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2. With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

3. With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

4. Paragraphs 2 and 3 shall also apply where payments are initiated through a payment initiation service provider. Paragraphs 1 and 3 shall also apply when the information is requested through an account information service provider.

5. Member States shall ensure that the account servicing payment service provider allows the payment initiation service provider and the account information service provider to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user in accordance with paragraphs 1 and 3 and, where the payment initiation service provider is involved, in accordance with paragraphs 1, 2 and 3.

[...]

CHAPTER 6

ADR procedures for the settlement of disputes

Section 1

Complaint procedures

Article 99

Complaints

1. Member States shall ensure that procedures are set up which allow payment service users and other interested parties including consumer associations, to submit complaints to the competent authorities with regard to payment service providers' alleged infringements of this Directive.

2. Where appropriate and without prejudice to the right to bring proceedings before a court in accordance with national procedural law, the reply from the competent authorities shall inform the complainant of the existence of the ADR procedures set up in accordance with Article 102.

[...]

Section 2

ADR procedures and penalties

Article 101

Dispute resolution

1. Member States shall ensure that payment service providers put in place and apply adequate and effective complaint resolution procedures for the settlement of complaints of payment service users concerning the rights and obligations arising under Titles III and IV of this Directive and shall monitor their performance in that regard.

Those procedures shall be applied in every Member State where the payment service provider offers the payment services and shall be available in an official language of the relevant Member State or in another language if agreed between the payment service provider and the payment service user.

2. Member States shall require that payment service providers make every possible effort to reply, on paper or, if agreed between payment service provider and payment service user,

on another durable medium, to the payment service users' complaints. Such a reply shall address all points raised, within an adequate timeframe and at the latest within 15 business days of receipt of the complaint. In exceptional situations, if the answer cannot be given within 15 business days for reasons beyond the control of the payment service provider, it shall be required to send a holding reply, clearly indicating the reasons for a delay in answering to the complaint and specifying the deadline by which the payment service user will receive the final reply. In any event, the deadline for receiving the final reply shall not exceed 35 business days.

Member States may introduce or maintain rules on dispute resolution procedures that are more advantageous to the payment service user than that referred to in the first subparagraph. Where they do so, those rules shall apply.

3. The payment service provider shall inform the payment service user about at least one ADR entity which is competent to deal with disputes concerning the rights and obligations arising under Titles III and IV.

4. The information referred to in paragraph 3 shall be mentioned in a clear, comprehensive and easily accessible way on the website of the payment service provider, where one exists, at the branch, and in the general terms and conditions of the contract between the payment service provider and the payment service user. It shall specify how further information on the ADR entity concerned and on the conditions for using it can be accessed.

Article 102

ADR procedures

1. Member States shall ensure that adequate, independent, impartial, transparent and effective ADR procedures for the settlement of disputes between payment service users and payment service providers concerning the rights and obligations arising under Titles III and IV of this Directive are established according to the relevant national and Union law in accordance with Directive 2013/11/EU of the European Parliament and the Council (35), using existing competent bodies where appropriate. Member States shall ensure that ADR procedures are applicable to payment service providers and that they also cover the activities of appointed representatives.

2. Member States shall require the bodies referred to in paragraph 1 of this Article to cooperate effectively for the resolution of cross-border disputes concerning the rights and obligations arising under Titles III and IV.

Article 103

Penalties

1. Member States shall lay down rules on penalties applicable to infringements of the national law transposing this Directive and shall take all necessary measures to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Member States shall allow their competent authorities to disclose to the public any administrative penalty that is imposed for infringement of the measures adopted in the transposition of this Directive, unless such disclosure would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.

TITLE V

DELEGATED ACTS AND REGULATORY TECHNICAL STANDARDS

Article 104

Delegated acts

The Commission shall be empowered to adopt delegated acts in accordance with Article 105 concerning:

(a) adapting the reference to Recommendation 2003/361/EC in point (36) of Article 4 of this Directive where that Recommendation is amended;

(b) updating the amounts specified in Article 32(1) and Article 74(1) to take account of inflation.

[..]

Article 106

Obligation to inform consumers of their rights

1. By 13 January 2018, the Commission shall produce a user-friendly electronic leaflet, listing in a clear and easily comprehensible manner, the rights of consumers under this Directive and related Union law.

2. The Commission shall inform Member States, European associations of payment service providers and European consumer associations of the publication of the leaflet referred to in paragraph 1.

The Commission, EBA and the competent authorities shall each ensure that the leaflet is made available in an easily accessible manner on their respective websites.

3. Payment service providers shall ensure that the leaflet is made available in an easily accessible manner on their websites, if existing, and on paper at their branches, their agents and the entities to which their activities are outsourced.

4. Payment service providers shall not charge their clients for making available information under this Article.

5. In respect of persons with disabilities, the provisions of this Article shall be applied using appropriate alternative means, allowing the information to be made available in an accessible format.

TITLE VI

FINAL PROVISIONS

Article 107

Full harmonisation

1. Without prejudice to Article 2, Article 8(3), Article 32, Article 38(2), Article 42(2), Article 55(6), Article 57(3), Article 58(3), Article 61(2) and (3), Article 62(5), Article 63(2) and (3), the second subparagraph of Article 74(1) and Article 86, insofar as this Directive contains harmonised provisions, Member States shall not maintain or introduce provisions other than those laid down in this Directive.

2. Where a Member State makes use of any of the options referred to in paragraph 1, it shall inform the Commission thereof as well as of any subsequent changes. The Commission shall make the information public on a website or other easily accessible means.

3. Member States shall ensure that payment service providers do not derogate, to the detriment of payment service users, from the provisions of national law transposing this Directive except where explicitly provided for therein.

However, payment service providers may decide to grant more favourable terms to payment service users.

[...]

Article 114

Repeal

Directive 2007/64/EC is repealed with effect from 13 January 2018.

Any reference to the repealed Directive shall be construed as a reference to this Directive and shall be read in accordance with the correlation table in Annex II to this Directive.

Article 115

Transposition

1. By 13 January 2018, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

2. They shall apply those measures from 13 January 2018.

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

3. Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.

4. By way of derogation from paragraph 2, Member States shall ensure the application of the security measures referred to in Articles 65, 66, 67 and 97 from 18 months after the date of entry

into force of the regulatory technical standards referred to in Article 98.

5. Member States shall not forbid legal persons that have performed in their territories, before 12 January 2016, activities of payment initiation service providers and account information service providers within the meaning of this Directive, to continue to perform the same activities in their territories during the transitional period referred to in paragraphs 2 and 4 in accordance with the currently applicable regulatory framework.

6. Member States shall ensure that until individual account servicing payment service providers comply with the regulatory technical standards referred to in paragraph 4, account servicing payment service providers do not abuse their non-compliance to block or obstruct the use of payment initiation and account information services for the accounts that they are servicing.

Article 116

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 117

Addresses

This Directive is addressed to the Member States.

Done at Strasbourg, 25 November 2015.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

N. SCHMIT

[...]

ANNEX I

PAYMENT SERVICES

(as referred to in point (3) of Article 4)

1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account.

2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.

3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider:

(a) execution of direct debits, including one-off direct debits;

(b) execution of payment transactions through a payment card or a similar device;

(c) execution of credit transfers, including standing orders.

4. Execution of payment transactions where the funds are covered by a credit line for a payment service user:

(a) execution of direct debits, including one-off direct debits;

(b) execution of payment transactions through a payment card or a similar device;

(c) execution of credit transfers, including standing orders.

5. Issuing of payment instruments and/or acquiring of payment transactions.

6. Money remittance.

7. Payment initiation services.

8. Account information services.

ANNEX II

CORRELATION TABLE

[...]

Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (“PAD” Directive)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Central Bank (1),
Having regard to the opinion of the European Economic and Social Committee (2),
Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) In accordance with Article 26(2) of the Treaty on the Functioning of the European Union (TFEU), the internal market is to comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured. Fragmentation of the internal market is detrimental to competitiveness, growth and job creation within the Union. Eliminating direct and indirect obstacles to the proper functioning of the internal market is essential for its completion. Union action with respect to the internal market in the retail financial services sector has already substantially contributed to developing cross-border activity of payment service providers, improving consumer choice and increasing the quality and transparency of the offers.

(2) In this respect, Directive 2007/64/EC of the European Parliament and of the Council (4) established basic transparency requirements for fees charged by payment service providers in relation to services offered on payment accounts. This has substantially facilitated the activity of payment service providers, creating uniform rules with respect to the provision of payment services and the information to be provided, reduced the administrative burden and generated cost savings for payment service providers.

(3) The smooth functioning of the internal market and the development of a modern, socially inclusive economy increasingly depends on the universal provision of payment services. Any new legislation in this regard must be part of a smart economic strategy for the Union, which must effectively take into account the needs of more vulnerable consumers.

(4) However, as indicated by the European Parliament in its resolution of 4 July 2012 with recommendations to the Commission on Access to Basic Banking Services, more must be done to improve and develop the internal market for retail banking. Currently, the lack of transparency and comparability of fees as well as the difficulties in switching payment accounts still create barriers to the deployment of a fully integrated market contributing to low competition in the retail banking sector. Those problems must be tackled and high-quality standards must be achieved.

(5) The current conditions of the internal market could deter payment service providers from exercising their freedom to establish or to provide services within the Union because of the difficulty in attracting customers when entering a new market. Entering new markets often entails large investment.

Such investment is only justified if the provider foresees sufficient opportunities and a corresponding demand from consumers. The low level of mobility of consumers with respect to retail financial services is to a large extent due to the lack of transparency and comparability as regards the fees and services on offer, as well as difficulties in relation to the switching of payment accounts. Those factors also stifle demand. This is particularly true in the cross-border context. (6) Moreover, significant barriers to the completion of the internal market in the area of payment accounts may be created by the fragmentation of existing national regulatory frameworks. Existing provisions at national level with respect to payment accounts, and particularly with respect to the comparability of fees and payment account switching, diverge. For switching, the lack of uniform binding measures at Union level has led to divergent practices and measures at national level. Those differences are even more marked in the area of comparability of fees, where no measures, even of a self-regulatory nature, exist at Union level. Should those differences become more significant in the future, as payment service providers tend to tailor their practices to national markets, this would raise the cost of operating across borders relative to the costs faced by domestic providers and would therefore make the pursuit of business on a cross-border basis less attractive. Cross-border activity in the internal market is hampered by obstacles to consumers opening a payment account abroad. Existing restrictive eligibility criteria may prevent Union citizens from moving freely within the Union. Providing all consumers with access to a payment account will permit their participation in the internal market and allow them to reap the benefits of the internal market.

[...]

(8) Transparency and comparability of fees were considered at Union level in a self-regulatory initiative, initiated by the banking industry. However, no final agreement was reached on that initiative. As regards switching, the common principles established in 2008 by the European Banking Industry Committee provide a model mechanism for switching between payment accounts offered by banks located in the same Member State.

[...]

(9) In order to support effective and smooth financial mobility in the long term, it is vital to establish a uniform set of rules to tackle the issue of low customer mobility, and in particular to improve comparison of payment account services and fees and to incentivise payment account switching, as well as to avoid discrimination on the basis of residency against consumers who intend to open and use a payment account on a cross-border basis. Moreover, it is essential to adopt adequate measures to foster consumers' participation in the payment accounts market. Those measures will incentivise entry for payment service providers in the internal market and ensure a level playing field, thereby strengthening competition and the efficient allocation of resources within the Union's financial retail market to the benefit of businesses and consumers. Also, transparent fee information and switching possibilities, combined with the right of access to a payment account with basic features, will allow Union citizens to move and shop around more easily within the Union, thereby benefitting from a fully functioning internal market in the area of retail financial services, and will contribute to the further development of the internal market.

[...]

(11) This Directive should not preclude Member States from retaining or adopting more stringent provisions in order to protect consumers, provided that such provisions are consistent with their obligations under Union law and this Directive.

[...]

(13) Since a payment account with basic features is a type of payment account for the purposes of this Directive, the provisions in respect of transparency and switching should also apply to such accounts.

[...]

(16) Consumers would benefit most from information that is concise, standardised and easy to compare between different payment service providers. The tools made available to consumers to compare payment account offers would not have a positive impact if the time invested in going through lengthy lists of fees for different offers outweighed the benefit of choosing the offer that represents the best value. Those tools should be multifold and consumer testing should be conducted. At this stage, fee terminology should only be standardised for the most representative terms and definitions within Member States in order to avoid the risk of excessive information and to facilitate swift implementation.

(17) The fee terminology should be determined by Member States, allowing for consideration of the specificities of local markets. To be considered representative, services should be subject to a fee at a minimum of one payment service provider in a Member State. In addition, where the services are common to a majority of Member States, the terminology used to define such services should be standardised at Union level, thus allowing for better comparison of payment account offers across the Union. [...]

(18) Once Member States have determined a provisional list of the most representative services subject to a fee at national level together with terms and definitions, EBA should review them to identify, by means of draft regulatory technical standards, the services that are common to the majority of Member States and propose standardised Union-level terms and definitions for them in all the official languages of the institutions of the Union. EBA should ensure that only one term is used for each service in any official language of each Member State which is also an official language of the institutions of the Union. This means that different terms can be used for the same service in different Member States sharing the same official language of the institutions of the Union, thereby taking into account national specificities. Member States should then integrate any applicable Union-level terms into their provisional lists and publish their final lists based on this.

[...]

(21) In order to ensure consistent use of applicable Union-level terminology across the Union, Member States should establish an obligation requiring payment service providers to use the applicable Union-level terminology together with the remaining national standardised terminology identified in the final list when communicating with consumers, including in the fee information document and the statement of fees. Payment service providers should be able to use brand names in their contractual, commercial and marketing information to consumers, as long as they clearly identify the applicable corresponding standardised term. Where they choose to use brand names in the fee information document or statement of fees, this should be in addition to the standardised terms as a secondary designation, such as in brackets or in a smaller font size.

(22) Comparison websites that are independent are an effective means for consumers to assess the merits of different payment account offers in one place. Such websites can provide the right balance between the need for information to be clear and concise and the need for it to be complete and comprehensive, by enabling users to obtain more detailed information where this is of interest to them. They should aim at including the broadest possible range of offers, so as to give

a representative overview, while also covering a significant part of the market. They can also reduce search costs as consumers will not need to collect information separately from payment service providers. It is crucial that the information given on such websites be trustworthy, impartial and transparent and that consumers be informed of the availability of such websites. In this regard, Member States should inform the public of such websites.

[...]

(26) Switching should not imply the transfer of the contract from the transferring payment service provider to the receiving payment service provider.

[...]

(29) The switching process should be as straightforward as possible for the consumer. Accordingly, Member States should ensure that the receiving payment service provider is responsible for initiating and managing the process on behalf of the consumer. Member States should be able to use additional means, such as a technical solution, when establishing the switching service. Such additional means may exceed the requirements of this Directive; for example, the switching service may be provided in a shorter time-frame or payment service providers may be required to ensure, upon a consumer's request, the automated or manual routing of credit transfers received on the former payment account to the new payment account for a set limited period starting from receipt of the authorisation to switch. Such additional means may also be used by payment service providers on a voluntary basis even where this is not required by a Member State.

(30) Consumers should be allowed to ask the receiving payment service provider to switch all or part of the incoming credit transfers, standing orders for credit transfers or direct debit mandates, ideally within a single meeting with the receiving payment service provider. To that end, consumers should be able to sign one authorisation giving consent to each of the abovementioned tasks. Member States could require that the authorisation from the consumer be in writing, but could also choose to accept equivalent means where appropriate, for example where an automated system for switching is in place. Before giving the authorisation, the consumer should be informed of all the steps of the procedure necessary to complete the switching. For example, the authorisation could include all the tasks that form part of the switching service and could allow for the possibility of the consumer choosing only some of those tasks.

[...]

(32) In order to facilitate cross-border account-opening, the consumer should be allowed to ask the new payment service provider to set up on the new payment account all or part of standing orders for credit transfers, accept direct debits from the date specified by the consumer, and provide the consumer with information giving details of the new payment account, preferably within a single meeting with the new payment service provider.

[...]

(34) Member States should guarantee that consumers who intend to open a payment account are not discriminated against on the basis of their nationality or place of residence. While it is important for credit institutions to ensure that their customers are not using the financial system for illegal purposes such as fraud, money laundering or terrorism financing, they should not impose barriers to consumers who want to benefit from the advantages of the internal market by opening and using payment accounts on a cross-border basis. Therefore, the provisions of Directive 2005/60/EC of the European Parliament and of the Council (9) should not be used as a pretext for rejecting commercially less attractive consumers.

[...]

(46) In order to ensure that payment accounts with basic features are available to the widest possible range of consumers, they should be offered free of charge or for a reasonable fee. To encourage unbanked vulnerable

consumers to participate in the retail banking market, Member States should be able to provide that payment accounts with basic features are to be offered to those consumers on particularly advantageous terms, such as free of charge. Member States should be free to define the mechanism to identify those consumers that can benefit from payment accounts with basic features on more advantageous terms, provided that the mechanism ensures that vulnerable consumers can access a payment account with basic features. In any event, such an approach should be without prejudice to the right of all consumers, including non-vulnerable ones, to access payment accounts with basic features at least at a reasonable fee. Furthermore, any additional charges to the consumer for non-compliance with the terms laid down in the contract should be reasonable. Member States should establish what constitutes a reasonable charge according to national circumstances.

(47) Credit institutions should refuse to open or should terminate a contract for a payment account with basic features only in specific circumstances, such as non-compliance with the legislation on money laundering and terrorist financing or on the prevention and investigation of crimes. Even in those cases, a refusal can only be justified where the consumer does not comply with that legislation and not because the procedure to check compliance with the legislation is too burdensome or costly. However, there could be cases where a consumer abuses his right to open and use a payment account with basic features. For example, a Member State should be able to permit credit institutions to take measures against consumers who have committed a crime, such as a serious fraud against a credit institution, with a view to avoiding a recurrence of such a crime. Such measures may include, for example, limiting access by that consumer to a payment account with basic features for a certain period of time. Besides, there may be cases in which the previous refusal of an application for a payment account may be necessary in order to identify consumers who could benefit from a payment account on more advantageous terms. In such a case, the credit institution should inform the consumer that he may use a specific mechanism in the event of refusal of an application for a payment account for which a fee is charged as provided for in this Directive to obtain access to a payment account with basic features that is free of charge. Both such additional cases should, however, be limited, specific and based on precisely identified provisions of national law. When identifying additional cases in which credit institutions can refuse to offer payment accounts to consumers, Member States should be able to include, inter alia, grounds of public security or public policy.

(48) Clear and comprehensible information on the right to open and use a payment account with basic features should be provided by Member States and credit institutions to consumers. Member States should ensure that communication measures are well-targeted and, in particular, that they reach out to unbanked, vulnerable and mobile consumers. Credit institutions should actively make available to consumers accessible information and adequate assistance about the specific features of the payment account with basic features on offer, their associated fees and their conditions of use, and also the steps consumers should take to exercise their right to open a payment account with basic features. In particular, consumers should be informed that the purchase of additional services is not compulsory in order to access a payment account with basic features.

[...]

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

Subject matter and scope

1. This Directive lays down rules concerning the transparency and comparability of fees charged to consumers on their

payment accounts held within the Union, rules concerning the switching of payment accounts within a Member State and rules to facilitate cross-border payment account-opening for consumers.

2. This Directive also defines a framework for the rules and conditions according to which Member States are required to guarantee a right for consumers to open and use payment accounts with basic features in the Union.

3. Chapters II and III apply to payment service providers.

4. Chapter IV applies to credit institutions.

Member States may decide to apply Chapter IV to payment service providers other than credit institutions.

5. Member States may decide not to apply all or part of this Directive to the entities referred to in Article 2(5) of Directive 2013/36/EU of the European Parliament and of the Council (17).

6. This Directive applies to payment accounts through which consumers are able at least to:

(a) place funds in a payment account;

(b) withdraw cash from a payment account;

(c) execute and receive payment transactions, including credit transfers, to and from a third party.

Member States may decide to apply all or part of this Directive to payment accounts other than those referred to in the first subparagraph.

7. The opening and use of a payment account with basic features pursuant to this Directive shall be in conformity with Directive 2005/60/EC.

Article 2

Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'consumer' means any natural person who is acting for purposes which are outside his trade, business, craft or profession;

(2) 'legally resident in the Union' means where a natural person has the right to reside in a Member State by virtue of Union or national law, including consumers with no fixed address and persons seeking asylum under the Geneva Convention of 28 July 1951 Relating to the Status of Refugees, the Protocol thereto of 31 January 1967 and other relevant international treaties;

(3) 'payment account' means an account held in the name of one or more consumers which is used for the execution of payment transactions;

(4) 'payment service' means a payment service as defined in point (3) of Article 4 of Directive 2007/64/EC;

(5) 'payment transaction' means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

(6) 'services linked to the payment account' means all services related to the opening, operating and closing of a payment account, including payment services and payment transactions falling within the scope of point (g) of Article 3 of Directive 2007/64/EC and overdraft facilities and overrunning;

(7) 'payment service provider' means a payment service provider as defined in point (9) of Article 4 of Directive 2007/64/EC;

(8) 'credit institution' means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council (18);

(9) 'payment instrument' means a payment instrument as defined in point (23) of Article 4 of Directive 2007/64/EC;

(10) 'transferring payment service provider' means the payment service provider from which the information required to perform the switching is transferred;

(11) 'receiving payment service provider' means the payment service provider to which the information required to perform the switching is transferred;

- (12) 'payment order' means any instruction by a payer or payee to his payment service provider requesting the execution of a payment transaction;
- (13) 'payer' means a natural or legal person who holds a payment account and allows a payment order from that payment account or, where there is no payer's payment account, a natural or legal person who makes a payment order to a payee's payment account;
- (14) 'payee' means a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction;
- (15) 'fees' means all charges and penalties, if any, payable by the consumer to the payment service provider for or in relation to services linked to a payment account;
- (16) 'credit interest rate' means any rate at which interest is paid to the consumer in respect of funds held in a payment account;
- (17) 'durable medium' means any instrument which enables the consumer to store information addressed personally to that consumer in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;
- (18) 'switching' or 'switching service' means, upon a consumer's request, transferring from one payment service provider to another either the information about all or some standing orders for credit transfers, recurring direct debits and recurring incoming credit transfers executed on a payment account, or any positive payment account balance from one payment account to the other, or both, with or without closing the former payment account;
- (19) 'direct debit' means a national or cross-border payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent;
- (20) 'credit transfer' means a national or cross-border payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the payment service provider which holds the payer's payment account, based on an instruction given by the payer;
- (21) 'standing order' means an instruction given by the payer to the payment service provider which holds the payer's payment account to execute credit transfers at regular intervals or on predetermined dates;
- (22) 'funds' means banknotes and coins, scriptural money, and electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council (19);
- (23) 'framework contract' means a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account;
- (24) 'business day' means a day on which the relevant payment service provider is open for business as required for the execution of a payment transaction;
- (25) 'overdraft facility' means an explicit credit agreement whereby a payment service provider makes available to a consumer funds which exceed the current balance in the consumer's payment account;
- (26) 'overrunning' means a tacitly accepted overdraft whereby a payment service provider makes available to a consumer funds which exceed the current balance in the consumer's payment account or the agreed overdraft facility;
- (27) 'competent authority' means an authority designated as competent by a Member State in accordance with Article 21.

CHAPTER II COMPARABILITY OF FEES CONNECTED WITH PAYMENT ACCOUNTS

Article 3

List of the most representative services linked to a payment account and subject to a fee at national level and standardised terminology

1. Member States shall establish a provisional list of at least 10 and no more than 20 of the most representative services linked to a payment account and subject to a fee, offered by at least one payment service provider at national level. The list shall contain terms and definitions for each of the services identified. In any official language of a Member State, only one term shall be used for each service.

2. For the purposes of paragraph 1, the Member States shall have regard to the services that:

(a) are most commonly used by consumers in relation to their payment account;

(b) generate the highest cost for consumers, both overall as well as per unit.

In order to ensure the sound application of the criteria set out in the first subparagraph of this paragraph, EBA shall issue guidelines pursuant to Article 16 of Regulation (EU) No 1093/2010 by 18 March 2015.

3. Member States shall notify to the Commission and to EBA the provisional lists referred to in paragraph 1 by 18 September 2015. On request, Member States shall provide the Commission with supplementary information concerning the data on the basis of which they have compiled those lists with regard to the criteria set out in paragraph 2.

[...]

5. Member States shall integrate the Union standardised terminology established under paragraph 4 into the provisional list referred to in paragraph 1 and shall publish the resulting final list of the most representative services linked to a payment account without delay and at the latest within three months after the delegated act referred to in paragraph 4 has entered into force.

6. Every four years, following publication of the final list referred to in paragraph 5, Member States shall assess and, where appropriate, update the list of the most representative services established pursuant to paragraphs 1 and 2. They shall notify to the Commission and to EBA the outcome of their assessment and, where applicable, of the updated list of the most representative services. EBA shall review and, where necessary, update the Union standardised terminology, in accordance with the process set out in paragraph 4. Upon the Union standardised terminology being updated, Member States shall update and publish their final list as referred to in paragraph 5 and shall ensure that payment service providers use the updated terms and definitions.

Article 4

Fee information document and glossary

1. Without prejudice to Article 42(3) of Directive 2007/64/EC and Chapter II of Directive 2008/48/EC, Member States shall ensure that, in good time before entering into a contract for a payment account with a consumer, payment service providers provide the consumer with a fee information document on paper or another durable medium containing the standardised terms in the final list of the most representative services linked to a payment account referred to in Article 3(5) of this Directive and, where such services are offered by a payment service provider, the corresponding fees for each service.

2. The fee information document shall:

(a) be a short and stand-alone document;

(b) be presented and laid out in a way that is clear and easy to read, using characters of a readable size;

(c) be no less comprehensible in the event that, having been originally produced in colour, it is printed or photocopied in black and white;

(d) be written in the official language of the Member State where the payment account is offered or, if agreed by the consumer and the payment service provider, in another language;

(e) be accurate, not misleading and expressed in the currency of the payment account or, if agreed by the consumer and the payment service provider, in another currency of the Union;

(f) contain the title 'fee information document' at the top of the first page next to a common symbol to distinguish the document from other documentation; and

(g) include a statement that it contains fees for the most representative services related to the payment account and that complete pre-contractual and contractual information on all the services is provided in other documents.

Member States may determine that, for the purposes of paragraph 1, the fee information document shall be provided together with information required pursuant to other Union or national legislative acts on payment accounts and related services on the condition that all the requirements of the first subparagraph of this paragraph are met.

3. Where one or more services are offered as part of a package of services linked to a payment account, the fee information document shall disclose the fee for the entire package, the services included in the package and their quantity, and the additional fee for any service that exceeds the quantity covered by the package fee.

4. Member States shall establish an obligation for payment service providers to make available to consumers a glossary of at least the standardised terms set out in the final list referred to in Article 3(5) and the related definitions.

Member States shall ensure that the glossary provided pursuant to the first subparagraph, including other definitions, if any, is drafted in clear, unambiguous and non-technical language and that it is not misleading.

5. The fee information document and the glossary shall be made available to consumers at any time by payment service providers. They shall be provided in an easily accessible manner, including to non-customers, in electronic form on their websites where available and in the premises of payment service providers accessible to consumers. They shall also be provided on paper or another durable medium free of charge upon request by a consumer.

[...]

Article 5

Statement of fees

1. Without prejudice to Articles 47 and 48 of Directive 2007/64/EC and Article 12 of Directive 2008/48/EC, Member States shall ensure that payment service providers provide the consumer, at least annually and free of charge, with a statement of all fees incurred, as well as, where applicable, information regarding the interest rates referred to in points (c) and (d) of paragraph 2 of this Article, for services linked to a payment account. Where applicable, payment service providers shall use the standardised terms set out in the final list referred to in Article 3(5) of this Directive.

The communication channel used to provide the statement of fees shall be agreed with the consumer. The statement of fees shall be provided on paper at least upon the request of the consumer.

2. The statement of fees shall specify at least the following information:

(a) the unit fee charged for each service and the number of times the service was used during the relevant period, and where the services are combined in a package, the fee charged for the package as a whole, the number of times the package fee was charged during the relevant period and the additional fee charged for any service exceeding the quantity covered by the package fee;

(b) the total amount of fees incurred during the relevant period for each service, each package of services provided and services exceeding the quantity covered by the package fee;

(c) the overdraft interest rate applied to the payment account and the total amount of interest charged relating to the overdraft during the relevant period, where applicable;

(d) the credit interest rate applied to the payment account and the total amount of interest earned during the relevant period, where applicable;

(e) the total amount of fees charged for all services provided during the relevant period.

3. The statement of fees shall:

(a) be presented and laid out in a way that is clear and easy to read, using characters of a readable size;

(b) be accurate, not misleading and expressed in the currency of the payment account or, if agreed by the consumer and the payment service provider, in another currency;

(c) contain the title 'statement of fees' at the top of the first page of the statement next to a common symbol to distinguish the document from other documentation; and

(d) be written in the official language of the Member State where the payment account is offered or, if agreed by the consumer and the payment service provider, in another language.

Member States may determine that the statement of fees shall be provided together with information required pursuant to other Union or national legislative acts on payment accounts and related services as long as all the requirements of the first subparagraph are met.

4. EBA, after consulting national authorities and after consumer testing, shall develop implementing technical standards regarding a standardised presentation format of the statement of fees and its common symbol.

EBA shall submit the draft implementing technical standards referred to in the first subparagraph to the Commission by 18 September 2016.

Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph of this paragraph in accordance with Article 15 of Regulation (EU) No 1093/2010.

5. Following the updating of the Union standardised terminology pursuant to Article 3(6), EBA shall, where necessary, review and update the standardised presentation format of the statement of fees and its common symbol, following the procedure set out in paragraph 4 of this Article.

Article 6

Information for consumers

1. Member States shall ensure that in their contractual, commercial and marketing information to consumers, payment service providers use, where applicable, the standardised terms set out in the final list referred to in Article 3(5). Payment service providers may use brand names in the fee information document and in the statement of fees, provided such brand names are used in addition to the standardised terms set out in the final list referred to in Article 3(5) as a secondary designation of those services.

2. Payment service providers may use brand names to designate their services in their contractual, commercial and marketing information to consumers, provided that they clearly identify, where applicable, the corresponding standardised terms set out in the final list referred to in Article 3(5).

Article 7

Comparison websites

1. Member States shall ensure that consumers have access, free of charge, to at least one website comparing fees charged by payment service providers for at least the services included in the final list referred to in Article 3(5) at national level.

Comparison websites may be operated either by a private operator or by a public authority.

2. Member States may require the comparison websites referred to in paragraph 1 to include further comparative determinants relating to the level of service offered by the payment service provider.

3. The comparison websites established in accordance with paragraph 1 shall:

(a) be operationally independent by ensuring that payment service providers are given equal treatment in search results;

(b) clearly disclose their owners;

(c) set out clear, objective criteria on which the comparison will be based;

(d) use plain and unambiguous language and, where applicable, the standardised terms set out in the final list referred to in Article 3(5);

(e) provide accurate and up-to-date information and state the time of the last update;

(f) include a broad range of payment account offers covering a significant part of the market and, where the information presented is not a complete overview of the market, a clear statement to that effect, before displaying results; and

(g) provide an effective procedure to report incorrect information on published fees.

4. Member States shall ensure that information is made available online about the availability of websites that comply with this Article.

Article 8

Payment accounts packaged with another product or service Member States shall ensure that, when a payment account is offered as part of a package together with another product or service which is not linked to a payment account, the payment service provider informs the consumer whether it is possible to purchase the payment account separately and, if so, provides separate information regarding the costs and fees associated with each of the other products and services offered in that package that can be purchased separately.

CHAPTER III

SWITCHING

Article 9

Provision of the switching service

Member States shall ensure that payment service providers provide a switching service as described in Article 10 between payment accounts held in the same currency to any consumer who opens or holds a payment account with a payment service provider located in the territory of the Member State concerned.

Article 10

The switching service

1. Member States shall ensure that the switching service is initiated by the receiving payment service provider at the request of the consumer. The switching service shall at least comply with paragraphs 2 to 6.

Member States may establish or maintain measures alternative to those referred to in paragraphs 2 to 6, provided that:

(a) it is clearly in the interest of the consumer;

(b) there is no additional burden for the consumer; and

(c) the switching is completed within, as a maximum, the same overall time-frame as that indicated in paragraphs 2 to 6.

2. The receiving payment service provider shall perform the switching service upon receipt of the authorisation from the consumer. In the case of two or more holders of the account, authorisation shall be obtained from each of them.

The authorisation shall be drawn up in an official language of the Member State where the switching service is being initiated or in any other language agreed between the parties. The authorisation shall allow the consumer to provide specific consent to the performance by the transferring payment service provider of each of the tasks referred to in paragraph 3 and to provide specific consent to the performance by the receiving payment service provider of each of the tasks referred to in paragraph 5.

The authorisation shall allow the consumer to specifically identify incoming credit transfers, standing orders for credit transfers and direct debit mandates that are to be switched. The authorisation shall also allow consumers to specify the date from which standing orders for credit transfers and direct debits are to be executed from the payment account opened or held with the receiving payment service provider. That date shall be at least six business days after the date on which the receiving payment service provider receives the documents transferred from the transferring payment service provider pursuant to paragraph 4. Member States may

require the authorisation from the consumer to be in writing and that a copy of the authorisation be provided to the consumer.

3. Within two business days from receipt of the authorisation referred to in paragraph 2, the receiving payment service provider shall request the transferring payment service provider to carry out the following tasks, if provided for in the consumer's authorisation:

(a) transmit to the receiving payment service provider and, if specifically requested by the consumer, to the consumer, a list of the existing standing orders for credit transfers and available information on direct debit mandates that are being switched;

(b) transmit to the receiving payment service provider and, if specifically requested by the consumer, to the consumer, the available information about recurring incoming credit transfers and creditor-driven direct debits executed on the consumer's payment account in the previous 13 months;

(c) where the transferring payment service provider does not provide a system for automated redirection of the incoming credit transfers and direct debits to the payment account held by the consumer with the receiving payment service provider, stop accepting direct debits and incoming credit transfers with effect from the date specified in the authorisation;

(d) cancel standing orders with effect from the date specified in the authorisation;

(e) transfer any remaining positive balance to the payment account opened or held with the receiving payment service provider on the date specified by the consumer; and

(f) close the payment account held with the transferring payment service provider on the date specified by the consumer.

4. Upon receipt of a request from the receiving payment service provider, the transferring payment service provider shall carry out the following tasks, if provided for in the consumer's authorisation:

(a) send the receiving payment service provider the information referred to in points (a) and (b) of paragraph 3 within five business days;

(b) where the transferring payment service provider does not provide a system for automated redirection of the incoming credit transfers and direct debits to the payment account held or opened by the consumer with the receiving payment service provider, stop accepting incoming credit transfers and direct debits on the payment account with effect from the date specified in the authorisation. Member States may require the transferring payment service provider to inform the payer or the payee of the reason for not accepting the payment transaction;

(c) cancel standing orders with effect from the date specified in the authorisation;

(d) transfer any remaining positive balance from the payment account to the payment account opened or held with the receiving payment service provider on the date specified in the authorisation;

(e) without prejudice to Article 45(1) and (6) of Directive 2007/64/EC, close the payment account on the date specified in the authorisation if the consumer has no outstanding obligations on that payment account and provided that the actions listed in points (a), (b) and (d) of this paragraph have been completed. The payment service provider shall immediately inform the consumer where such outstanding obligations prevent the consumer's payment account from being closed.

5. Within five business days of receipt of the information requested from the transferring payment service provider as referred to in paragraph 3, the receiving payment service provider shall, as and if provided for in the authorisation and to the extent that the information provided by the transferring payment service provider or the consumer enables the receiving payment service provider to do so, carry out the following tasks:

(a) set up the standing orders for credit transfers requested by the consumer and execute them with effect from the date specified in the authorisation;

(b) make any necessary preparations to accept direct debits and accept them with effect from the date specified in the authorisation;

(c) where relevant, inform consumers of their rights pursuant to point (d) of Article 5(3) of Regulation (EU) No 260/2012;

(d) inform payers specified in the authorisation and making recurring incoming credit transfers into a consumer's payment account of the details of the consumer's payment account with the receiving payment service provider and transmit to the payers a copy of the consumer's authorisation. If the receiving payment service provider does not have all the information it needs to inform the payers, it shall ask the consumer or the transferring payment service provider to provide the missing information;

(e) inform payees specified in the authorisation and using a direct debit to collect funds from the consumer's payment account of the details of the consumer's payment account with the receiving payment service provider and the date from which direct debits are to be collected from that payment account and transmit to the payees a copy of the consumer's authorisation. If the receiving payment service provider does not have all the information it needs to inform the payees, it shall ask the consumer or the transferring payment service provider to provide the missing information.

Where the consumer chooses to personally provide the information referred to in points (d) and (e) of the first subparagraph of this paragraph to the payers or payees rather than provide specific consent in accordance with paragraph 2 to the receiving payment service provider to do so, the receiving payment service provider shall provide the consumer with standard letters providing details of the payment account and the starting date specified in the authorisation within the deadline referred to in the first subparagraph of this paragraph.

6. Without prejudice to Article 55(2) of Directive 2007/64/EC, the transferring payment service provider shall not block payment instruments before the date specified in the consumer's authorisation, so that the provision of payment services to the consumer is not interrupted in the course of the provision of the switching service.

Article 11

Facilitation of cross-border account-opening for consumers

1. Member States shall ensure that where a consumer indicates to his payment service provider that he wishes to open a payment account with a payment service provider located in another Member State, the payment service provider with which the consumer holds a payment account shall on receipt of such request provide the following assistance to the consumer:

(a) provide the consumer free of charge with a list of all the currently active standing orders for credit transfers and debtor-driven direct debit mandates, where available, and with available information about recurring incoming credit transfers and creditor-driven direct debits executed on the consumer's payment account in the previous 13 months. That list shall not entail any obligation on the part of the new payment service provider to set up services that it does not provide;

(b) transfer any positive balance remaining on the payment account held by the consumer to the payment account opened or held by the consumer with the new payment service provider, provided that the request includes full details allowing the new payment service provider and the consumer's payment account to be identified;

(c) close the payment account held by the consumer.

2. Without prejudice to Articles 45(1) and 45(6) of Directive 2007/64/EC and if the consumer has no outstanding obligations on a payment account, the payment service provider with which the consumer holds that payment account shall conclude the steps set out in points (a), (b) and

(c) of paragraph 1 of this Article on the date specified by the consumer, which shall be at least six business days after that payment service provider receives the consumer's request unless otherwise agreed between the parties. The payment service provider shall immediately inform the consumer where outstanding obligations prevent his payment account from being closed.

Article 12

Fees connected with the switching service

1. Member States shall ensure that consumers are able to access free of charge their personal information regarding existing standing orders and direct debits held by either the transferring or the receiving payment service provider.

2. Member States shall ensure that the transferring payment service provider provides the information requested by the receiving payment service provider pursuant to point (a) of Article 10(4) without charging the consumer or the receiving payment service provider.

3. Member States shall ensure that fees, if any, applied by the transferring payment service provider to the consumer for the termination of the payment account held with it are determined in accordance with Article 45(2), (4) and (6) of Directive 2007/64/EC.

4. Member States shall ensure that fees, if any, applied by the transferring or the receiving payment service provider to the consumer for any service provided under Article 10, other than those referred to in paragraphs 1, 2 and 3 of this Article, are reasonable and in line with the actual costs of that payment service provider.

Article 13

Financial loss for consumers

1. Member States shall ensure that any financial loss, including charges and interest, incurred by the consumer and resulting directly from the non-compliance of a payment service provider involved in the switching process with its obligations under Article 10 is refunded by that payment service provider without delay.

2. Liability under paragraph 1 shall not apply in cases of abnormal and unforeseeable circumstances beyond the control of the payment service provider pleading for the application of those circumstances, the consequences of which would have been unavoidable despite all efforts to the contrary, or where a payment service provider is bound by other legal obligations covered by Union or national legislative acts.

3. Member States shall ensure that liability under paragraphs 1 and 2 is established in accordance with the legal requirements applicable at national level.

[...]

CHAPTER IV

ACCESS TO PAYMENT ACCOUNTS

Article 15

Non-discrimination

Member States shall ensure that credit institutions do not discriminate against consumers legally resident in the Union by reason of their nationality or place of residence or by reason of any other ground as referred to in Article 21 of the Charter, when those consumers apply for or access a payment account within the Union. The conditions applicable to holding a payment account with basic features shall be in no way discriminatory.

Article 16

Right of access to a payment account with basic features

1. Member States shall ensure that payment accounts with basic features are offered to consumers by all credit institutions or a sufficient number of credit institutions to guarantee access thereto for all consumers in their territory, and to prevent distortions of competition. Member States shall ensure that payment accounts with basic features are

not only offered by credit institutions that provide payment accounts with solely online facilities.

2. Member States shall ensure that consumers legally resident in the Union, including consumers with no fixed address and asylum seekers, and consumers who are not granted a residence permit but whose expulsion is impossible for legal or factual reasons, have the right to open and use a payment account with basic features with credit institutions located in their territory. Such a right shall apply irrespective of the consumer's place of residence.

Member States may, in full respect of the fundamental freedoms guaranteed by the Treaties, require consumers who wish to open a payment account with basic features in their territory to show a genuine interest in doing so.

Member States shall ensure that the exercise of the right is not made too difficult or burdensome for the consumer.

3. Member States shall ensure that credit institutions offering payment accounts with basic features open the payment account with basic features or refuse a consumer's application for a payment account with basic features, in each case without undue delay and at the latest 10 business days after receiving a complete application.

4. Member States shall ensure that credit institutions refuse an application for a payment account with basic features where opening such an account would result in an infringement of the provisions on the prevention of money laundering and the countering of terrorist financing laid down in Directive 2005/60/EC.

5. Member States may permit credit institutions that offer payment accounts with basic features to refuse an application for such an account where a consumer already holds a payment account with a credit institution located in their territory which allows him to make use of the services listed in Article 17(1), save where a consumer declares that he has received notice that a payment account will be closed.

In such cases, before opening a payment account with basic features, the credit institution may verify whether the consumer holds or does not hold a payment account with a credit institution located in the same Member State which enables consumers to make use of the services listed in Article 17(1). Credit institutions may rely on a declaration of honour signed by consumers for that purpose.

6. Member States may identify limited and specific additional cases where credit institutions may be required or may choose to refuse an application for a payment account with basic features. Such cases shall be based on provisions of national law applicable in their territory and shall be aimed either at facilitating access by the consumer to a payment account with basic features free of charge under the mechanism of Article 25 or at avoiding abuses by consumers of their right to access a payment account with basic features.

7. Member States shall ensure that, in the cases referred to in paragraphs 4, 5 and 6, after taking its decision, the credit institution immediately informs the consumer of the refusal and of the specific reason for that refusal, in writing and free of charge, unless such disclosure would be contrary to objectives of national security, public policy or Directive 2005/60/EC. In the event of refusal, the credit institution shall advise the consumer of the procedure to submit a complaint against the refusal, and of the consumer's right to contact the relevant competent authority and designated alternative dispute resolution body and provide the relevant contact details.

8. Member States shall ensure that, in the cases referred to in paragraph 4, the credit institution adopts appropriate measures pursuant to Chapter III of Directive 2005/60/EC.

9. Member States shall ensure that access to a payment account with basic features is not made conditional on the purchase of additional services or of shares in the credit institution, unless the latter is conditional for all customers of the credit institution.

10. Member States shall be deemed to comply with the obligations laid down in Chapter IV where an existing binding framework ensures its full application in a sufficiently clear

and precise manner so that the persons concerned can ascertain the full extent of their rights and rely on them before the national courts.

Article 17

Characteristics of a payment account with basic features

1. Member States shall ensure that a payment account with basic features includes the following services:

(a) services enabling all the operations required for the opening, operating and closing of a payment account;

(b) services enabling funds to be placed in a payment account;

(c) services enabling cash withdrawals within the Union from a payment account at the counter or at automated teller machines during or outside the credit institution's opening hours;

(d) execution of the following payment transactions within the Union:

(i) direct debits;

(ii) payment transactions through a payment card, including online payments;

(iii) credit transfers, including standing orders, at, where available, terminals and counters and via the online facilities of the credit institution.

The services listed in points (a) to (d) of the first subparagraph shall be offered by credit institutions to the extent that they already offer them to consumers holding payment accounts other than a payment account with basic features.

2. Member States may establish an obligation requiring credit institutions established in their territory to provide additional services, which are considered essential for consumers based on common practice at national level, with a payment account with basic features.

3. Member States shall ensure that payment accounts with basic features are offered by credit institutions established in their territory at least in the national currency of the Member State concerned.

4. Member States shall ensure that a payment account with basic features allows consumers to execute an unlimited number of operations in relation to the services referred to in paragraph 1.

5. With respect to the services referred to in points (a), (b), (c) and (d)(ii) of paragraph 1 of this Article excluding payment transactions through a credit card, Member States shall ensure that credit institutions do not charge any fees beyond the reasonable fees, if any, referred to in Article 18, irrespective of the number of operations executed on the payment account.

6. With respect to the services referred to in point (d)(i) of paragraph 1 of this Article, point d(ii) of paragraph 1 of this Article only as regards payment transactions through a credit card and point (d)(iii) of paragraph 1 of this Article, Member States may determine a minimum number of operations for which credit institutions can only charge the reasonable fees, if any, referred to in Article 18. Member States shall ensure that the minimum number of operations is sufficient to cover the personal use by the consumer, taking into account existing consumer behaviour and common commercial practices. The fees charged for operations above the minimum number of operations shall never be higher than those charged under the usual pricing policy of the credit institution.

7. Member States shall ensure that the consumer is able to manage and initiate payment transactions from the consumer's payment account with basic features in the credit institution's premises and/or via online facilities, where available.

8. Without prejudice to the requirements laid down in Directive 2008/48/EC, Member States may allow credit institutions to provide, upon the consumer's request, an overdraft facility in relation to a payment account with basic features. Member States may define a maximum amount and a maximum duration of any such overdraft. Access to, or use of, the payment account with basic features shall not be

restricted by, or made conditional on, the purchase of such credit services.

Article 18

Associated fees

1. Member States shall ensure that the services referred to in Article 17 are offered by credit institutions free of charge or for a reasonable fee.

2. Member States shall ensure that the fees charged to the consumer for non-compliance with the consumer's commitments laid down in the framework contract are reasonable.

3. Member States shall ensure that the reasonable fees referred to in paragraphs 1 and 2 are established taking into account at least the following criteria:

(a) national income levels;

(b) average fees charged by credit institutions in the Member State concerned for services provided on payment accounts.

4. Without prejudice to the right referred to in Article 16(2) and the obligation contained in paragraph 1 of this Article, Member States may require credit institutions to implement various pricing schemes depending on the level of banking inclusion of the consumer, allowing for, in particular, more advantageous conditions for unbanked vulnerable consumers. In such cases, Member States shall ensure that consumers are provided with guidance, as well as adequate information, on the available options.

[...]

Article 25

Mechanism in the event of refusal of a payment account for which a fee is charged

Without prejudice to Article 16, Member States may set up a specific mechanism to ensure that consumers who do not have a payment account in their territory and who have been denied access to a payment account for which a fee is charged by credit institutions will have effective access to a payment account with basic features, free of charge.

[...]

CHAPTER VII

FINAL PROVISIONS

[...]

Article 29

Transposition

By 18 September 2016, Member States shall adopt and publish the laws, Regulations and administrative provisions necessary to comply with this Directive. They shall immediately communicate to the Commission the text of those measures.

2. They shall apply the measures referred to in paragraph 1 from 18 September 2016.

By way of derogation from the first subparagraph:

(a) Article 3 shall apply from 17 September 2014;

(b) Member States shall apply the measures necessary to comply with Article 4(1) to (5), Article 5(1), (2) and (3), Article 6(1) and (2) and Article 7 by nine months after the entry into force of the delegated act referred to in Article 3(4);

(c) Member States in which the equivalent of a fee information document at national level already exists may choose to integrate the common format and its common symbol at the latest 18 months after the entry into force of the delegated act referred to in Article 3(4);

(d) Member States in which the equivalent of a statement of fees at national level already exists may choose to integrate the common format and its common symbol at the latest 18 months after the entry into force of the delegated act referred to in Article 3(4).

3. When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

4. Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.

Article 30

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 31

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels, 23 July 2014.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

S. GOZI

[...]

Relevant Case-Law on Payments and Payment Frauds

C-616/11 T-Mobile Austria

Judgment of the Court (Fifth Chamber) of 9 April 2014
(request for a preliminary ruling from the Oberster
Gerichtshof — Austria) — 2014/C 175/04

Re: Request for a preliminary ruling — Oberster Gerichtshof — Interpretation of Article 4.23 and Article 52(3) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ 2007 L 319, p. 1) — Scope — Concept of 'payment instrument' — Provisions of national law which lay down a general prohibition of the imposition of handling charges in respect of the use of a payment instrument — Contract between a mobile phone operator and an individual — Payment by way of signed cash payment form, by transfer of cash payment form, or by transfer through online banking

Operative part of the judgment

1) Article 52(3) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC must be interpreted as being applicable to the use of a payment instrument in the course of the contractual relationship between a mobile phone operator, as payee, and that operator's customer, as payer.

2) Article 4.23 of Directive 2007/64 must be interpreted as meaning that both the procedure for ordering transfers by means of a transfer order form signed by the payer in person and the procedure for ordering transfers through online banking constitute payment instruments within the meaning of that provision.

3) Article 52(3) of Directive 2007/64 must be interpreted as meaning that it gives Member States the power to prohibit

generally payees from levying charges on the payer for the use of any payment instrument, if the national legislation, as a whole, takes into account the need to encourage competition and the use of efficient payment instruments, which is for the referring court to ascertain.

C-494/12 Dixons Retail plc v Commissioners for Her Majesty's Revenue and Customs

Judgment of the Court (Second Chamber) of 21 November 2013 (request for a preliminary ruling from the First-tier Tribunal (Tax Chamber) — United Kingdom) – 2014/C 39/11

(Directive 2006/112/EC - Value added tax - Supply of goods - Concept - Fraudulent use of a bank card)

Re: Request for a preliminary ruling — First-tier Tribunal (Tax Chamber) — Interpretation of Articles 14(1) and 73 of Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (OJ 2006 L 347, p. 1) — Concept of 'supply of goods' — Supply following a purchase made by means of the unauthorised and fraudulent use of a credit card

Operative part of the judgment

Articles 2(1), 5(1) and 11A(1)(a) of Sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the Member States relating to turnover taxes — Common system of value added tax: uniform basis of assessment and Articles 2(1)(a), 14(1) and 73 of Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax must be interpreted as meaning that, in circumstances such as those at issue in the main proceedings, the physical transfer of goods to a purchaser who fraudulently uses a bank card as a means of payment constitutes a 'supply of goods' within the meaning of Articles 2(1) and 5(1) of Directive 77/388 and Articles 2(1)(a) and 14(1) of Directive 2006/112 and that, in the context of such a transfer, the payment made by a third party, under an agreement concluded between it and the supplier of those goods by which the third party has undertaken to pay the supplier for the goods sold by the latter to purchasers using such a card as a means of payment, constitutes 'consideration' within the meaning of Article 11A(1)(a) of Directive 77/388 and Article 73 of Directive 2006/112.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE COMP/34.579 — MasterCard, Case COMP/36.518 — EuroCommerce, Case COMP/38.580 — Commercial Cards

Text with EEA relevance

Summary of Commission Decision of 19 December 2007 relating to a proceeding under Article 81 of the EC Treaty and Article 53 of the EEA Agreement (2009/C 264/04, notified under document C(2007) 6474)

(Only the English text is authentic)

On 19 December 2007, the Commission adopted a decision relating to a proceeding under Article 81 of the EC Treaty and Article 53 of the EEA Agreement (the Decision). In accordance with the provisions of Article 30 of Council Regulation (EC) No 1/2003 [1], the Commission herewith publishes the names of the parties and the main content of the Decision, having regard to the legitimate interest of undertakings in the protection of their business interests. A non-confidential version of the Decision is available on the Directorate-General for Competition's website at the following address: <http://europa.eu.int/comm/competition/antitrust/cases/in dex/>

1. INTRODUCTION

(1) The Decision finds that the MasterCard payment organisation and the entities representing it, that is MasterCard Incorporated, MasterCard International Incorporated and MasterCard Europe SPRL, have infringed Article 81 of the Treaty and Article 53 of the EEA Agreement by in effect setting a minimum price merchants must pay to their acquiring bank for accepting payment cards in the European Economic Area, by means of the Intra-EEA fallback interchange fees for MasterCard branded consumer credit and charge cards and for MasterCard or Maestro branded debit cards.

2. CASE DESCRIPTION

2.1. The proceedings

(2) The procedure was initiated on the basis of a complaint submitted on 30 March 1992 by the British Retail Consortium (BRC), a trade association representing UK retailers. In its complaint the BRC alleged that each of Europay International SA and Visa restricted competition by its arrangements on cross-border interchange fees.

(3) The BRC complaint was withdrawn when a similar complaint was filed by EuroCommerce, a retail, wholesale and international trade representation in the European Union, on 23 May 1997. This complaint addresses certain practices and rules of MasterCard and Visa, in particular multilaterally agreed interchange fees.

(4) In the time between 22 May 1992 and 1 July 1995 Europay notified the network rules of the Europay payment card association including those on multilateral interchange fees.

(5) On 22 November 2002 the Commission opened an ex-officio investigation regarding Visa's and MasterCard's respective intra-EEA interchange fees for commercial cards.

(6) On 25 July 2003 MasterCard informed the Commission of its intention to initiate proceedings under Article 232 of the EC Treaty (failure to act) unless the Commission took a formal position with respect to MasterCard's intra-EEA interchange fees.

(7) On 24 September 2003 and 21 June 2006 the Commission sent two Statements of Objections to MasterCard Europe SPRL, the legal successor of Europay, as well as to MasterCard International Inc. and MasterCard Incorporated addressing the organisation's network rules and decisions on intra-EEA interchange fees.

(8) On 14 and 15 November 2006 MasterCard exercised its right to be heard in an oral hearing. The hearing was also attended by EuroCommerce and nine third parties.

(9) On 23 March 2007 the Commission sent a letter to MasterCard (letter of facts) providing MasterCard with access to documents collected since MasterCard had access to the file in July and August 2006 and setting out possible conclusions the Commission intended to draw from the new facts in the Decision.

(10) On 13 December 2007 the Advisory Committee gave a favourable opinion on the draft Commission Decision.

2.2. The facts

(11) MasterCard operates an international "open" or "four-party" point of sales (POS) payment system. MasterCard's payment cards system enables consumers to use plastic cards for payment transactions at POS, which is — most often — a payment terminal in a merchant outlet. Such a system involves five main groups of players: (i) cardholders; (ii) merchants; (iii) the scheme owner (here: MasterCard); (iv) card issuing banks; and (v) acquiring banks. Issuers issue cards to cardholders and acquirers recruit merchants for payment card acceptance.

(12) The Decision deals with MasterCard's network rules and decisions of its member bank delegates and the organisation's management on Intra-EEA fallback interchange fees and SEPA fallback interchange fees. These multilateral interchange fees (MIFs) are retained for each payment card transaction. Under the MasterCard organisation's network rules the acquiring banks pay interchange fees to the issuing banks. When the cardholder uses his or her card to buy from the merchant, the merchant receives from the acquiring bank the retail price

less a merchant service charge. The issuing bank pays the acquiring bank the retail price minus an interchange fee. In addition to the interchange fee from the acquiring bank, the issuing bank receives from the customer the value of the payment plus any annual fee, any interest payment on debt outstanding, late payment fees, etc.

(13) Intra-EEA fallback interchange fees and SEPA fallback interchange fees apply to cross-border card payments in the European Economic Area (EEA) and domestic card payments within several Member States of the EEA with MasterCard or Maestro branded payment cards. The fees are "fallback" fees in the sense that they are only charged in the absence of specific bilateral agreements between an issuing and an acquiring bank on interchange fees.

3. LEGAL ASSESSMENT

Article 81(1) of the Treaty

(14) The MIF in MasterCard's scheme restricts competition between acquiring banks by inflating the base on which acquiring banks set charges to merchants and thereby setting a floor under the merchant fee. In the absence of the multilateral interchange fee the merchant fees set by acquiring banks would be lower.

(15) The MasterCard's European Board (...) [**] and/or the Global Board (...) [**] decisions on the level and structure of Intra-EEA fallback interchange fees and the related network rules adopted by the Global Board of MasterCard International Inc. are decisions of an association of undertakings within the meaning of Article 81(1) of the Treaty. They remain decisions of an association also after the Initial Public Offering (IPO) of MasterCard Incorporated on 25 May 2006 and the related changes in the governance of the payment organisation in Europe with regard to the authority for setting the level of multilateral fallback interchange fees. The member banks of the MasterCard payment organisation agreed to the IPO and the ensuing changes in the organisation's governance in order to perpetuate the MIF as part of the business model in a form which they perceived to be less exposed to antitrust scrutiny. Even after the IPO of MasterCard Incorporated interchange fees in the MasterCard organisation are not "unilaterally imposed". MasterCard's member banks still share a common interest as regards the MIF because it yields guaranteed revenues for their issuing business. There is thus a continuing commonality of the banks' interests in a MIF after the IPO which is also reflected in the setting of interchange fee rates by MasterCard (...) [**]. In setting interchange fee rates the Global Board cannot ignore the commercial interests of the banks without whom the system would not function, because it yields guaranteed revenues for their issuing business.

(16) An open payment card scheme such as MasterCard's can operate without a MIF as is evidenced by the existence of comparable open payment card schemes without a MIF.

Article 81(3) of the Treaty

(17) The conditions set out in Article 81(3) EC for an exemption from the prohibition of Article 81(1) EC are not fulfilled.

(18) In relation to the first condition of Article 81(3) (contribution to technical or economic progress), MasterCard has failed to demonstrate a causal link between its MIF and objective efficiencies. MasterCard alleges that the central efficiency of its MIF is to help the scheme to maximise system output by balancing cardholder and merchant demands.

(19) The Commission does not dispute in general that payment systems are characterised by indirect network externalities and that in theory a revenue transfer between issuing and acquiring banks may help optimise the utility of the network to its users. However, whether a collectively fixed interchange fee should flow from acquirers to issuers or vice versa, and at which level it should be set cannot be determined in a general manner by economic theory alone, as theories always rely on assumptions that may not sufficiently reflect market reality. Rather, any claim that a MIF creates efficiencies within the first condition of Article 81(3) of the

Treaty must be founded on a detailed, robust and compelling analysis that relies in its assumptions and deductions on empirical data and facts. MasterCard in particular failed to provide empirical evidence for its central claim that the MIF maximises the scheme's "output" and for a causal link to other objective efficiencies claimed. It was therefore not established that the restrictive effects of the MIF in the acquiring markets are duly offset by objective efficiencies. Despite repeated requests by the Commission MasterCard failed to submit any empirical evidence on the positive effects of its MIF on system output and related efficiencies.

(20) The Commission does not share MasterCard's view that the competitive process and market forces automatically lead to a MIF that can safely be assumed to be efficiency enhancing. Neither the forces of inter-system competition nor acquiring banks or merchants exert sufficient constraints on the body in charge of setting the MIF in the MasterCard organisation.

(21) The specific framework underlying MasterCard's MIF is a model written by William Baxter in 1983. This model is, however, severely limited by the fact that it takes consumer and merchant demand as given in that neither strategically reacts to possible actions by the other. The Baxter model also relies on the unrealistic assumption that there is no variation in the benefits that merchants perceive from accepting cards, in other words it regards merchants as homogeneous. Baxter's result finally relies on the unrealistic assumption of a perfectly competitive banking industry.

(22) Moreover, the methodologies used by MasterCard for implementing this framework in practise are unconvincing as they do not sufficiently reflect the underlying theory. The methodologies suffer from considerable shortcomings as they establish an imbalance between card issuing and merchants acquiring solely on the basis of cost considerations while omitting to consider the banks' revenues, as well. Moreover, contrary to the merchant demand analysis, MasterCard does not even attempt to quantify the willingness to pay of cardholders and simply assumes the relative unwillingness of this customer group to pay for the convenience of using payment cards. There are also doubts as to the usefulness of MasterCard's proxy for quantifying the willingness to pay of merchants in the credit card segment.

(23) Under the second condition of Article 81(3) of the Treaty consumers (that is merchants and their subsequent purchasers) must get a fair share of the benefits which result from the efficiencies of a MIF. While merchants may benefit through enhanced network effects from the issuing side, this does not necessarily offset their losses which result from paying inflated merchant fees. The Commission has therefore reviewed MasterCard's methodology for setting an upper limit to its interchange fee rates. However, MasterCard's cost based benchmarks include cost items that are neither intrinsic in the payment functionality of a card nor related to services that clearly benefit the customers that bear the expenses of this MIF. Without further evidence, which MasterCard failed to submit, it cannot therefore safely be assumed that by maximising system output MasterCard is equally benefiting its member banks' customers. MasterCard failed to demonstrate that efficiencies outweigh restrictions to merchants (as well as subsequent purchasers).

(24) As to the third condition of Article 81(3) of the Treaty MasterCard has not proven to the requisite standard that its current MIF is indispensable to maximise system output.

(25) Due to unrealistic assumptions underlying the conceptual underpinnings of MasterCard's MIF, due to the lack of evidence for a causal link between this MIF and objective efficiencies claimed and due to the fact that MasterCard's methodologies do not sufficiently reflect the underlying framework and operate with inflated cost benchmarks, the Commission concludes that such MIF does not fulfil the first three conditions of Article 81(3) of the Treaty.

4. REMEDY

(26) As MasterCard's MIF restricts price competition between acquiring banks without fulfilling the first three conditions of Article 81(3) of the Treaty, the MasterCard payment organisation and the legal entities representing it are obliged to bring the infringement to an end within 6 months after notification of the Commission Decision by repealing the Intra-EEA fallback interchange fees, as well as the SEPA/Intra-Eurozone fallback interchange fees.

(27) The remedy does not apply to MasterCard's MIF for commercial cards, a segment that the Commission will further investigate.

5. FINES AND PERIODIC PENALTY PAYMENTS

(28) As MasterCard's MIF was notified to the Commission and given the specific circumstances of the present case, no fine is imposed.

(29) If MasterCard fails to comply with the remedy after the 6-month transition period lapses, the Commission imposes provisional periodic penalty payments of 3,5 % of MasterCard Incorporated's daily consolidated global turnover in the preceding business year according to Article 24(1)(a) of Regulation (EC) No 1/2003.

6. DECISION

(30) From 22 May 1992 until 19 December 2007 the MasterCard payment organisation and the legal entities representing it (MasterCard Incorporated, MasterCard International Incorporated and MasterCard Europe SPRL) have infringed Article 81 of the Treaty and, from 1 January 1994 until 19 December 2007, Article 53 of the EEA Agreement by in effect setting a minimum price merchants must pay to their acquiring bank for accepting payment cards in the European Economic Area, by means of the Intra-EEA fallback interchange fees for MasterCard branded consumer credit and charge cards and for MasterCard or Maestro branded debit cards.

(31) The MasterCard payment organisation and the legal entities representing it shall bring to an end the infringement

by formally repealing its intra-EEA and SEPA/intra-Eurozone fallback interchange fees within 6 months upon notification of the Decision. They shall moreover modify the association's network rules to reflect the Commission Decision. They shall repeal all decisions taken by MasterCard's European Board and/or by MasterCard's Global Board (...) [**] on Intra-EEA fallback interchange fees on SEPA fallback interchange fees and on Intra-Eurozone fallback interchange fees.

(32) The MasterCard payment organisation and the legal entities representing it shall refrain from repeating the infringement through any act or conduct having the same or equivalent object or effect. They shall in particular refrain from implementing the SEPA/the Intra-Eurozone fallback interchange fees.

(33) Within 6 months after notification of this Decision the legal entities representing the MasterCard payment organisation shall communicate all changes of the association's network rules and the repeal of decisions to all financial institutions holding a license for issuing and/or acquiring in the MasterCard payment organisation in the European Economic Area and to all clearing houses and settlement banks which clear and/or settle POS payment card transactions in the MasterCard payment organisation in the European Economic Area.

(34) If the legal entities representing the MasterCard payment organisation fail to comply with any of the orders set out in the Decision, the Decision imposes a daily penalty payment on the legal entities representing the MasterCard payment organisation of 3,5 % of MasterCard Incorporated's daily consolidated global turnover in the preceding business year according to Article 24(1)(a) of Regulation (EC) No 1/2003. This penalty will be calculated as from the first day after the infringed order takes effect.

[1] OJ L 1, 4.1.2003, p. 1.

[**] Business secret — information pertaining to MasterCard's interchange fee rules and procedure for determining the level of the interchange fee.

Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (4th Anti-Money Laundering = "4AML" Directive)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Flows of illicit money can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development. Money laundering, terrorism financing and organised crime remain significant problems which should be addressed at Union level. In addition to further developing the criminal law approach at Union level, targeted and proportionate prevention of the use of the financial system for the purposes of money laundering and terrorist financing is indispensable and can produce complementary results.

(2) The soundness, integrity and stability of credit institutions and financial institutions, and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates to disguise the origin

of criminal proceeds or to channel lawful or illicit money for terrorist purposes. In order to facilitate their criminal activities, money launderers and financiers of terrorism could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the Union's integrated financial area entails. Therefore, certain coordinating measures are necessary at Union level. At the same time, the objectives of protecting society from crime and protecting the stability and integrity of the Union's financial system should be balanced against the need to create a regulatory environment that allows companies to grow their businesses without incurring disproportionate compliance costs.

(3) This Directive is the fourth Directive to address the threat of money laundering. Council Directive 91/308/EEC (4) defined money laundering in terms of drugs offences and imposed obligations solely on the financial sector. Directive 2001/97/EC of the European Parliament and of the Council (5) extended the scope of Directive 91/308/EEC both in terms of the crimes covered and in terms of the range of professions and activities covered. In June 2003, the Financial Action Task Force (FATF) revised its Recommendations to cover terrorist financing, and provided more detailed requirements in relation to customer identification and verification, the situations where a higher risk of money laundering or terrorist financing may justify enhanced measures and also the situations where a reduced risk may justify less rigorous controls. Those changes were reflected in Directive 2005/60/EC of the European Parliament and of the Council (6) and in Commission Directive 2006/70/EC (7).

(4) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even at Union level, without taking into account international coordination and cooperation, would have very limited effect. The measures adopted by the Union in that field should therefore be compatible with, and at least as stringent as, other actions undertaken in international fora. Union action should continue to take particular account of the FATF Recommendations and instruments of other international bodies active in the fight against money laundering and terrorist financing. With a view to reinforcing the efficacy of the fight against money laundering and terrorist financing, the relevant Union legal acts should, where appropriate, be aligned with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by the FATF in February 2012 (the 'revised FATF Recommendations').

(5) Furthermore, the misuse of the financial system to channel illicit or even lawful money into terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. Accordingly, the preventive measures laid down in this Directive should address the manipulation of money derived from serious crime and the collection of money or property for terrorist purposes.

(6) The use of large cash payments is highly vulnerable to money laundering and terrorist financing. In order to increase vigilance and mitigate the risks posed by such cash payments, persons trading in goods should be covered by this Directive to the extent that they make or receive cash payments of EUR 10 000 or more. Member States should be able to adopt lower thresholds, additional general limitations to the use of cash and further stricter provisions.

(7) The use of electronic money products is increasingly considered to be a substitute for bank accounts, which, in addition to the measures laid down in Directive 2009/110/EC of the European Parliament and of the Council (8), justifies subjecting those products to anti-money laundering and countering the financing of terrorism (AML/CFT) obligations. However, in certain proven low-risk circumstances and under strict risk-mitigating conditions, Member States should be allowed to exempt electronic money products from certain customer due diligence measures, such as the identification and verification of the customer and of the beneficial owner, but not from the monitoring of transactions or of business

relationships. The risk-mitigating conditions should include a requirement that exempt electronic money products be used exclusively for purchasing goods or services, and that the amount stored electronically be low enough to preclude circumvention of the AML/CFT rules. Such an exemption should be without prejudice to the discretion given to Member States to allow obliged entities to apply simplified customer due diligence measures to other electronic money products posing lower risks, in accordance with Article 15.

[...]

(9) Legal professionals, as defined by the Member States, should be subject to this Directive when participating in financial or corporate transactions, including when providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing. There should, however, be exemptions from any obligation to report information obtained before, during or after judicial proceedings, or in the course of ascertaining the legal position of a client. Therefore, legal advice should remain subject to the obligation of professional secrecy, except where the legal professional is taking part in money laundering or terrorist financing, the legal advice is provided for the purposes of money laundering or terrorist financing, or the legal professional knows that the client is seeking legal advice for the purposes of money laundering or terrorist financing.

[...]

(12) There is a need to identify any natural person who exercises ownership or control over a legal entity. In order to ensure effective transparency, Member States should ensure that the widest possible range of legal entities incorporated or created by any other mechanism in their territory is covered. While finding a specified percentage shareholding or ownership interest does not automatically result in finding the beneficial owner, it should be one evidential factor among others to be taken into account. Member States should be able, however, to decide that a lower percentage may be an indication of ownership or control.

(13) Identification and verification of beneficial owners should, where relevant, extend to legal entities that own other legal entities, and obliged entities should look for the natural person(s) who ultimately exercises control through ownership or through other means of the legal entity that is the customer. Control through other means may, inter alia, include the criteria of control used for the purpose of preparing consolidated financial statements, such as through a shareholders' agreement, the exercise of dominant influence or the power to appoint senior management. There may be cases where no natural person is identifiable who ultimately owns or exerts control over a legal entity. In such exceptional cases, obliged entities, having exhausted all other means of identification, and provided there are no grounds for suspicion, may consider the senior managing official(s) to be the beneficial owner(s).

(14) The need for accurate and up-to-date information on the beneficial owner is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure. Member States should therefore ensure that entities incorporated within their territory in accordance with national law obtain and hold adequate, accurate and current information on their beneficial ownership, in addition to basic information such as the company name and address and proof of incorporation and legal ownership. With a view to enhancing transparency in order to combat the misuse of legal entities, Member States should ensure that beneficial ownership information is stored in a central register located outside the company, in full compliance with Union law. Member States can, for that purpose, use a central database which collects beneficial ownership information, or the business register, or another central register. Member States may decide that obliged entities are responsible for filling in the register. Member States should make sure that in all cases that information is made available to competent authorities

and FIUs and is provided to obliged entities when the latter take customer due diligence measures. Member States should also ensure that other persons who are able to demonstrate a legitimate interest with respect to money laundering, terrorist financing, and the associated predicate offences, such as corruption, tax crimes and fraud, are granted access to beneficial ownership information, in accordance with data protection rules. The persons who are able to demonstrate a legitimate interest should have access to information on the nature and extent of the beneficial interest held consisting of its approximate weight.

[...]

(16) Timely access to information on beneficial ownership should be ensured in ways which avoid any risk of tipping off the company concerned.

[...]

(18) This Directive should also apply to activities of obliged entities which are performed on the internet.

(19) New technologies provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering.

[...]

(21) The use of gambling sector services to launder the proceeds of criminal activity is of concern. In order to mitigate the risks relating to gambling services, this Directive should provide for an obligation for providers of gambling services posing higher risks to apply customer due diligence measures for single transactions amounting to EUR 2 000 or more. Member States should ensure that obliged entities apply the same threshold to the collection of winnings, wagering a stake, including by the purchase and exchange of gambling chips, or both. Providers of gambling services with physical premises, such as casinos and gaming houses, should ensure that customer due diligence, if it is taken at the point of entry to the premises, can be linked to the transactions conducted by the customer on those premises. However, in proven low-risk circumstances, Member States should be allowed to exempt certain gambling services from some or all of the requirements laid down in this Directive. The use of an exemption by a Member State should be considered only in strictly limited and justified circumstances, and where the risks of money laundering or terrorist financing are low. Such exemptions should be subject to a specific risk assessment which also considers the degree of vulnerability of the applicable transactions. They should be notified to the Commission. In the risk assessment, Member States should indicate how they have taken into account any relevant findings in the reports issued by the Commission in the framework of the supranational risk assessment.

[...]

(29) Member States should at least provide for enhanced customer due diligence measures to be applied by the obliged entities when dealing with natural persons or legal entities established in high-risk third countries identified by the Commission. Reliance on third parties established in such high-risk third countries should also be prohibited. Countries not included in the list should not be automatically considered to have effective AML/CFT systems and natural persons or legal entities established in such countries should be assessed on a risk-sensitive basis.

[...]

(34) Obtaining approval from senior management for establishing business relationships does not need to imply, in all cases, obtaining approval from the board of directors. It should be possible for such approval to be granted by someone with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and of sufficient seniority to take decisions affecting its risk exposure.

[...]

(36) In the case of agency or outsourcing relationships on a contractual basis between obliged entities and external persons not covered by this Directive, any AML/CFT obligations upon those agents or outsourcing service providers as part of the obliged entities could arise only from the contract between the parties and not from this Directive. Therefore the responsibility for complying with this Directive should remain primarily with the obliged entity.

(37) All Member States have, or should, set up operationally independent and autonomous FIUs to collect and analyse the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing. An operationally independent and autonomous FIU should mean that the FIU has the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and disseminate specific information. Suspicious transactions and other information relevant to money laundering, associated predicate offences and terrorist financing should be reported to the FIU, which should serve as a central national unit for receiving, analysing and disseminating to the competent authorities the results of its analyses. All suspicious transactions, including attempted transactions, should be reported, regardless of the amount of the transaction. Reported information could also include threshold-based information.

(38) By way of derogation from the general prohibition against carrying out suspicious transactions, obliged entities should be able to carry out suspicious transactions before informing the competent authorities where refraining from such carrying out is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. This, however, should be without prejudice to the international obligations accepted by the Member States to freeze without delay funds or other assets of terrorists, terrorist organisations or those who finance terrorism, in accordance with the relevant United Nations Security Council resolutions.

(39) For certain obliged entities, Member States should have the possibility to designate an appropriate self-regulatory body as the authority to be informed in the first instance instead of the FIU. In accordance with the case-law of the European Court of Human Rights, a system of first instance reporting to a self-regulatory body constitutes an important safeguard for upholding the protection of fundamental rights as concerns the reporting obligations applicable to lawyers. Member States should provide for the means and manner by which to achieve the protection of professional secrecy, confidentiality and privacy.

(40) Where a Member State decides to designate such a self-regulatory body, it may allow or require that body not to transmit to the FIU any information obtained from persons represented by that body where such information has been received from, or obtained on, one of their clients, in the course of ascertaining the legal position of their client, or in performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings.

(41) There have been a number of cases where employees who have reported their suspicions of money laundering have been subjected to threats or hostile action. Although this Directive cannot interfere with Member States' judicial procedures, it is crucial that this issue be addressed to ensure effectiveness of the AML/CFT system. Member States should be aware of this problem and should do whatever they can to protect individuals, including employees and representatives of the obliged entity, from such threats or hostile action, and to provide, in accordance with national law, appropriate protection to such persons, particularly with regard to their right to the protection of their personal data and their rights to effective judicial protection and representation.

[...]

(46) The rights of access to data by the data subject are applicable to the personal data processed for the purpose of this Directive. However, access by the data subject to any information related to a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Exceptions to and restrictions of that right in accordance with Article 13 of Directive 95/46/EC and, where relevant, Article 20 of Regulation (EC) No 45/2001, may therefore be justified. The data subject has the right to request that a supervisory authority referred to in Article 28 of Directive 95/46/EC or, where applicable, the European Data Protection Supervisor, check the lawfulness of the processing and has the right to seek a judicial remedy referred to in Article 22 of that Directive. The supervisory authority referred to in Article 28 of Directive 95/46/EC may also act on an ex-officio basis. Without prejudice to the restrictions to the right to access, the supervisory authority should be able to inform the data subject that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question.

[...]

(48) Money laundering and terrorist financing are international problems and the effort to combat them should be global. Where Union credit institutions and financial institutions have branches and subsidiaries located in third countries in which the requirements in that area are less strict than those of the Member State, they should, in order to avoid the application of very different standards within the institution or group of institutions, apply to those branches and subsidiaries Union standards or notify the competent authorities of the home Member State if the application of such standards is not possible.

[...]

(50) Where Member States require issuers of electronic money and payment service providers which are established in their territory in forms other than a branch and the head office of which is situated in another Member State, to appoint a central contact point in their territory, they should be able to require that such a central contact point, acting on behalf of the appointing institution, ensure the establishments' compliance with AML/CFT rules. They should also ensure that that requirement is proportionate and does not go beyond what is necessary to achieve the aim of compliance with AML/CFT rules, including by facilitating the respective supervision.

(51) Competent authorities should ensure that, with regard to currency exchange offices, cheque cashing offices, trust or company service providers or gambling service providers, the persons who effectively direct the business of such entities and the beneficial owners of such entities are fit and proper. The criteria for determining whether or not a person is fit and proper should, as a minimum, reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.

(52) Where an obliged entity operates establishments in another Member State, including through a network of agents, the competent authority of the home Member State should be responsible for supervising the obliged entity's application of group-wide AML/CFT policies and procedures. This could involve on-site visits in establishments based in another Member State. The competent authority of the home Member State should cooperate closely with the competent authority of the host Member State and should inform the latter of any issues that could affect their assessment of the establishment's compliance with the host AML/CFT rules.

[...]

(54) Taking into account the transnational nature of money laundering and terrorist financing, coordination and cooperation between FIUs are extremely important. In order to improve such coordination and cooperation, and, in particular, to ensure that suspicious transaction reports reach

the FIU of the Member State where the report would be of most use, detailed rules are laid down in this Directive.

(55) The EU Financial Intelligence Units' Platform (the 'EU FIUs Platform'), an informal group composed of representatives from FIUs and active since 2006, is used to facilitate cooperation among FIUs and exchange views on cooperation-related issues such as effective cooperation among FIUs and between FIUs and third-country financial intelligence units, joint analysis of cross-border cases and trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level.

(56) Improving the exchange of information between FIUs within the Union is particularly important in addressing the transnational character of money laundering and terrorist financing. The use of secure facilities for the exchange of information, in particular the decentralised computer network FIU.net (the 'FIU.net') or its successor and the techniques offered by FIU.net, should be encouraged by Member States. The initial exchange of information between FIUs relating to money laundering or terrorist financing for analytical purposes which is not further processed or disseminated should be permitted unless such exchange of information would be contrary to fundamental principles of national law. The exchange of information on cases identified by FIUs as possibly involving tax crimes should be without prejudice to the exchange of information in the field of taxation in accordance with Council Directive 2011/16/EU (15) or in accordance with international standards on the exchange of information and administrative cooperation in tax matters.

[...]

(64) Since the objective of this Directive, namely the protection of the financial system by means of prevention, detection and investigation of money laundering and terrorist financing, cannot be sufficiently achieved by the Member States, as individual measures adopted by Member States to protect their financial systems could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Union public policy, but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(65) This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular the right to respect for private and family life, the right to the protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

[...]

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

SECTION 1 Subject-matter, scope and definitions

Article 1

1. This Directive aims to prevent the use of the Union's financial system for the purposes of money laundering and terrorist financing.
2. Member States shall ensure that money laundering and terrorist financing are prohibited.
3. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:

- (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
 - (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
 - (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
 - (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).
4. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.
5. For the purposes of this Directive, 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA (20).
6. Knowledge, intent or purpose required as an element of the activities referred to in paragraphs 3 and 5 may be inferred from objective factual circumstances.

Article 2

1. This Directive shall apply to the following obliged entities:
- (1) credit institutions;
 - (2) financial institutions;
 - (3) the following natural or legal persons acting in the exercise of their professional activities:
 - (a) auditors, external accountants and tax advisors;
 - (b) notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:
 - (i) buying and selling of real property or business entities;
 - (ii) managing of client money, securities or other assets;
 - (iii) opening or management of bank, savings or securities accounts;
 - (iv) organisation of contributions necessary for the creation, operation or management of companies;
 - (v) creation, operation or management of trusts, companies, foundations, or similar structures;
 - (c) trust or company service providers not already covered under point (a) or (b);
 - (d) estate agents;
 - (e) other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
 - (f) providers of gambling services.
2. With the exception of casinos, and following an appropriate risk assessment, Member States may decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing this Directive on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services. Among the factors considered in their risk assessments, Member States shall assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used.

In their risk assessments, Member States shall indicate how they have taken into account any relevant findings in the reports issued by the Commission pursuant to Article 6. Any decision taken by a Member State pursuant to the first subparagraph shall be notified to the Commission, together with a justification based on the specific risk assessment. The Commission shall communicate that decision to the other Member States.

3. Member States may decide that persons that engage in a financial activity on an occasional or very limited basis where there is little risk of money laundering or terrorist financing do not fall within the scope of this Directive, provided that all of the following criteria are met:

- (a) the financial activity is limited in absolute terms;
- (b) the financial activity is limited on a transaction basis;
- (c) the financial activity is not the main activity of such persons;
- (d) the financial activity is ancillary and directly related to the main activity of such persons;
- (e) the main activity of such persons is not an activity referred to in points (a) to (d) or point (f) of paragraph 1(3);
- (f) the financial activity is provided only to the customers of the main activity of such persons and is not generally offered to the public.

The first subparagraph shall not apply to persons engaged in the activity of money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC of the European Parliament and of the Council (21).

4. For the purposes of point (a) of paragraph 3, Member States shall require that the total turnover of the financial activity does not exceed a threshold which must be sufficiently low. That threshold shall be established at national level, depending on the type of financial activity.

5. For the purposes of point (b) of paragraph 3, Member States shall apply a maximum threshold per customer and per single transaction, whether the transaction is carried out in a single operation or in several operations which appear to be linked. That maximum threshold shall be established at national level, depending on the type of financial activity. It shall be sufficiently low in order to ensure that the types of transactions in question are an impractical and inefficient method for money laundering or terrorist financing, and shall not exceed EUR 1 000.

6. For the purposes of point (c) of paragraph 3, Member States shall require that the turnover of the financial activity does not exceed 5 % of the total turnover of the natural or legal person concerned.

7. In assessing the risk of money laundering or terrorist financing for the purposes of this Article, Member States shall pay particular attention to any financial activity which is considered to be particularly likely, by its nature, to be used or abused for the purposes of money laundering or terrorist financing.

8. Decisions taken by Member States pursuant to paragraph 3 shall state the reasons on which they are based. Member States may decide to withdraw such decisions where circumstances change. They shall notify such decisions to the Commission. The Commission shall communicate such decisions to the other Member States.

9. Member States shall establish risk-based monitoring activities or take other adequate measures to ensure that the exemption granted by decisions pursuant to this Article is not abused.

Article 3

For the purposes of this Directive, the following definitions apply:

- (1) 'credit institution' means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council (22), including branches thereof, as defined in point (17) of Article 4(1) of that Regulation, located in the Union, whether its head office is situated within the Union or in a third country;
- (2) 'financial institution' means:

(a) an undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council (23), including the activities of currency exchange offices (bureaux de change);

(b) an insurance undertaking as defined in point (1) of Article 13 of Directive 2009/138/EC of the European Parliament and of the Council (24), insofar as it carries out life assurance activities covered by that Directive;

(c) an investment firm as defined in point (1) of Article 4(1) of Directive 2004/39/EC of the European Parliament and of the Council (25);

(d) a collective investment undertaking marketing its units or shares;

(e) an insurance intermediary as defined in point (5) of Article 2 of Directive 2002/92/EC of the European Parliament and of the Council (26) where it acts with respect to life insurance and other investment-related services, with the exception of a tied insurance intermediary as defined in point (7) of that Article;

(f) branches, when located in the Union, of financial institutions as referred to in points (a) to (e), whether their head office is situated in a Member State or in a third country;

(3) 'property' means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;

(4) 'criminal activity' means any kind of criminal involvement in the commission of the following serious crimes:

(a) acts set out in Articles 1 to 4 of Framework Decision 2002/475/JHA;

(b) any of the offences referred in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;

(c) the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA (27);

(d) fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1(1) and Article 2(1) of the Convention on the protection of the European Communities' financial interests (28);

(e) corruption;

(f) all offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the national law of the Member States, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards Member States that have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months;

(5) 'self-regulatory body' [...]

(6) 'beneficial owner' means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:

(a) in the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of

Member States to decide that a lower percentage may be an indication of ownership or control. Control through other means may be determined, *inter alia*, in accordance with the criteria in Article 22(1) to (5) of Directive 2013/34/EU of the European Parliament and of the Council (29);

(ii) if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s), the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point (i) and this point;

(b) in the case of trusts:

(i) the settlor;

(ii) the trustee(s);

(iii) the protector, if any;

(iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

(c) in the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point (b);

(7) 'trust or company service provider' means any person that, by way of its business, provides any of the following services to third parties:

(a) the formation of companies or other legal persons;

(b) acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;

(d) acting as, or arranging for another person to act as, a trustee of an express trust or a similar legal arrangement;

(e) acting as, or arranging for another person to act as, a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in accordance with Union law or subject to equivalent international standards;

(8) 'correspondent relationship' means:

(a) the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;

(b) the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers;

(9) 'politically exposed person' means a natural person who is or who has been entrusted with prominent public functions and includes the following:

(a) heads of State, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament or of similar legislative bodies;

(c) members of the governing bodies of political parties;

(d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, *chargés d'affaires* and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of State-owned enterprises;

(h) directors, deputy directors and members of the board or equivalent function of an international organisation.

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials;

(10) 'family members' includes the following:

(a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

(b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;

(c) the parents of a politically exposed person;

(11) 'persons known to be close associates' means:

(a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;

(b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

(12) 'senior management' means an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors;

(13) 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration;

(14) 'gambling services' [...]

(15) 'group' [...]

(16) 'electronic money' means electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC;

(17) 'shell bank' means a credit institution or financial institution, or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

Article 4

1. Member States shall, in accordance with the risk-based approach, ensure that the scope of this Directive is extended in whole or in part to professions and to categories of undertakings, other than the obliged entities referred to in Article 2(1), which engage in activities which are particularly likely to be used for the purposes of money laundering or terrorist financing.

2. Where a Member State extends the scope of this Directive to professions or to categories of undertaking other than those referred to in Article 2(1), it shall inform the Commission thereof.

Article 5

Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing, within the limits of Union law.

SECTION 2

Risk assessment

[...]

Article 8

1. Member States shall ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the nature and size of the obliged entities.

2. The risk assessments referred to in paragraph 1 shall be documented, kept up-to-date and made available to the relevant competent authorities and self-regulatory bodies concerned. Competent authorities may decide that individual documented risk assessments are not required where the specific risks inherent in the sector are clear and understood.

3. Member States shall ensure that obliged entities have in place policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity. Those policies, controls and procedures shall be proportionate to the nature and size of the obliged entities.

4. The policies, controls and procedures referred to in paragraph 3 shall include:

(a) the development of internal policies, controls and procedures, including model risk management practices, customer due diligence, reporting, record-keeping, internal control, compliance management including, where appropriate with regard to the size and nature of the business, the appointment of a compliance officer at management level, and employee screening;

(b) where appropriate with regard to the size and nature of the business, an independent audit function to test the internal policies, controls and procedures referred to in point (a).

5. Member States shall require obliged entities to obtain approval from their senior management for the policies, controls and procedures that they put in place and to monitor and enhance the measures taken, where appropriate.

[...]

CHAPTER II CUSTOMER DUE DILIGENCE

SECTION 1

General provisions

Article 10

1. Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts or anonymous passbooks. Member States shall, in any event, require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be subject to customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.

2. Member States shall take measures to prevent misuse of bearer shares and bearer share warrants.

Article 11

Member States shall ensure that obliged entities apply customer due diligence measures in the following circumstances:

(a) when establishing a business relationship;

(b) when carrying out an occasional transaction that:

(i) amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or

(ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council (30), exceeding EUR 1 000;

(c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(d) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

(f) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Article 12

1. By way of derogation from points (a), (b) and (c) of the first subparagraph of Article 13(1) and Article 14, and based on an appropriate risk assessment which demonstrates a low risk, a Member State may allow obliged entities not to apply certain customer due diligence measures with respect to electronic money, where all of the following risk-mitigating conditions are met:

- (a) the payment instrument is not reloadable, or has a maximum monthly payment transactions limit of EUR 250 which can be used only in that Member State;
- (b) the maximum amount stored electronically does not exceed EUR 250;
- (c) the payment instrument is used exclusively to purchase goods or services;
- (d) the payment instrument cannot be funded with anonymous electronic money;
- (e) the issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions.

For the purposes of point (b) of the first subparagraph, a Member State may increase the maximum amount to EUR 500 for payment instruments that can be used only in that Member State.

2. Member States shall ensure that the derogation provided for in paragraph 1 is not applicable in the case of redemption in cash or cash withdrawal of the monetary value of the electronic money where the amount redeemed exceeds EUR 100.

Article 13

1. Customer due diligence measures shall comprise:

- (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- (b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;
- (c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- (d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

When performing the measures referred to in points (a) and (b) of the first subparagraph, obliged entities shall also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

2. Member States shall ensure that obliged entities apply each of the customer due diligence requirements laid down in paragraph 1. However, obliged entities may determine the extent of such measures on a risk-sensitive basis.

3. Member States shall require that obliged entities take into account at least the variables set out in Annex I when assessing the risks of money laundering and terrorist financing.

4. Member States shall ensure that obliged entities are able to demonstrate to competent authorities or self-regulatory bodies that the measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified.

5. For life or other investment-related insurance business, Member States shall ensure that, in addition to the customer due diligence measures required for the customer and the beneficial owner, credit institutions and financial institutions conduct the following customer due diligence measures on the beneficiaries of life insurance and other investment-related insurance policies, as soon as the beneficiaries are identified or designated:

- (a) in the case of beneficiaries that are identified as specifically named persons or legal arrangements, taking the name of the person;
- (b) in the case of beneficiaries that are designated by characteristics or by class or by other means, obtaining sufficient information concerning those beneficiaries to satisfy the credit institutions or financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

With regard to points (a) and (b) of the first subparagraph, the verification of the identity of the beneficiaries shall take place at the time of the payout. In the case of assignment, in whole or in part, of the life or other investment-related insurance to a third party, credit institutions and financial institutions aware of the assignment shall identify the beneficial owner at the time of the assignment to the natural or legal person or legal arrangement receiving for its own benefit the value of the policy assigned.

6. In the case of beneficiaries of trusts or of similar legal arrangements that are designated by particular characteristics or class, an obliged entity shall obtain sufficient information concerning the beneficiary to satisfy the obliged entity that it will be able to establish the identity of the beneficiary at the time of the payout or at the time of the exercise by the beneficiary of its vested rights.

Article 14

1. Member States shall require that verification of the identity of the customer and the beneficial owner take place before the establishment of a business relationship or the carrying out of the transaction.

2. By way of derogation from paragraph 1, Member States may allow verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. In such situations, those procedures shall be completed as soon as practicable after initial contact.

3. By way of derogation from paragraph 1, Member States may allow the opening of an account with a credit institution or financial institution, including accounts that permit transactions in transferable securities, provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the customer due diligence requirements laid down in points (a) and (b) of the first subparagraph of Article 13(1) is obtained.

4. Member States shall require that, where an obliged entity is unable to comply with the customer due diligence requirements laid down in point (a), (b) or (c) of the first subparagraph of Article 13(1), it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, and shall terminate the business relationship and consider making a suspicious transaction report to the FIU in relation to the customer in accordance with Article 33.

Member States shall not apply the first subparagraph to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that those persons ascertain the legal position of their client, or perform the task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.

5. Member States shall require that obliged entities apply the customer due diligence measures not only to all new

customers but also at appropriate times to existing customers on a risk-sensitive basis, including at times when the relevant circumstances of a customer change.

SECTION 2

Simplified customer due diligence

Article 15

1. Where a Member State or an obliged entity identifies areas of lower risk, that Member State may allow obliged entities to apply simplified customer due diligence measures.

2. Before applying simplified customer due diligence measures, obliged entities shall ascertain that the business relationship or the transaction presents a lower degree of risk.

3. Member States shall ensure that obliged entities carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions.

Article 16

When assessing the risks of money laundering and terrorist financing relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, Member States and obliged entities shall take into account at least the factors of potentially lower risk situations set out in Annex II.

[...]

SECTION 3

Enhanced customer due diligence

Article 18

1. In the cases referred to in Articles 19 to 24, and when dealing with natural persons or legal entities established in the third countries identified by the Commission as high-risk third countries, as well as in other cases of higher risk that are identified by Member States or obliged entities, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.

Enhanced customer due diligence measures need not be invoked automatically with respect to branches or majority-owned subsidiaries of obliged entities established in the Union which are located in high-risk third countries, where those branches or majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 45. Member States shall ensure that those cases are handled by obliged entities by using a risk-based approach.

[...]

Article 19

With respect to cross-border correspondent relationships with a third-country respondent institution, Member States shall, in addition to the customer due diligence measures laid down in Article 13, require their credit institutions and financial institutions to:

(a) gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;

(b) assess the respondent institution's AML/CFT controls;

(c) obtain approval from senior management before establishing new correspondent relationships;

(d) document the respective responsibilities of each institution;

(e) with respect to payable-through accounts, be satisfied that the respondent institution has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent institution, and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

Article 20

With respect to transactions or business relationships with politically exposed persons, Member States shall, in addition to the customer due diligence measures laid down in Article 13, require obliged entities to:

(a) have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a politically exposed person;

(b) apply the following measures in cases of business relationships with politically exposed persons:

(i) obtain senior management approval for establishing or continuing business relationships with such persons;

(ii) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;

(iii) conduct enhanced, ongoing monitoring of those business relationships.

Article 21

Member States shall require obliged entities to take reasonable measures to determine whether the beneficiaries of a life or other investment-related insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. Those measures shall be taken no later than at the time of the payout or at the time of the assignment, in whole or in part, of the policy. Where there are higher risks identified, in addition to applying the customer due diligence measures laid down in Article 13, Member States shall require obliged entities to:

(a) inform senior management before payout of policy proceeds;

(b) conduct enhanced scrutiny of the entire business relationship with the policyholder.

[...]

Article 24

Member States shall prohibit credit institutions and financial institutions from entering into, or continuing, a correspondent relationship with a shell bank. They shall require that those institutions take appropriate measures to ensure that they do not engage in or continue correspondent relationships with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank.

SECTION 4

Performance by third parties

Article 25

Member States may permit obliged entities to rely on third parties to meet the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1). However, the ultimate responsibility for meeting those requirements shall remain with the obliged entity which relies on the third party.

Article 26

1. For the purposes of this Section, 'third parties' means obliged entities listed in Article 2, the member organisations or federations of those obliged entities, or other institutions or persons situated in a Member State or third country that:

(a) apply customer due diligence requirements and record-keeping requirements that are consistent with those laid down in this Directive; and

(b) have their compliance with the requirements of this Directive supervised in a manner consistent with Section 2 of Chapter VI.

2. Member States shall prohibit obliged entities from relying on third parties established in high-risk third countries. Member States may exempt branches and majority-owned subsidiaries of obliged entities established in the Union from that prohibition where those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 45.

Article 27

1. Member States shall ensure that obliged entities obtain from the third party relied upon the necessary information concerning the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1).

2. Member States shall ensure that obliged entities to which the customer is referred take adequate steps to ensure that the third party provides, immediately, upon request, relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner.

[...]

Article 29

This Section shall not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the obliged entity.

CHAPTER III

BENEFICIAL OWNERSHIP INFORMATION

Article 30

1. Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held.

Member States shall ensure that those entities are required to provide, in addition to information about their legal owner, information on the beneficial owner to obliged entities when the obliged entities are taking customer due diligence measures in accordance with Chapter II.

2. Member States shall require that the information referred to in paragraph 1 can be accessed in a timely manner by competent authorities and FIUs.

3. Member States shall ensure that the information referred to in paragraph 1 is held in a central register in each Member State, for example a commercial register, companies register as referred to in Article 3 of Directive 2009/101/EC of the European Parliament and of the Council (31), or a public register. Member States shall notify to the Commission the characteristics of those national mechanisms. The information on beneficial ownership contained in that database may be collected in accordance with national systems.

4. Member States shall require that the information held in the central register referred to in paragraph 3 is adequate, accurate and current.

5. Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:

- (a) competent authorities and FIUs, without any restriction;
- (b) obliged entities, within the framework of customer due diligence in accordance with Chapter II;
- (c) any person or organisation that can demonstrate a legitimate interest.

The persons or organisations referred to in point (c) shall access at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held.

For the purposes of this paragraph, access to the information on beneficial ownership shall be in accordance with data protection rules and may be subject to online registration and to the payment of a fee. The fees charged for obtaining the information shall not exceed the administrative costs thereof.

6. The central register referred to in paragraph 3 shall ensure timely and unrestricted access by competent authorities and FIUs, without alerting the entity concerned. It shall also allow timely access by obliged entities when taking customer due diligence measures.

7. Member States shall ensure that competent authorities and FIUs are able to provide the information referred to in

paragraphs 1 and 3 to the competent authorities and to the FIUs of other Member States in a timely manner.

8. Member States shall require that obliged entities do not rely exclusively on the central register referred to in paragraph 3 to fulfil their customer due diligence requirements in accordance with Chapter II. Those requirements shall be fulfilled by using a risk-based approach.

9. Member States may provide for an exemption to the access referred to in points (b) and (c) of paragraph 5 to all or part of the information on the beneficial ownership on a case-by-case basis in exceptional circumstances, where such access would expose the beneficial owner to the risk of fraud, kidnapping, blackmail, violence or intimidation, or where the beneficial owner is a minor or otherwise incapable. Exemptions granted pursuant to this paragraph shall not apply to the credit institutions and financial institutions, and to obliged entities referred to in point (3)(b) of Article 2(1) that are public officials.

10. By 26 June 2019, the Commission shall submit a report to the European Parliament and to the Council assessing the conditions and the technical specifications and procedures for ensuring the safe and efficient interconnection of the central registers referred to in paragraph 3 via the European central platform established by Article 4a(1) of Directive 2009/101/EC. Where appropriate, that report shall be accompanied by a legislative proposal.

Article 31

1. Member States shall require that trustees of any express trust governed under their law obtain and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust. That information shall include the identity of:

- (a) the settlor;
- (b) the trustee(s);
- (c) the protector (if any);
- (d) the beneficiaries or class of beneficiaries; and
- (e) any other natural person exercising effective control over the trust.

2. Member States shall ensure that trustees disclose their status and provide the information referred to in paragraph 1 to obliged entities in a timely manner where, as a trustee, the trustee forms a business relationship or carries out an occasional transaction above the thresholds set out in points (b), (c) and (d) of Article 11.

3. Member States shall require that the information referred to in paragraph 1 can be accessed in a timely manner by competent authorities and FIUs.

4. Member States shall require that the information referred to in paragraph 1 is held in a central register when the trust generates tax consequences. The central register shall ensure timely and unrestricted access by competent authorities and FIUs, without alerting the parties to the trust concerned. It may also allow timely access by obliged entities, within the framework of customer due diligence in accordance with Chapter II. Member States shall notify to the Commission the characteristics of those national mechanisms.

5. Member States shall require that the information held in the central register referred to in paragraph 4 is adequate, accurate and up-to-date.

6. Member States shall ensure that obliged entities do not rely exclusively on the central register referred to in paragraph 4 to fulfil their customer due diligence requirements as laid down in Chapter II. Those requirements shall be fulfilled by using a risk-based approach.

7. Member States shall ensure that competent authorities and FIUs are able to provide the information referred to in paragraphs 1 and 4 to the competent authorities and to the FIUs of other Member States in a timely manner.

8. Member States shall ensure that the measures provided for in this Article apply to other types of legal arrangements having a structure or functions similar to trusts.

9. By 26 June 2019, the Commission shall submit a report to the European Parliament and to the Council assessing the

conditions and the technical specifications and procedures for ensuring safe and efficient interconnection of the central registers. Where appropriate, that report shall be accompanied by a legislative proposal.

CHAPTER IV REPORTING OBLIGATIONS SECTION 1

General provisions

Article 32

1. Each Member State shall establish an FIU in order to prevent, detect and effectively combat money laundering and terrorist financing.

2. Member States shall notify the Commission in writing of the name and address of their respective FIUs.

3. Each FIU shall be operationally independent and autonomous, which means that the FIU shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information. The FIU as the central national unit shall be responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing. The FIU shall be responsible for disseminating the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing. It shall be able to obtain additional information from obliged entities.

Member States shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks.

4. Member States shall ensure that their FIUs have access, directly or indirectly, in a timely manner, to the financial, administrative and law enforcement information that they require to fulfil their tasks properly. FIUs shall be able to respond to requests for information by competent authorities in their respective Member States when such requests for information are motivated by concerns relating to money laundering, associated predicate offences or terrorist financing. The decision on conducting the analysis or dissemination of information shall remain with the FIU.

5. Where there are objective grounds for assuming that the provision of such information would have a negative impact on ongoing investigations or analyses, or, in exceptional circumstances, where disclosure of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested, the FIU shall be under no obligation to comply with the request for information.

6. Member States shall require competent authorities to provide feedback to the FIU about the use made of the information provided in accordance with this Article and about the outcome of the investigations or inspections performed on the basis of that information.

7. Member States shall ensure that the FIU is empowered to take urgent action, directly or indirectly, where there is a suspicion that a transaction is related to money laundering or terrorist financing, to suspend or withhold consent to a transaction that is proceeding, in order to analyse the transaction, confirm the suspicion and disseminate the results of the analysis to the competent authorities. The FIU shall be empowered to take such action, directly or indirectly, at the request of an FIU from another Member State for the periods and under the conditions specified in the national law of the FIU receiving the request.

8. The FIU's analysis function shall consist of the following:

(a) an operational analysis which focuses on individual cases and specific targets or on appropriate selected information, depending on the type and volume of the disclosures received and the expected use of the information after dissemination; and

(b) a strategic analysis addressing money laundering and terrorist financing trends and patterns.

Article 33

1. Member States shall require obliged entities, and, where applicable, their directors and employees, to cooperate fully by promptly:

(a) informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases; and

(b) providing the FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law.

All suspicious transactions, including attempted transactions, shall be reported.

2. The person appointed in accordance with point (a) of Article 8(4) shall transmit the information referred to in paragraph 1 of this Article to the FIU of the Member State in whose territory the obliged entity transmitting the information is established.

Article 34

1. By way of derogation from Article 33(1), Member States may, in the case of obliged entities referred to in point (3)(a), (b) and (d) of Article 2(1), designate an appropriate self-regulatory body of the profession concerned as the authority to receive the information referred to in Article 33(1).

Without prejudice to paragraph 2, the designated self-regulatory body shall, in cases referred to in the first subparagraph of this paragraph, forward the information to the FIU promptly and unfiltered.

2. Member States shall not apply the obligations laid down in Article 33(1) to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such exemption relates to information that they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of their client, or performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings.

Article 35

1. Member States shall require obliged entities to refrain from carrying out transactions which they know or suspect to be related to proceeds of criminal activity or to terrorist financing until they have completed the necessary action in accordance with point (a) of the first subparagraph of Article 33(1) and have complied with any further specific instructions from the FIU or the competent authorities in accordance with the law of the relevant Member State.

2. Where refraining from carrying out transactions referred to in paragraph 1 is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected operation, the obliged entities concerned shall inform the FIU immediately afterwards.

Article 36

1. Member States shall ensure that if, in the course of checks carried out on the obliged entities by the competent authorities referred to in Article 48, or in any other way, those authorities discover facts that could be related to money laundering or to terrorist financing, they shall promptly inform the FIU.

2. Member States shall ensure that supervisory bodies empowered by law or Regulation to oversee the stock, foreign exchange and financial derivatives markets inform the FIU if they discover facts that could be related to money laundering or terrorist financing.

Article 37

Disclosure of information in good faith by an obliged entity or by an employee or director of such an obliged entity in accordance with Articles 33 and 34 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether illegal activity actually occurred.

Article 38

Member States shall ensure that individuals, including employees and representatives of the obliged entity, who report suspicions of money laundering or terrorist financing internally or to the FIU, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

SECTION 2

Prohibition of disclosure

Article 39

1. Obligated entities and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information is being, will be or has been transmitted in accordance with Article 33 or 34 or that a money laundering or terrorist financing analysis is being, or may be, carried out.

2. The prohibition laid down in paragraph 1 shall not include disclosure to the competent authorities, including the self-regulatory bodies, or disclosure for law enforcement purposes.

3. The prohibition laid down in paragraph 1 shall not prevent disclosure between the credit institutions and financial institutions or between those institutions and their branches and majority-owned subsidiaries located in third countries, provided that those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures, including procedures for sharing information within the group, in accordance with Article 45, and that the group-wide policies and procedures comply with the requirements laid down in this Directive.

4. The prohibition laid down in paragraph 1 shall not prevent disclosure between the obliged entities as referred to in point (3)(a) and (b) of Article 2(1), or entities from third countries which impose requirements equivalent to those laid down in this Directive, who perform their professional activities, whether as employees or not, within the same legal person or a larger structure to which the person belongs and which shares common ownership, management or compliance control.

[...]

CHAPTER V

DATA PROTECTION, RECORD-RETENTION AND STATISTICAL DATA

Article 40

1. Member States shall require obliged entities to retain the following documents and information in accordance with national law for the purpose of preventing, detecting and investigating, by the FIU or by other competent authorities, possible money laundering or terrorist financing:

(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction;

(b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of five

years after the end of a business relationship with their customer or after the date of an occasional transaction.

Upon expiry of the retention periods referred to in the first subparagraph, Member States shall ensure that obliged entities delete personal data, unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention after they have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five additional years.

[...]

Article 41

1. The processing of personal data under this Directive is subject to Directive 95/46/EC, as transposed into national law. Personal data that is processed pursuant to this Directive by the Commission or by the ESAs is subject to Regulation (EC) No 45/2001.

2. Personal data shall be processed by obliged entities on the basis of this Directive only for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Directive for any other purposes, such as commercial purposes, shall be prohibited.

[...]

Article 42

Member States shall require that their obliged entities have systems in place that enable them to respond fully and speedily to enquiries from their FIU or from other authorities, in accordance with their national law, as to whether they are maintaining or have maintained, during a five-year period prior to that enquiry a business relationship with specified persons, and on the nature of that relationship, through secure channels and in a manner that ensures full confidentiality of the enquiries.

Article 43

The processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under Directive 95/46/EC.

[...]

CHAPTER VI

POLICIES, PROCEDURES AND SUPERVISION

SECTION 1

Internal procedures, training and feedback

Article 45

1. Member States shall require obliged entities that are part of a group to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes. Those policies and procedures shall be implemented effectively at the level of branches and majority-owned subsidiaries in Member States and third countries.

2. Member States shall require that obliged entities that operate establishments in another Member State ensure that those establishments respect the national provisions of that other Member State transposing this Directive.

3. Member States shall ensure that where obliged entities have branches or majority-owned subsidiaries located in third countries where the minimum AML/CFT requirements are less strict than those of the Member State, their branches and majority-owned subsidiaries located in the third country implement the requirements of the Member State, including data protection, to the extent that the third country's law so allows.

[...]

Article 46

1. Member States shall require that obliged entities take measures proportionate to their risks, nature and size so that their employees are aware of the provisions adopted pursuant to this Directive, including relevant data protection requirements.

Those measures shall include participation of their employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

Where a natural person falling within any of the categories listed in point (3) of Article 2(1) performs professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person.

2. Member States shall ensure that obliged entities have access to up-to-date information on the practices of money launderers and financiers of terrorism and on indications leading to the recognition of suspicious transactions.

3. Member States shall ensure that, where practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided to obliged entities.

4. Member States shall require that, where applicable, obliged entities identify the member of the management board who is responsible for the implementation of the laws, Regulations and administrative provisions necessary to comply with this Directive.

SECTION 2

Supervision

Article 47

1. Member States shall provide that currency exchange and cheque cashing offices and trust or company service providers be licensed or registered and providers of gambling services be regulated.

2. Member States shall require competent authorities to ensure that the persons who hold a management function in the entities referred to in paragraph 1, or are the beneficial owners of such entities, are fit and proper persons.

3. With respect to the obliged entities referred to in point (3)(a), (b) and (d) of Article 2(1), Member States shall ensure that competent authorities take the necessary measures to prevent criminals convicted in relevant areas or their associates from holding a management function in or being the beneficial owners of those obliged entities.

[...]

SECTION 3

Cooperation

Subsection I

National cooperation

Article 49

Member States shall ensure that policy makers, the FIUs, supervisors and other competent authorities involved in AML/CFT have effective mechanisms to enable them to cooperate and coordinate domestically concerning the development and implementation of policies and activities to combat money laundering and terrorist financing, including with a view to fulfilling their obligation under Article 7.

[...]

Subsection III

Cooperation between FIUs and with the Commission

Article 51

The Commission may lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Union. It may regularly convene meetings of the EU FIUs' Platform composed of representatives from Member States' FIUs, in order to facilitate cooperation among FIUs, exchange views and

provide advice on implementation issues relevant for FIUs and reporting entities as well as on cooperation-related issues such as effective FIU cooperation, the identification of suspicious transactions with a cross-border dimension, the standardisation of reporting formats through the FIU.net or its successor, the joint analysis of cross-border cases, and the identification of trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level.

[...]

Article 53

1. Member States shall ensure that FIUs exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing and the natural or legal person involved, even if the type of predicate offences that may be involved is not identified at the time of the exchange.

A request shall contain the relevant facts, background information, reasons for the request and how the information sought will be used. Different exchange mechanisms may apply if so agreed between the FIUs, in particular as regards exchanges through the FIU.net or its successor.

When an FIU receives a report pursuant to point (a) of the first subparagraph of Article 33(1) which concerns another Member State, it shall promptly forward it to the FIU of that Member State.

2. Member States shall ensure that the FIU to whom the request is made is required to use the whole range of its available powers which it would normally use domestically for receiving and analysing information when it replies to a request for information referred to in paragraph 1 from another FIU. The FIU to whom the request is made shall respond in a timely manner.

When an FIU seeks to obtain additional information from an obliged entity established in another Member State which operates on its territory, the request shall be addressed to the FIU of the Member State in whose territory the obliged entity is established. That FIU shall transfer requests and answers promptly.

3. An FIU may refuse to exchange information only in exceptional circumstances where the exchange could be contrary to fundamental principles of its national law. Those exceptions shall be specified in a way which prevents misuse of, and undue limitations on, the free exchange of information for analytical purposes.

[...]

Article 55

1. Member States shall ensure that the information exchanged pursuant to Articles 52 and 53 is used only for the purpose for which it was sought or provided and that any dissemination of that information by the receiving FIU to any other authority, agency or department, or any use of this information for purposes beyond those originally approved, is made subject to the prior consent by the FIU providing the information.

2. Member States shall ensure that the requested FIU's prior consent to disseminate the information to competent authorities is granted promptly and to the largest extent possible. The requested FIU shall not refuse its consent to such dissemination unless this would fall beyond the scope of application of its AML/CFT provisions, could lead to impairment of a criminal investigation, would be clearly disproportionate to the legitimate interests of a natural or legal person or the Member State of the requested FIU, or would otherwise not be in accordance with fundamental principles of national law of that Member State. Any such refusal to grant consent shall be appropriately explained.

Article 56

1. Member States shall require their FIUs to use protected channels of communication between themselves and encourage the use of the FIU.net or its successor.
2. Member States shall ensure that, in order to fulfil their tasks as laid down in this Directive, their FIUs cooperate in the application of state-of-the-art technologies in accordance with their national law. Those technologies shall allow FIUs to match their data with that of other FIUs in an anonymous way by ensuring full protection of personal data with the aim of detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds.

Article 57

Differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information or provide assistance to another FIU, to the greatest extent possible under their national law.

SECTION 4

Sanctions

Article 58

1. Member States shall ensure that obliged entities can be held liable for breaches of national provisions transposing this Directive in accordance with this Article and Articles 59 to 61. Any resulting sanction or measure shall be effective, proportionate and dissuasive.

2. Without prejudice to the right of Member States to provide for and impose criminal sanctions, Member States shall lay down rules on administrative sanctions and measures and ensure that their competent authorities may impose such sanctions and measures with respect to breaches of the national provisions transposing this Directive, and shall ensure that they are applied.

Member States may decide not to lay down rules for administrative sanctions or measures for breaches which are subject to criminal sanctions in their national law. In that case, Member States shall communicate to the Commission the relevant criminal law provisions.

3. Member States shall ensure that where obligations apply to legal persons in the event of a breach of national provisions transposing this Directive, sanctions and measures can be applied to the members of the management body and to other natural persons who under national law are responsible for the breach.

4. Member States shall ensure that the competent authorities have all the supervisory and investigatory powers that are necessary for the exercise of their functions.

5. Competent authorities shall exercise their powers to impose administrative sanctions and measures in accordance with this Directive, and with national law, in any of the following ways:

- (a) directly;
- (b) in collaboration with other authorities;
- (c) under their responsibility by delegation to such other authorities;
- (d) by application to the competent judicial authorities.

In the exercise of their powers to impose administrative sanctions and measures, competent authorities shall cooperate closely in order to ensure that those administrative sanctions or measures produce the desired results and coordinate their action when dealing with cross-border cases.
[...]

Article 61

1. Member States shall ensure that competent authorities establish effective and reliable mechanisms to encourage the reporting to competent authorities of potential or actual breaches of the national provisions transposing this Directive.

2. The mechanisms referred to in paragraph 1 shall include at least:

- (a) specific procedures for the receipt of reports on breaches and their follow-up;

(b) appropriate protection for employees or persons in a comparable position, of obliged entities who report breaches committed within the obliged entity;

(c) appropriate protection for the accused person;

(d) protection of personal data concerning both the person who reports the breaches and the natural person who is allegedly responsible for a breach, in compliance with the principles laid down in Directive 95/46/EC;

(e) clear rules that ensure that confidentiality is guaranteed in all cases in relation to the person who reports the breaches committed within the obliged entity, unless disclosure is required by national law in the context of further investigations or subsequent judicial proceedings.

3. Member States shall require obliged entities to have in place appropriate procedures for their employees, or persons in a comparable position, to report breaches internally through a specific, independent and anonymous channel, proportionate to the nature and size of the obliged entity concerned.
[...]

CHAPTER VII

FINAL PROVISIONS

[...]

Article 66

Directives 2005/60/EC and 2006/70/EC are repealed with effect from 26 June 2017.

References to the repealed Directives shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex IV.

Article 67

1. Member States shall bring into force the laws, Regulations and administrative provisions necessary to comply with this Directive by 26 June 2017. They shall immediately communicate the text of those measures to the Commission.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.
[...]

Article 68

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 69

This Directive is addressed to the Member States.

Done at Strasbourg, 20 May 2015.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

Z. KALNIŅA-LUKAŠEVICA

[...]

ANNEX I

The following is a non-exhaustive list of risk variables that obliged entities shall consider when determining to what extent to apply customer due diligence measures in accordance with Article 13(3):

- (i) the purpose of an account or relationship;
- (ii) the level of assets to be deposited by a customer or the size of transactions undertaken;
- (iii) the regularity or duration of the business relationship.

ANNEX II

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in Article 16:

- (1) Customer risk factors:
- (a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
 - (b) public administrations or enterprises;
 - (c) customers that are resident in geographical areas of lower risk as set out in point (3);
- (2) Product, service, transaction or delivery channel risk factors:
- (a) life insurance policies for which the premium is low;
 - (b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
 - (c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
 - (d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
 - (e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money);
- (3) Geographical risk factors:
- (a) Member States;
 - (b) third countries having effective AML/CFT systems;
 - (c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
 - (d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3):

- (1) Customer risk factors:
- (a) the business relationship is conducted in unusual circumstances;
 - (b) customers that are resident in geographical areas of higher risk as set out in point (3);
 - (c) legal persons or arrangements that are personal asset-holding vehicles;
 - (d) companies that have nominee shareholders or shares in bearer form;
 - (e) businesses that are cash-intensive;
 - (f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
- (2) Product, service, transaction or delivery channel risk factors:
- (a) private banking;
 - (b) products or transactions that might favour anonymity;
 - (c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
 - (d) payment received from unknown or unassociated third parties;
 - (e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;
- (3) Geographical risk factors:
- (a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
 - (b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
 - (c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
 - (d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

ANNEX IV Correlation table

[...]

Relevant Case-Law on Anti-Money Laundering

Joined cases C-478/11 P to C-482/11 P – Laurent Gbagbo (C-478/11 P), Katinan Justin Koné (C-479/11 P), Akissi Danièle Boni-Claverie (C-480/11 P), Alcide Djédjé (C-481/11 P) and Affi Pascal N'Guessan (C-482/11 P) v Council of the European Union

JUDGMENT OF THE COURT (Grand Chamber)
23 April 2013 (*)

In Joined Cases C-478/11 P to C-482/11 P,
Five APPEALS under Article 56 of the Statute of the Court of Justice of the European Union, brought on 21 September 2011,

Laurent Gbagbo (C-478/11 P),
Katinan Justin Koné (C-479/11 P),
Akissi Danièle Boni-Claverie (C-480/11 P),
Alcide Djédjé (C-481/11 P),
Affi Pascal N'Guessan (C-482/11 P),
represented by L. Bourthoumieux, lawyer,
appellants,

the other party to the proceedings being:

Council of the European Union, represented by B. Driessen and M.-M. Joséphidès, acting as Agents,
defendant at first instance,

1 By their appeals, Mr Gbagbo, Mr Koné, Ms Boni-Claverie, Mr Djédjé and Mr N'Guessan request that the Court set aside the orders of the General Court of the European Union of 13 July 2011 in, respectively, Case T-348/11 Gbagbo v Council, Case T-349/11 Koné v Council, Case T-350/11 Boni-Claverie v Council, Case T-351/11 Djédjé v Council and Case T-352/11 N'Guessan v Council ('the orders under appeal'), whereby the General Court dismissed as being manifestly inadmissible their actions for the annulment of, first, Council Decisions 2011/17/CFSP of 11 January 2011 (OJ 2011 L 11, p. 31), 2011/18/CFSP of 14 January 2011 (OJ 2011 L 11, p. 36) and 2011/221/CFSP of 6 April 2011 (OJ 2011 L 93, p. 20), amending Council Decision 2010/656/CFSP renewing the restrictive measures against Côte d'Ivoire, and, secondly, Council Regulations (EU) No 25/2011 of 14 January 2011 (OJ 2011 L 11, p. 1) and (EU) No 330/2011 of 6 April 2011 (OJ 2011 L 93, p. 10), amending Council Regulation (EC) No 560/2005 imposing certain specific restrictive measures

directed against certain persons and entities in view of the situation in Côte d'Ivoire ('the contested measures'), in so far as those measures concern them.

Legal context and background to the dispute

2 On 15 November 2004 the United Nations Security Council adopted Resolution 1572 (2004) in which it declared, *inter alia*, that the situation in Côte d'Ivoire continued to pose a threat to international peace and security in the region and decided to impose certain restrictive measures against that country.

3 Paragraph 14 of Resolution 1572 (2004) established a committee ('the Sanctions Committee') whose tasks included the designation of persons and entities to be subject to the restrictive measures in respect of travel and freezing of funds, financial assets and economic resources imposed by paragraphs 9 and 11 of that resolution and the regular updating of the list of persons and entities.

4 On 13 December 2004 the Council of the European Union, considering that action by the European Community was necessary in order to implement Resolution 1572 (2004), adopted Common Position 2004/852/CFSP concerning restrictive measures against Côte d'Ivoire (OJ 2004 L 368, p. 50).

5 On 12 April 2005, since it took the view that a Regulation was necessary in order to implement, at Community level, the measures described in Common Position 2004/852, the Council adopted Council Regulation (EC) No 560/2005 of 12 April 2005 imposing certain specific restrictive measures directed against certain persons and entities in view of the situation in Côte d'Ivoire (OJ 2005 L 95, p. 1).

6 Common Position 2004/852 was extended and amended on several occasions, before being repealed and replaced by Council Decision 2010/656/CFSP of 29 October 2010 renewing the restrictive measures against Côte d'Ivoire (OJ 2010 L 285, p. 28).

7 An election for the office of President of the Republic of Côte d'Ivoire was held on 31 October and 28 November 2010.

8 On 3 December 2010 the Special Representative of the United Nations Secretary General for Côte d'Ivoire certified the final result of the second round of the presidential election, as declared by the president of the independent electoral commission on 2 December 2010, confirming the victory of Mr Alassane Ouattara in the Presidential election.

9 On 13 December 2010 the Council emphasised the importance of the Presidential election held on 31 October and 28 November 2010 for the return of peace and stability in Côte d'Ivoire and declared it to be imperative that the sovereign wish expressed by the Ivorian people should be respected. The Council also noted the conclusions of the Special Representative of the United Nations Secretary General for Côte d'Ivoire as part of his task of certification and congratulated Mr Ouattara on his election as President of the Republic of Côte d'Ivoire.

10 On 17 December 2010 the European Council called on all Ivorian leaders, both civilian and military, who had not yet done so, to place themselves under the authority of the democratically elected President, Mr Ouattara. The European Council confirmed the determination of the European Union to take targeted measures against those who might continue to obstruct respect of the sovereign wish expressed by the Ivorian people.

11 In order to impose restrictive measures, in respect of travel, against certain persons who, though not designated by the United Nations Security Council or the Sanctions Committee, are obstructing the processes of peace and national reconciliation in Côte d'Ivoire, in particular those who are jeopardising the proper outcome of the electoral process, the Council adopted Council Decision 2010/801/CFSP of 22 December 2010 amending Council Decision 2010/656 (OJ 2010 L 341, p. 45). Those persons are listed in Annex II to Decision 2010/656, as amended by Decision 2010/801.

12 Article 4(1) of Decision 2010/656, as amended by Decision 2010/801, reads as follows:

'Member States shall take the necessary measures to prevent the entry into, or transit through, their territories of:

(a) the persons referred to in Annex I and designated by the Sanctions Committee ...;

(b) the persons referred to in Annex II who are not included in the list in Annex I and who are obstructing the process of peace and national reconciliation, and in particular who are jeopardising the proper outcome of the electoral process.'

13 The names of Mr Gbagbo and Mr N'Guessan were, by means of Decision 2010/801, included in the list in Annex II to Decision 2010/656, as amended by Decision 2010/81.

14 On 11 January 2011 the Council adopted Decision 2011/17 in order to enter, in view of the gravity of the situation in Côte d'Ivoire, the names of additional persons in the list in Annex II to Decision 2010/656, as amended by Decision 2010/801.

15 Accordingly, the names of Mr Koné and Ms Boni-Claverie were, by means of Decision 2011/17, included in the list in Annex II to Decision 2010/656, as amended by Decision 2010/801.

16 On 14 January 2011 the Council adopted Decision 2011/18 in order to impose additional restrictive measures, in particular the freezing of funds.

17 Under Article 5(1) and (2) of Decision 2010/656 as amended by Decision 2011/18:

'1. All funds and economic resources owned or controlled directly or indirectly by:

(a) the persons referred to in Annex I designated by the Sanctions Committee ..., or held by entities owned or controlled directly or indirectly by them or by any persons acting on their behalf or at their direction, as designated by the Sanctions Committee,

(b) the persons or entities referred to in Annex II who are not included in the list in Annex I and who are obstructing the process of peace and national reconciliation, and in particular who are jeopardising the proper outcome of the electoral process, or held by entities owned or controlled directly or indirectly by them or by any persons acting on their behalf or at their direction,

2. No funds, financial assets or economic resources shall be made available, directly or indirectly, to or for the benefit of persons or entities referred to in paragraph 1.'

18 In order to ensure consistency with the process for amending and reviewing Annexes I and II to Decision 2010/656, as amended by Decision 2011/18, the Council adopted, on 14 January 2011, Regulation No 25/2011.

19 Article 2 of Regulation No 560/2005, as amended by Regulation No 25/2011, states:

'1. All funds and economic resources belonging to, owned, held or controlled by the natural or legal persons, entities and bodies listed in Annex I or in Annex IA shall be frozen.

2. No funds or economic resources shall be made available, directly or indirectly, to or for the benefit of the natural or legal persons, entities or bodies listed in Annex I or in Annex IA.

3. The participation, knowing and intentional, in activities the object or effect of which is, directly or indirectly, to circumvent the measures referred to in paragraphs 1 and 2 shall be prohibited.

4. Annex I shall consist of the natural or legal persons, entities and bodies referred to in Article 5(1)(a) of [Decision 2010/656] as amended.

5. Annex IA shall consist of the natural or legal persons, entities and bodies referred to in Article 5(1)(b) of [Decision 2010/656] as amended.'

20 By means of Decision 2011/18 and Regulation No 25/2011 the Council maintained the names of Mr Gbagbo, Mr Koné, Mr N'Guessan and Ms Boni-Claverie in the list in Annex II to Decision 2010/656, as amended by Decision 2011/17, and also entered their names in the list in Annex IA to Regulation No 560/2005, as amended by Regulation No 25/2011.

21 On 30 March 2011 the United Nations Security Council adopted Resolution 1975 (2011), Annex I to which lists a number of persons who had obstructed peace and

reconciliation in Côte d'Ivoire, had obstructed the work of the United Nations Operation in Côte d'Ivoire (UNOCI) and other international actors in Côte d'Ivoire and had committed serious violations of human rights and international humanitarian law. Mr Gbagbo, Mr Djédjé and Mr N'Guessan are named in Annex I.

22 On 6 April 2011 the Council adopted Decision 2011/221 and Regulation No 330/2011 whereby it, inter alia, imposed additional restrictive measures and amended the lists of persons and entities in Annexes I and II to Decision 2010/656, as amended by Decision 2011/18, and in Annexes I and IA to Regulation No 560/2005, as amended by Regulation No 25/2011.

23 Decision 2011/221 in particular removed the names of Mr Gbagbo and Mr N'Guessan from the list in Annex II to Decision 2010/656, as amended by Decision 2011/18, and added their names to the list in Annex I to Decision 2010/656, as amended.

24 Further, Decision 2011/221 added the name of Mr Djédjé to the list in Annex I to Decision 2010/656, as amended by Decision 2011/18.

25 Regulation No 330/2011, for its part, removed the names of Mr Gbagbo and Mr N'Guessan from the list in Annex IA to Regulation No 560/2005, as amended by Regulation No 25/2011, and added their names to the list in Annex I to Regulation No 560/2005, as amended.

26 Regulation No 330/2011 also added the name of Mr Djédjé to the list in Annex I to Regulation No 560/2005, as amended by Regulation No 25/2011.

27 Article 7 of Decision 2010/656, as amended by Decision 2010/801, provides:

'1 Where the Security Council or the Sanctions Committee designates a person or entity, the Council shall include such person or entity in the list in Annex I.

2. Where the Council decides to apply to a person or entity the measures referred to in Article 4(1)(b), it shall amend Annex II accordingly.

3. The Council shall communicate its Decision, including the grounds for listing, to the person or entity concerned, either directly, if the address is known, or through the publication of a notice, providing such person or entity with an opportunity to present observations.

4. Where observations are submitted, or where substantial new evidence is presented, the Council shall review its Decision and inform the person or entity accordingly.'

28 Article 11a(3) of Regulation No 560/2005, as amended by Regulation No 25/2011, provides:

'The Council shall communicate its decision, including the grounds for listing, to the natural or legal person, entity or body referred to in paragraphs 1 and 2, either directly, if the address is known, or through the publication of a notice, providing such natural or legal person, entity or body with an opportunity to present observations.'

29 The Council published in the Official Journal of the European Union of 18 January 2011 and 7 April 2011 notices for the attention of the persons to whom the restrictive measures laid down in the contested measures applied (OJ 2011 C 14, p. 8, and OJ 2011 C 108, pp. 2 and 4). In those notices the Council intimates the existence of those restrictive measures, refers to the relevant texts in relation to the reasons for each listing and draws attention to the possibility of making an application to the competent authorities of the relevant Member State in order to obtain authorisation to use frozen funds for basic needs or to make specific payments. The Council further adds that the persons and entities concerned may submit to it a request for reconsideration. Finally the Council gives notice of the possibility of challenging its decision before the General Court, in accordance with the conditions laid down in the second paragraph of Article 275 TFEU and the fourth and sixth paragraphs of Article 263 TFEU.

The procedure before the General Court and the orders under appeal

30 By applications lodged at the Registry of the General Court on 7 July 2011, the appellants sought the annulment of the contested measures in so far as those measures concerned them. In support of their action, they relied on, first, an infringement of the rights of the defence and of the right to an effective remedy and, secondly, an infringement of their rights of property and free movement.

31 The appellants further claimed that their actions should be declared to be admissible by the General Court, since the time-limit of two months laid down in Article 263 TFEU for the bringing of an action could not apply to them given the failure to notify them of the contested measures.

32 By the orders under appeal, the General Court dismissed the actions as being manifestly inadmissible.

33 The General Court first recalled the settled case-law that the time-limit for bringing an action laid down in the sixth paragraph of Article 263 TFEU is a matter of public policy, since it was laid down with a view to ensuring clarity and legal certainty and avoiding discrimination or arbitrary treatment in the administration of justice, and that the courts of the European Union must ascertain of their own motion whether that time-limit has been observed.

34 The General Court then found that the contested measures had been published in the Official Journal of the European Union:

– on 15 January 2011, as regards Decisions 2011/17 and 2011/18, and Regulation No 25/2011, and

– on 7 April 2011, as regards Decision 2011/221 and Regulation No 330/2011.

35 Consequently, the time-limit of two months for bringing proceedings started to run, in accordance with Article 102(1) of the Rules of Procedure of the General Court, fourteen days after those dates of publication and expired, pursuant to Article 102(2) of those Rules:

– at midnight on 8 April 2011, as regards Decisions 2011/17 and 2011/18 and Regulation No 25/2011, and

– at midnight on 1 July 2011, as regards Decision 2011/221 and Regulation No 330/2011.

36 Given that the applications had been lodged at the Registry of the General Court on 7 July 2011, the General Court concluded that the actions had been brought out of time.

37 The General Court rejected the appellants' arguments that the time-limit of two months for bringing proceedings could apply to them on the grounds that the contested measures had not been notified to them. On that subject the General Court stated the following:

'Given the fact that time-limits for bringing proceedings are intended to ensure legal certainty by preventing European Union measures which produce legal effects from being called into question indefinitely, the date of publication, if there is one, is the decisive criterion for determining the starting point of the period prescribed for initiating proceedings (orders of 25 November 2008 in C-500/07 TEA v Commission, ..., paragraph 23, and in C-501/07 P S.A.B.A.R. v Commission, ..., paragraph 22; order of 9 July 2009 in C-498/08 P Fornaci Laterizi Danesi v Commission, ..., paragraph 22; judgment of 11 November 2010 in C-36/09 P Transportes Evaristo Molina v Commission, ..., paragraph 37). An applicant cannot plead that he became aware of the contested measure after the date of its publication in order to defer that starting point (orders in TEA v Commission, paragraph 23; S.A.B.A.R. v Commission, paragraph 22, and Fornaci Laterizi Danesi v Commission, paragraph 22). It follows that, since the [contested] measures were published, the time-limit for bringing proceedings must be calculated from the date of their publication (see, as regards the calculation of the time-limit for bringing an action against a decision imposing restrictive measures from the publication of that decision, the order of 18 November 2005 in Case T-299/04 Selmani v Council and Commission, ..., paragraph 61), even if the measures have not been notified [to the appellants]. In that regard, it must also be observed that the Council published ... notices for the attention of persons to whom the restrictive measures provided for in [the contested measures] apply, in which notices the Council, in particular,

drew the attention of the persons concerned to the possibility of challenging its decision before the General Court, in accordance with the conditions laid down in the second paragraph of Article 275 TFEU and the fourth and sixth paragraphs of Article 263 TFEU.'

38 Lastly, the General Court observed that the appellants had not established or even argued the existence of unforeseeable circumstances or of force majeure which would allow the Court to waive the time-limit in question on the basis of the second paragraph of Article 45 of the Statute of the Court of Justice of the European Union.

Forms of order of the parties and procedure before the Court
39 The appellants claim that the Court should:

- set aside the orders under appeal and declare their actions at first instance to be admissible;
- refer the cases back the General Court for it to give a ruling on the substance, and
- order the Council to pay the costs.

40 The Council contends that the Court should:

- dismiss the appeals, and
- order the appellants to pay the costs.

41 By order of the President of the Court of 14 December 2011, Cases C-478/11 P to C-482/11 P were joined for the purposes of the written and oral procedure and the judgment.

42 By letter dated 11 May 2012, sent by fax and registered mail, the Registrar of the Court informed the parties that a hearing would be held on 26 June 2012 and asked them to reply in writing no later than by 15 June 2012 to the questions of the Court annexed to the notification of the hearing.

43 The Council's reply to the question put to it was received at the Registry of the Court on 14 June 2012. However, the time-limit of 15 June 2012 passed without any reply being received by the Court from the appellants to the question put to them or any reply as regards whether they would attend the hearing.

44 A final time-limit was set for the appellants to indicate whether they would attend the hearing. That time-limit of 21 June 2012 having passed without reply from them, the hearing was cancelled.

The appeals

45 In support of their appeals, the appellants rely on two grounds. By the first ground of appeal, they claim that the General Court erred in law by not accepting the existence of force majeure. By the second ground of appeal, the appellants claim that the General Court was wrong to hold that the time-limit for bringing proceedings and the principle of legal certainty underlying that time-limit barred their action where the distinguishing features of this case were, first, that there was no notification of the contested measures and, secondly, the inapplicability of the extension of the time-limit on account of distance as set out in the Rules of Procedure of the General Court.

46 The second ground of appeal should be examined first.

The second ground of appeal

Arguments of the parties

47 The appellants claim, first, that the General Court disregarded the principle of effective judicial protection and thus erred in law by holding that, since the contested measures had been published, the time-limit for bringing proceedings should be calculated from the date of their publication. According to the appellants, the General Court ought to have taken account of the fact that the contested measures had not, contrary to the provisions of, in particular, Article 7(3) of Decision 2010/656, as amended by Decision 2010/801, been notified, as there had been no individual communication to put the persons affected by the measures in a position to take cognisance of them.

48 The appellants consider, secondly, that the General Court should not have applied the provisions of Article 102(2) of its Rules of Procedure on the extension of the time-limit on account of distance to the appellants, residing in a State in

Africa, particularly when that State was in a situation of armed conflict.

49 The Council contends that the procedural context of the present cases is not the same as that examined by the Court in its judgment of 16 November 2011 in *C-548/09 P Bank Melli Iran v Council* [2011] ECR I-11381. In that judgment, the Court based the obligation to communicate individually the reasons for the adoption of restrictive measures on Article 15(3) of Council Regulation (EC) No 423/2007 of 19 April 2007 concerning restrictive measures against Iran (OJ 2007 L 103, p. 1). Unlike Regulation No 423/2007, Article 7(3) of Decision 2010/656, as amended by Decision 2010/801, provides for the possibility of communication through the publication of a notice in cases where the address of the person concerned is not known to the Council.

50 In this case, the Council contends that it communicated the contested measures to the appellants by means of a published notice, in accordance with Article 7(3) of Decision 2010/656, as amended by Decision 2010/801. The Council argues that it could not have communicated the measures otherwise, since the private addresses of the appellants were not known.

51 In any event, according to the Council, the date of publication of the contested measures marked the starting point for the calculation of the period established in Article 263 TFEU. That interpretation follows from the requirements of legal certainty which permeate the rules on procedural time-limits.

52 Lastly, the Council states that the appellants' arguments on the extension of the time-limit on account of distance are manifestly unfounded and amount, in essence, to a challenge to the validity of Article 102(2) of the General Court's Rules of Procedure. That provision is however no more than an extension of the period laid down in the sixth paragraph of Article 263 TFEU.

Findings of the Court

53 First, it must be stated that the General Court was correct to hold that it is entitled to examine of its own motion whether the time-limit for bringing proceedings has been observed, that being a matter of public policy (see, *inter alia*, Case 79/70 *Müllers v CES* [1971] ECR 689, paragraph 6, and *Transportes Evaristo Molina v Commission*, paragraph 33).

54 It must next be recalled that, according to the sixth paragraph of Article 263 TFEU, 'proceedings provided for in this article shall be instituted within two months of the publication of the measure, or of its notification to the plaintiff, or, in the absence thereof, of the day on which it came to the knowledge of the latter, as the case may be'.

55 In this case, the contested measures were published in the Official Journal of the European Union, Series L, but were also, pursuant to Article 7(3) of Decision 2010/656, as amended by Decision 2010/801, and Article 11a(3) of Regulation No 560/2005, as amended by Regulation No 25/2011, to be communicated to the persons and entities concerned, either directly if their addresses were known, or, if not, through the publication of a notice.

56 That situation is a consequence of the particular nature of the contested measures, which at the same time resemble both measures of general application in that they impose on a category of addressees determined in a general and abstract manner a prohibition on, *inter alia*, making available funds and economic resources to persons and entities named in the lists contained in their annexes and also a bundle of individual decisions affecting those persons and entities (see, to that effect, Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation v Council and Commission* [2008] ECR I-6351, paragraphs 241 to 244).

57 It must, moreover, be recalled that, as regards measures adopted on the basis of provisions relating to the Common Foreign and Security Policy, such as the contested measures, it is the individual nature of those measures which, in accordance with the second paragraph of Article 275 TFEU and the fourth paragraph of Article 263 TFEU, permits access to the Courts of the European Union.

58 Having regard to those particular features and the consequent rules relating to publication and communication, the sixth paragraph of Article 263 TFEU would not be applied consistently if, when applied to persons and entities who are named in the lists contained in the annexes to those measures, the starting point for the calculation of the period for bringing an action for annulment was, for those persons, fixed as the date of publication of the measure at issue and not as the date when that measure was communicated to them. The purpose of that communication is precisely to ensure that persons to whom the measures are addressed are able to defend their rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in their applying to the Courts of the European Union (*Kadi and Al Barakaat International Foundation v Council and Commission*, paragraph 337).

59 It follows that while, admittedly, the entry into force of measures such as the contested measures is effected by their publication, the period for the bringing of an action for the annulment of those measures under the fourth paragraph of Article 263 TFEU runs, for each of those persons and entities, from the date of the communication which they must receive.

60 In the present case, contrary to what is claimed by the appellants, the contested measures were communicated to them.

61 It is true that those measures were not directly communicated to them at their addresses. As the Council found that it was impossible to undertake direct communication to Mr Gbagbo, Mr Koné, Ms Boni-Claverie, Mr Djédjé and Mr N'Guessan, it had recourse to publication of the notice provided for in Article 7(3) of Decision 2010/656, as amended by Decision 2010/801, and in Article 11a(3) of Regulation No 560/2005, as amended by Regulation No 25/2011. The Council therefore published, in the Official Journal of the European Union, Series C, of 18 January 2011 and 7 April 2011, the notices referred to in paragraph 29 of this judgment.

62 Given that such notices are capable of enabling the persons concerned to identify the legal remedies available to them in order to challenge their designation in the lists concerned and the date when the period for bringing proceedings expires (*C-417/11 P Council v Bamba* [2012] ECR, paragraph 81), it is important that the appellants should not be able to defer the starting point of the period for bringing proceedings by relying on the fact that there was no direct communication or that they actually became aware of the contested measures at a later date. If such a possibility were, in the absence of force majeure, open to the appellants, it would jeopardise the very objective of a time-limit for bringing proceedings, which is to protect legal certainty by ensuring that European Union measures which produce legal effects may not indefinitely be called into question (see, *inter alia*, *C-178/95 Wiljo* [1997] ECR I-585, paragraph 19; *C-241/01 National Farmers' Union* [2002] ECR I-9079, paragraph 34, and order of 15 November 2012 in *C-102/12 P Städter v ECB*, paragraph 12).

63 As regards, lastly, the appellants' argument that the extension of the time-limit on account of distance by ten days as provided for in Article 102(2) of the General Court's Rules of Procedure cannot be applied to them because they are established in a non-Member State, suffice it to observe that that argument is invalidated by the fact that the extension is for a single fixed period. It follows that the fact that the appellants were, during the period for bringing proceedings, in a non-Member State, does not, in itself, mean that they were in a situation which was objectively different, with regard to the application of that time-limit, from the situation of persons and entities established within the European Union who were the subject of restrictive measures of the same kind.

64 It follows from all the foregoing that, even though the General Court erred in law by holding that the periods for bringing proceedings started to run on the dates of publication of the contested measures, those periods, which should have been calculated from the dates referred to in paragraph 61 of this judgment, had expired on 7 July 2011, the

date when the actions were brought. That being the case, the second ground of appeal must be rejected (see, by analogy, *C-282/05 P Holcim (Deutschland) v Commission* [2007] ECR I-2941, paragraph 33).

The first ground of appeal

Arguments of the parties

65 The appellants submit that the General Court infringed Article 45 of the Statute of the Court of Justice by not finding that there was force majeure for the purposes of that article.

66 The appellants claim that the armed conflict which took place in Côte d'Ivoire should be regarded as a case of force majeure as far as they are concerned, since, during that period, they had no means of communication whereby they could become aware of the contested measures and therefore could not exercise their right to bring proceedings.

67 The Council states that one of the constituent elements of the concept of force majeure is the occurrence of an event outside the control of the person who wishes to rely on it, that is to say when something happens which the person concerned can take no action to influence (*C-334/08 Commission v Italy* [2010] ECR I-6869, paragraph 47). Yet the post-election crisis in Côte d'Ivoire and the violence associated with that crisis were provoked by the refusal of Mr Gbagbo and his colleagues to surrender power to the elected President. Those circumstances are therefore not outside the control of the appellants.

Findings of the Court

68 Under the second paragraph of Article 45 of the Statute of the Court, 'no right shall be prejudiced in consequence of the expiry of a time-limit if the party concerned proves the existence of unforeseeable circumstances or of force majeure.'

69 It is clear that, as stated by the General Court in the orders under appeal, the appellants did not argue before it that such circumstances existed.

[...]

72 It must next be observed that, in accordance with the sixth paragraph of Article 263 TFEU and Article 45 of the Statute of the Court, it is for the party concerned to establish, first, that abnormal circumstances, unforeseeable and outside his control, made it impossible for him to comply with the time-limit for bringing proceedings laid down in the sixth paragraph of Article 263 TFEU and, secondly, that he could not guard against the consequences of those circumstances by taking appropriate steps without making unreasonable sacrifices (see, to that effect, *C-314/06 Société Pipeline Méditerranée et Rhône* [2007] ECR I-12273, paragraph 24 and case-law cited).

73 In this case, the appellants make general reference to there being in Côte d'Ivoire a situation of armed conflict, which according to them began in November 2010 and continued at least until April 2011.

74 However, none of the appellants has presented, in their appeals before the Court, any material which might enable the Court to understand in what way and for what specific period of time the general situation of armed conflict in Côte d'Ivoire and the personal circumstances relied on by the appellants prevented them from bringing their actions in good time.

75 In those circumstances, the first ground of appeal must be rejected.

76 Since neither of the grounds relied on by the appellants is well founded, the appeals must be dismissed.

Costs

77 Under Article 138(1) of the Court's Rules of Procedure, which applies to the procedure on appeal by virtue of Article 184(1) thereof, the unsuccessful party is to be ordered to pay the costs if they have been applied for in the successful party's pleadings. Since the Council has applied for costs and the appellants have been unsuccessful, the appellants must be ordered to pay the costs.

On those grounds, the Court (Grand Chamber) hereby

1. Dismisses the appeals;
2. Orders Mr Laurent Gbagbo, Mr Katinan Justin Koné, Ms Akissi Danièle Boni-Claverie, Mr Alcide Djédjé and Mr Affi Pascal N'Guessan to pay the costs.

[Signatures]

C-212/11, Jyske Bank Gibraltar Ltd v Administración del Estado

JUDGMENT OF THE COURT (Third Chamber)
25 April 2013 (*)

In C-212/11,

REQUEST for a preliminary ruling under Article 267 TFEU from the Tribunal Supremo (Spain), made by decision of 21 March 2011, received at the Court on 9 May 2011, in the proceedings
Jyske Bank Gibraltar Ltd
v
Administración del Estado,

1 This request for a preliminary ruling concerns the interpretation of Article 22(2) of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ 2005 L 309, p. 15).

2 The request has been made in proceedings between Jyske Bank Gibraltar Ltd ('Jyske'), a credit institution situated in Gibraltar operating in Spain under the rules on the freedom to provide services, and the Administración del Estado concerning the decision of the Consejo de Ministros (Spanish Council of Ministers) of 23 October 2009 which rejected the application for review brought against the decision of that Consejo de Ministros of 17 April 2009 imposing on Jyske two financial penalties for a total amount of EUR 1 700 000 and two public reprimands following a refusal or lack of diligence to provide the information requested by the Servicio Ejecutivo de la Comisión para la Prevención de Blanqueo de Capitales (Executive service for the prevention of money laundering) ('the Servicio Ejecutivo').

On those grounds, the Court (Third Chamber) hereby rules:

1. Article 22(2) of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing must be interpreted as not precluding legislation of a Member State which requires credit institutions to communicate the information required for the purpose of combating money laundering and terrorist financing directly to the FIU of that Member State where the institutions carry out their activities in that State under the freedom to provide services, to the extent that that legislation does not compromise the effectiveness of that Directive and of Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.

2. Article 56 TFEU must be interpreted as not precluding such legislation if the latter is justified by overriding reasons in the public interest, secures the attainment of the aim in view and does not go beyond that which is necessary in order to attain it, and is applied in a non-discriminatory manner, which it is for the national court to ascertain taking account of the following considerations:

- such legislation is appropriate to attain the aim of preventing money laundering and terrorist financing if it enables the Member State concerned effectively to supervise and suspend suspicious financial transactions concluded by credit institutions offering their services in the national territory and, if appropriate, to pursue and punish those responsible;
- the obligation imposed by that legislation on credit institutions carrying out their activities under the freedom to provide services may constitute a proportionate measure in pursuit of that aim in the absence, at the time of the facts in the main proceedings, of any effective mechanism guaranteeing full and complete cooperation between financial intelligence units.

[Signatures]

* Language of the case: Spanish.

Relevant EU Regulations on EU Supervisory Authorities

Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010 on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board

Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC

Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC

Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC

XI. Jurisdiction

Regulation (EU) No 1215/2012 European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 67(4) and points (a), (c) and (e) of Article 81(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) On 21 April 2009, the Commission adopted a report on the application of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (3). The report concluded that, in general, the operation of that Regulation is satisfactory, but that it is desirable to improve the application of certain of its provisions, to further facilitate the free circulation of judgments and to further enhance access to justice. Since a number of amendments are to be made to that Regulation it should, in the interests of clarity, be recast.

(2) At its meeting in Brussels on 10 and 11 December 2009, the European Council adopted a new multiannual programme entitled 'The Stockholm Programme – an open and secure Europe serving and protecting citizens' (4). In the Stockholm Programme the European Council considered that the process of abolishing all intermediate measures (the *exequatur*) should be continued during the period covered by that Programme. At the same time the abolition of the *exequatur* should also be accompanied by a series of safeguards.

(3) The Union has set itself the objective of maintaining and developing an area of freedom, security and justice, *inter alia*, by facilitating access to justice, in particular through the principle of mutual recognition of judicial and extra-judicial decisions in civil matters. For the gradual establishment of such an area, the Union is to adopt measures relating to judicial cooperation in civil matters having cross-border implications, particularly when necessary for the proper functioning of the internal market.

(4) Certain differences between national rules governing jurisdiction and recognition of judgments hamper the sound operation of the internal market. Provisions to unify the rules of conflict of jurisdiction in civil and commercial matters, and to ensure rapid and simple recognition and

enforcement of judgments given in a Member State, are essential.

(5) Such provisions fall within the area of judicial cooperation in civil matters within the meaning of Article 81 of the Treaty on the Functioning of the European Union (TFEU).

(6) In order to attain the objective of free circulation of judgments in civil and commercial matters, it is necessary and appropriate that the rules governing jurisdiction and the recognition and enforcement of judgments be governed by a legal instrument of the Union which is binding and directly applicable.

(7) On 27 September 1968, the then Member States of the European Communities, acting under Article 220, fourth indent, of the Treaty establishing the European Economic Community, concluded the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, subsequently amended by conventions on the accession to that Convention of new Member States (5) ('the 1968 Brussels Convention'). On 16 September 1988, the then Member States of the European Communities and certain EFTA States concluded the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (6) ('the 1988 Lugano Convention'), which is a parallel convention to the 1968 Brussels Convention. The 1988 Lugano Convention became applicable to Poland on 1 February 2000.

(8) On 22 December 2000, the Council adopted Regulation (EC) No 44/2001, which replaces the 1968 Brussels Convention with regard to the territories of the Member States covered by the TFEU, as between the Member States except Denmark. By Council Decision 2006/325/EC (7), the Community concluded an agreement with Denmark ensuring the application of the provisions of Regulation (EC) No 44/2001 in Denmark. The 1988 Lugano Convention was revised by the Convention on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (8), signed at Lugano on 30 October 2007 by the Community, Denmark, Iceland, Norway and Switzerland ('the 2007 Lugano Convention').

(9) The 1968 Brussels Convention continues to apply to the territories of the Member States which fall within the territorial scope of that Convention and which are excluded from this Regulation pursuant to Article 355 of the TFEU.

(10) The scope of this Regulation should cover all the main civil and commercial matters apart from certain well-defined matters, in particular maintenance obligations, which should be excluded from the scope of this Regulation following the adoption of Council Regulation

- (EC) No 4/2009 of 18 December 2008 on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations (9).
- (11) For the purposes of this Regulation, courts or tribunals of the Member States should include courts or tribunals common to several Member States, such as the Benelux Court of Justice when it exercises jurisdiction on matters falling within the scope of this Regulation. Therefore, judgments given by such courts should be recognised and enforced in accordance with this Regulation.
- (12) This Regulation should not apply to arbitration. Nothing in this Regulation should prevent the courts of a Member State, when seised of an action in a matter in respect of which the parties have entered into an arbitration agreement, from referring the parties to arbitration, from staying or dismissing the proceedings, or from examining whether the arbitration agreement is null and void, inoperative or incapable of being performed, in accordance with their national law. A ruling given by a court of a Member State as to whether or not an arbitration agreement is null and void, inoperative or incapable of being performed should not be subject to the rules of recognition and enforcement laid down in this Regulation, regardless of whether the court decided on this as a principal issue or as an incidental question. On the other hand, where a court of a Member State, exercising jurisdiction under this Regulation or under national law, has determined that an arbitration agreement is null and void, inoperative or incapable of being performed, this should not preclude that court's judgment on the substance of the matter from being recognised or, as the case may be, enforced in accordance with this Regulation. This should be without prejudice to the competence of the courts of the Member States to decide on the recognition and enforcement of arbitral awards in accordance with the Convention on the Recognition and Enforcement of Foreign Arbitral Awards, done at New York on 10 June 1958 ('the 1958 New York Convention'), which takes precedence over this Regulation. This Regulation should not apply to any action or ancillary proceedings relating to, in particular, the establishment of an arbitral tribunal, the powers of arbitrators, the conduct of an arbitration procedure or any other aspects of such a procedure, nor to any action or judgment concerning the annulment, review, appeal, recognition or enforcement of an arbitral award.
- (13) There must be a connection between proceedings to which this Regulation applies and the territory of the Member States. Accordingly, common rules of jurisdiction should, in principle, apply when the defendant is domiciled in a Member State.
- (14) A defendant not domiciled in a Member State should in general be subject to the national rules of jurisdiction applicable in the territory of the Member State of the court seised. However, in order to ensure the protection of consumers and employees, to safeguard the jurisdiction of the courts of the Member States in situations where they have exclusive jurisdiction and to respect the autonomy of the parties, certain rules of jurisdiction in this Regulation should apply regardless of the defendant's domicile.
- (15) The rules of jurisdiction should be highly predictable and founded on the principle that jurisdiction is generally based on the defendant's domicile. Jurisdiction should always be available on this ground save in a few well-defined situations in which the subject-matter of the dispute or the autonomy of the parties warrants a different connecting factor. The domicile of a legal person must be defined autonomously so as to make the common rules more transparent and avoid conflicts of jurisdiction.
- (16) In addition to the defendant's domicile, there should be alternative grounds of jurisdiction based on a close connection between the court and the action or in order to facilitate the sound administration of justice. The existence of a close connection should ensure legal certainty and avoid the possibility of the defendant being sued in a court of a Member State which he could not reasonably have foreseen. This is important, particularly in disputes concerning non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation.
- (17) The owner of a cultural object as defined in Article 1(1) of Council Directive 93/7/EEC of 15 March 1993 on the return of cultural objects unlawfully removed from the territory of a Member State (10) should be able under this Regulation to initiate proceedings as regards a civil claim for the recovery, based on ownership, of such a cultural object in the courts for the place where the cultural object is situated at the time the court is seised. Such proceedings should be without prejudice to proceedings initiated under Directive 93/7/EEC.
- (18) In relation to insurance, consumer and employment contracts, the weaker party should be protected by rules of jurisdiction more favourable to his interests than the general rules.
- (19) The autonomy of the parties to a contract, other than an insurance, consumer or employment contract, where only limited autonomy to determine the courts having jurisdiction is allowed, should be respected subject to the exclusive grounds of jurisdiction laid down in this Regulation.
- (20) Where a question arises as to whether a choice-of-court agreement in favour of a court or the courts of a Member State is null and void as to its substantive validity, that question should be decided in accordance with the law of the Member State of the court or courts designated in the agreement, including the conflict-of-laws rules of that Member State.
- (21) In the interests of the harmonious administration of justice it is necessary to minimise the possibility of concurrent proceedings and to ensure that irreconcilable judgments will not be given in different Member States. There should be a clear and effective mechanism for resolving cases of *lis pendens* and related actions, and for obviating problems flowing from national differences as to the determination of the time when a case is regarded as pending. For the purposes of this Regulation, that time should be defined autonomously.
- (22) However, in order to enhance the effectiveness of exclusive choice-of-court agreements and to avoid abusive litigation tactics, it is necessary to provide for an exception to the general *lis pendens* rule in order to deal satisfactorily with a particular situation in which concurrent proceedings may arise. This is the situation where a court not designated in an exclusive choice-of-court agreement has been seised of proceedings and the designated court is seised subsequently of proceedings involving the same cause of action and between the same parties. In such a case, the court first seised should be required to stay its proceedings as soon as the designated court has been seised and until such time as the latter court declares that it has no jurisdiction under the exclusive choice-of-court agreement. This is to ensure that, in such a situation, the designated court has priority to decide on the validity of the agreement and on the

- extent to which the agreement applies to the dispute pending before it. The designated court should be able to proceed irrespective of whether the non-designated court has already decided on the stay of proceedings..This exception should not cover situations where the parties have entered into conflicting exclusive choice-of-court agreements or where a court designated in an exclusive choice-of-court agreement has been seised first. In such cases, the generalis pendensrule of this Regulation should apply.
- (23) This Regulation should provide for a flexible mechanism allowing the courts of the Member States to take into account proceedings pending before the courts of third States, considering in particular whether a judgment of a third State will be capable of recognition and enforcement in the Member State concerned under the law of that Member State and the proper administration of justice.
- (24) When taking into account the proper administration of justice, the court of the Member State concerned should assess all the circumstances of the case before it. Such circumstances may include connections between the facts of the case and the parties and the third State concerned, the stage to which the proceedings in the third State have progressed by the time proceedings are initiated in the court of the Member State and whether or not the court of the third State can be expected to give a judgment within a reasonable time..That assessment may also include consideration of the question whether the court of the third State has exclusive jurisdiction in the particular case in circumstances where a court of a Member State would have exclusive jurisdiction.
- (25) The notion of provisional, including protective, measures should include, for example, protective orders aimed at obtaining information or preserving evidence as referred to in Articles 6 and 7 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (11). It should not include measures which are not of a protective nature, such as measures ordering the hearing of a witness. This should be without prejudice to the application of Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (12).
- (26) Mutual trust in the administration of justice in the Union justifies the principle that judgments given in a Member State should be recognised in all Member States without the need for any special procedure. In addition, the aim of making cross-border litigation less time-consuming and costly justifies the abolition of the declaration of enforceability prior to enforcement in the Member State addressed. As a result, a judgment given by the courts of a Member State should be treated as if it had been given in the Member State addressed.
- (27) For the purposes of the free circulation of judgments, a judgment given in a Member State should be recognised and enforced in another Member State even if it is given against a person not domiciled in a Member State.
- (28) Where a judgment contains a measure or order which is not known in the law of the Member State addressed, that measure or order, including any right indicated therein, should, to the extent possible, be adapted to one which, under the law of that Member State, has equivalent effects attached to it and pursues similar aims. How, and by whom, the adaptation is to be carried out should be determined by each Member State.
- (29) The direct enforcement in the Member State addressed of a judgment given in another Member State without a declaration of enforceability should not jeopardise respect for the rights of the defence. Therefore, the person against whom enforcement is sought should be able to apply for refusal of the recognition or enforcement of a judgment if he considers one of the grounds for refusal of recognition to be present. This should include the ground that he had not had the opportunity to arrange for his defence where the judgment was given in default of appearance in a civil action linked to criminal proceedings. It should also include the grounds which could be invoked on the basis of an agreement between the Member State addressed and a third State concluded pursuant to Article 59 of the 1968 Brussels Convention.
- (30) A party challenging the enforcement of a judgment given in another Member State should, to the extent possible and in accordance with the legal system of the Member State addressed, be able to invoke, in the same procedure, in addition to the grounds for refusal provided for in this Regulation, the grounds for refusal available under national law and within the time-limits laid down in that law..The recognition of a judgment should, however, be refused only if one or more of the grounds for refusal provided for in this Regulation are present.
- (31) Pending a challenge to the enforcement of a judgment, it should be possible for the courts in the Member State addressed, during the entire proceedings relating to such a challenge, including any appeal, to allow the enforcement to proceed subject to a limitation of the enforcement or to the provision of security.
- (32) In order to inform the person against whom enforcement is sought of the enforcement of a judgment given in another Member State, the certificate established under this Regulation, if necessary accompanied by the judgment, should be served on that person in reasonable time before the first enforcement measure. In this context, the first enforcement measure should mean the first enforcement measure after such service.
- (33) Where provisional, including protective, measures are ordered by a court having jurisdiction as to the substance of the matter, their free circulation should be ensured under this Regulation. However, provisional, including protective, measures which were ordered by such a court without the defendant being summoned to appear should not be recognised and enforced under this Regulation unless the judgment containing the measure is served on the defendant prior to enforcement. This should not preclude the recognition and enforcement of such measures under national law. Where provisional, including protective, measures are ordered by a court of a Member State not having jurisdiction as to the substance of the matter, the effect of such measures should be confined, under this Regulation, to the territory of that Member State.
- (34) Continuity between the 1968 Brussels Convention, Regulation (EC) No 44/2001 and this Regulation should be ensured, and transitional provisions should be laid down to that end. The same need for continuity applies as regards the interpretation by the Court of Justice of the European Union of the 1968 Brussels Convention and of the Regulations replacing it.
- (35) Respect for international commitments entered into by the Member States means that this Regulation should not affect conventions relating to specific matters to which the Member States are parties.

(36) Without prejudice to the obligations of the Member States under the Treaties, this Regulation should not affect the application of bilateral conventions and agreements between a third State and a Member State concluded before the date of entry into force of Regulation (EC) No 44/2001 which concern matters governed by this Regulation.

(37) In order to ensure that the certificates to be used in connection with the recognition or enforcement of judgments, authentic instruments and court settlements under this Regulation are kept up-to-date, the power to adopt acts in accordance with Article 290 of the TFEU should be delegated to the Commission in respect of amendments to Annexes I and II to this Regulation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(38) This Regulation respects fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union, in particular the right to an effective remedy and to a fair trial guaranteed in Article 47 of the Charter.

(39) Since the objective of this Regulation cannot be sufficiently achieved by the Member States and can be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(40) The United Kingdom and Ireland, in accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland, annexed to the TEU and to the then Treaty establishing the European Community, took part in the adoption and application of Regulation (EC) No 44/2001. In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU, the United Kingdom and Ireland have notified their wish to take part in the adoption and application of this Regulation.

(41) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application, without prejudice to the possibility for Denmark of applying the amendments to Regulation (EC) No 44/2001 pursuant to Article 3 of the Agreement of 19 October 2005 between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (13),

HAVE ADOPTED THIS REGULATION:

CHAPTER I SCOPE AND DEFINITIONS

Article 1

1. This Regulation shall apply in civil and commercial matters whatever the nature of the court or tribunal. It shall not extend, in particular, to revenue, customs or administrative matters or to the liability of the State for acts and omissions in the exercise of State authority (*acta iure imperii*).

2. This Regulation shall not apply to:

(a) the status or legal capacity of natural persons, rights in property arising out of a matrimonial relationship or out of

a relationship deemed by the law applicable to such relationship to have comparable effects to marriage;

(b) bankruptcy, proceedings relating to the winding-up of insolvent companies or other legal persons, judicial arrangements, compositions and analogous proceedings;

(c) social security;

(d) arbitration;

(e) maintenance obligations arising from a family relationship, parentage, marriage or affinity;

(f) wills and succession, including maintenance obligations arising by reason of death.

Article 2

For the purposes of this Regulation:

(a) 'judgment' means any judgment given by a court or tribunal of a Member State, whatever the judgment may be called, including a decree, order, decision or writ of execution, as well as a decision on the determination of costs or expenses by an officer of the court.

For the purposes of Chapter III, 'judgment' includes provisional, including protective, measures ordered by a court or tribunal which by virtue of this Regulation has jurisdiction as to the substance of the matter. It does not include a provisional, including protective, measure which is ordered by such a court or tribunal without the defendant being summoned to appear, unless the judgment containing the measure is served on the defendant prior to enforcement;

(b) 'court settlement' means a settlement which has been approved by a court of a Member State or concluded before a court of a Member State in the course of proceedings;

(c) 'authentic instrument' means a document which has been formally drawn up or registered as an authentic instrument in the Member State of origin and the authenticity of which:

(i) relates to the signature and the content of the instrument; and

(ii) has been established by a public authority or other authority empowered for that purpose;

(d) 'Member State of origin' means the Member State in which, as the case may be, the judgment has been given, the court settlement has been approved or concluded, or the authentic instrument has been formally drawn up or registered;

(e) 'Member State addressed' means the Member State in which the recognition of the judgment is invoked or in which the enforcement of the judgment, the court settlement or the authentic instrument is sought;

(f) 'court of origin' means the court which has given the judgment the recognition of which is invoked or the enforcement of which is sought.

Article 3

For the purposes of this Regulation, 'court' includes the following authorities to the extent that they have jurisdiction in matters falling within the scope of this Regulation:

(a) in Hungary, in summary proceedings concerning orders to pay (*fizetési meghagyásos eljárás*), the notary (*közjegyző*);

(b) in Sweden, in summary proceedings concerning orders to pay (*betalningsföreläggande*) and assistance (*handräckning*), the Enforcement Authority (*Kronofogdemyndigheten*).

CHAPTER II JURISDICTION

SECTION 1

General provisions

Article 4

1. Subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State.

2. Persons who are not nationals of the Member State in which they are domiciled shall be governed by the rules of jurisdiction applicable to nationals of that Member State.

Article 5

1. Persons domiciled in a Member State may be sued in the courts of another Member State only by virtue of the rules set out in Sections 2 to 7 of this Chapter.

2. In particular, the rules of national jurisdiction of which the Member States are to notify the Commission pursuant to point (a) of Article 76(1) shall not be applicable as against the persons referred to in paragraph 1.

Article 6

1. If the defendant is not domiciled in a Member State, the jurisdiction of the courts of each Member State shall, subject to Article 18(1), Article 21(2) and Articles 24 and 25, be determined by the law of that Member State.

2. As against such a defendant, any person domiciled in a Member State may, whatever his nationality, avail himself in that Member State of the rules of jurisdiction there in force, and in particular those of which the Member States are to notify the Commission pursuant to point (a) of Article 76(1), in the same way as nationals of that Member State.

SECTION 2

Special jurisdiction

Article 7

A person domiciled in a Member State may be sued in another Member State:

- (1)(a) in matters relating to a contract, in the courts for the place of performance of the obligation in question;
(b) for the purpose of this provision and unless otherwise agreed, the place of performance of the obligation in question shall be:
 - in the case of the sale of goods, the place in a Member State where, under the contract, the goods were delivered or should have been delivered,
 - in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided;(c) if point (b) does not apply then point (a) applies;
- (2) in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur;
- (3) as regards a civil claim for damages or restitution which is based on an act giving rise to criminal proceedings, in the court seised of those proceedings, to the extent that that court has jurisdiction under its own law to entertain civil proceedings;
- (4) as regards a civil claim for the recovery, based on ownership, of a cultural object as defined in point 1 of Article 1 of Directive 93/7/EEC initiated by the person claiming the right to recover such an object, in the courts for the place where the cultural object is situated at the time when the court is seised;
- (5) as regards a dispute arising out of the operations of a branch, agency or other establishment, in the courts for the place where the branch, agency or other establishment is situated;
- (6) as regards a dispute brought against a settlor, trustee or beneficiary of a trust created by the operation of a statute, or by a written instrument, or created orally and evidenced in writing, in the courts of the Member State in which the trust is domiciled;
- (7) as regards a dispute concerning the payment of remuneration claimed in respect of the salvage of a cargo or freight, in the court under the authority of which the cargo or freight in question:
 - (a) has been arrested to secure such payment; or
 - (b) could have been so arrested, but bail or other security has been given;provided that this provision shall apply only if it is claimed that the defendant has an interest in the cargo or freight or had such an interest at the time of salvage.

Article 8

A person domiciled in a Member State may also be sued:

- (1) where he is one of a number of defendants, in the courts for the place where any one of them is domiciled, provided the claims are so closely connected that it is expedient to hear and determine them together to avoid the risk of

irreconcilable judgments resulting from separate proceedings;

- (2) as a third party in an action on a warranty or guarantee or in any other third-party proceedings, in the court seised of the original proceedings, unless these were instituted solely with the object of removing him from the jurisdiction of the court which would be competent in his case;
- (3) on a counter-claim arising from the same contract or facts on which the original claim was based, in the court in which the original claim is pending;
- (4) in matters relating to a contract, if the action may be combined with an action against the same defendant in matters relating to rights *in rem* in immovable property, in the court of the Member State in which the property is situated.

Article 9

Where by virtue of this Regulation a court of a Member State has jurisdiction in actions relating to liability from the use or operation of a ship, that court, or any other court substituted for this purpose by the internal law of that Member State, shall also have jurisdiction over claims for limitation of such liability.

SECTION 3

Jurisdiction in matters relating to insurance

Article 10

In matters relating to insurance, jurisdiction shall be determined by this Section, without prejudice to Article 6 and point 5 of Article 7.

Article 11

1. An insurer domiciled in a Member State may be sued:
 - (a) in the courts of the Member State in which he is domiciled;
 - (b) in another Member State, in the case of actions brought by the policyholder, the insured or a beneficiary, in the courts for the place where the claimant is domiciled; or
 - (c) if he is a co-insurer, in the courts of a Member State in which proceedings are brought against the leading insurer.
2. An insurer who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State.

Article 12

In respect of liability insurance or insurance of immovable property, the insurer may in addition be sued in the courts for the place where the harmful event occurred. The same applies if movable and immovable property are covered by the same insurance policy and both are adversely affected by the same contingency.

Article 13

1. In respect of liability insurance, the insurer may also, if the law of the court permits it, be joined in proceedings which the injured party has brought against the insured.
2. Articles 10, 11 and 12 shall apply to actions brought by the injured party directly against the insurer, where such direct actions are permitted.
3. If the law governing such direct actions provides that the policyholder or the insured may be joined as a party to the action, the same court shall have jurisdiction over them.

Article 14

1. Without prejudice to Article 13(3), an insurer may bring proceedings only in the courts of the Member State in which the defendant is domiciled, irrespective of whether he is the policyholder, the insured or a beneficiary.
2. The provisions of this Section shall not affect the right to bring a counter-claim in the court in which, in accordance with this Section, the original claim is pending.

Article 15

The provisions of this Section may be departed from only by an agreement:

- (1) which is entered into after the dispute has arisen;
- (2) which allows the policyholder, the insured or a beneficiary to bring proceedings in courts other than those indicated in this Section;

- (3) which is concluded between a policyholder and an insurer, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, and which has the effect of conferring jurisdiction on the courts of that Member State even if the harmful event were to occur abroad, provided that such an agreement is not contrary to the law of that Member State;
- (4) which is concluded with a policyholder who is not domiciled in a Member State, except in so far as the insurance is compulsory or relates to immovable property in a Member State; or
- (5) which relates to a contract of insurance in so far as it covers one or more of the risks set out in Article 16.

Article 16

The following are the risks referred to in point 5 of Article 15:

- (1) any loss of or damage to:
 - (a) seagoing ships, installations situated offshore or on the high seas, or aircraft, arising from perils which relate to their use for commercial purposes;
 - (b) goods in transit other than passengers' baggage where the transit consists of or includes carriage by such ships or aircraft;
- (2) any liability, other than for bodily injury to passengers or loss of or damage to their baggage:
 - (a) arising out of the use or operation of ships, installations or aircraft as referred to in point 1(a) in so far as, in respect of the latter, the law of the Member State in which such aircraft are registered does not prohibit agreements on jurisdiction regarding insurance of such risks;
 - (b) for loss or damage caused by goods in transit as described in point 1(b);
- (3) any financial loss connected with the use or operation of ships, installations or aircraft as referred to in point 1(a), in particular loss of freight or charter-hire;
- (4) any risk or interest connected with any of those referred to in points 1 to 3;
- (5) notwithstanding points 1 to 4, all 'large risks' as defined in Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (14).

SECTION 4

Jurisdiction over consumer contracts

Article 17

1. In matters relating to a contract concluded by a person, the consumer, for a purpose which can be regarded as being outside his trade or profession, jurisdiction shall be determined by this Section, without prejudice to Article 6 and point 5 of Article 7, if:

- (a) it is a contract for the sale of goods on instalment credit terms;
- (b) it is a contract for a loan repayable by instalments, or for any other form of credit, made to finance the sale of goods; or
- (c) in all other cases, the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities.

2. Where a consumer enters into a contract with a party who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, that party shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State.

3. This Section shall not apply to a contract of transport other than a contract which, for an inclusive price, provides for a combination of travel and accommodation.

Article 18

1. A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the

other party, in the courts for the place where the consumer is domiciled.

2. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled.

3. This Article shall not affect the right to bring a counter-claim in the court in which, in accordance with this Section, the original claim is pending.

Article 19

The provisions of this Section may be departed from only by an agreement:

- (1) which is entered into after the dispute has arisen;
- (2) which allows the consumer to bring proceedings in courts other than those indicated in this Section; or
- (3) which is entered into by the consumer and the other party to the contract, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, and which confers jurisdiction on the courts of that Member State, provided that such an agreement is not contrary to the law of that Member State.

SECTION 5

Jurisdiction over individual contracts of employment

Article 20

1. In matters relating to individual contracts of employment, jurisdiction shall be determined by this Section, without prejudice to Article 6, point 5 of Article 7 and, in the case of proceedings brought against an employer, point 1 of Article 8.

2. Where an employee enters into an individual contract of employment with an employer who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, the employer shall, in disputes arising out of the operations of the branch, agency or establishment, be deemed to be domiciled in that Member State.

Article 21

1. An employer domiciled in a Member State may be sued:

- (a) in the courts of the Member State in which he is domiciled; or
- (b) in another Member State:
 - (i) in the courts for the place where or from where the employee habitually carries out his work or in the courts for the last place where he did so; or
 - (ii) if the employee does not or did not habitually carry out his work in any one country, in the courts for the place where the business which engaged the employee is or was situated.

2. An employer not domiciled in a Member State may be sued in a court of a Member State in accordance with point (b) of paragraph 1.

Article 22

1. An employer may bring proceedings only in the courts of the Member State in which the employee is domiciled.

2. The provisions of this Section shall not affect the right to bring a counter-claim in the court in which, in accordance with this Section, the original claim is pending.

Article 23

The provisions of this Section may be departed from only by an agreement:

- (1) which is entered into after the dispute has arisen; or
- (2) which allows the employee to bring proceedings in courts other than those indicated in this Section.

SECTION 6

Exclusive jurisdiction

Article 24

The following courts of a Member State shall have exclusive jurisdiction, regardless of the domicile of the parties:

(1) in proceedings which have as their object rights *in rem* in immovable property or tenancies of immovable property, the courts of the Member State in which the property is situated.

However, in proceedings which have as their object tenancies of immovable property concluded for temporary private use for a maximum period of six consecutive months, the courts of the Member State in which the

defendant is domiciled shall also have jurisdiction, provided that the tenant is a natural person and that the landlord and the tenant are domiciled in the same Member State;

- (2) in proceedings which have as their object the validity of the constitution, the nullity or the dissolution of companies or other legal persons or associations of natural or legal persons, or the validity of the decisions of their organs, the courts of the Member State in which the company, legal person or association has its seat. In order to determine that seat, the court shall apply its rules of private international law;
- (3) in proceedings which have as their object the validity of entries in public registers, the courts of the Member State in which the register is kept;
- (4) in proceedings concerned with the registration or validity of patents, trade marks, designs, or other similar rights required to be deposited or registered, irrespective of whether the issue is raised by way of an action or as a defence, the courts of the Member State in which the deposit or registration has been applied for, has taken place or is under the terms of an instrument of the Union or an international convention deemed to have taken place.
Without prejudice to the jurisdiction of the European Patent Office under the Convention on the Grant of European Patents, signed at Munich on 5 October 1973, the courts of each Member State shall have exclusive jurisdiction in proceedings concerned with the registration or validity of any European patent granted for that Member State;
- (5) in proceedings concerned with the enforcement of judgments, the courts of the Member State in which the judgment has been or is to be enforced.

SECTION 7

Prorogation of jurisdiction

Article 25

1. If the parties, regardless of their domicile, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction, unless the agreement is null and void as to its substantive validity under the law of that Member State. Such jurisdiction shall be exclusive unless the parties have agreed otherwise. The agreement conferring jurisdiction shall be either:

- (a) in writing or evidenced in writing;
 - (b) in a form which accords with practices which the parties have established between themselves; or
 - (c) in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned.
2. Any communication by electronic means which provides a durable record of the agreement shall be equivalent to 'writing'.
3. The court or courts of a Member State on which a trust instrument has conferred jurisdiction shall have exclusive jurisdiction in any proceedings brought against a settlor, trustee or beneficiary, if relations between those persons or their rights or obligations under the trust are involved.
4. Agreements or provisions of a trust instrument conferring jurisdiction shall have no legal force if they are contrary to Articles 15, 19 or 23, or if the courts whose jurisdiction they purport to exclude have exclusive jurisdiction by virtue of Article 24.
5. An agreement conferring jurisdiction which forms part of a contract shall be treated as an agreement independent of the other terms of the contract.

The validity of the agreement conferring jurisdiction cannot be contested solely on the ground that the contract is not valid.

Article 26

1. Apart from jurisdiction derived from other provisions of this Regulation, a court of a Member State before which a defendant enters an appearance shall have jurisdiction. This rule shall not apply where appearance was entered to contest the jurisdiction, or where another court has exclusive jurisdiction by virtue of Article 24.

2. In matters referred to in Sections 3, 4 or 5 where the policyholder, the insured, a beneficiary of the insurance contract, the injured party, the consumer or the employee is the defendant, the court shall, before assuming jurisdiction under paragraph 1, ensure that the defendant is informed of his right to contest the jurisdiction of the court and of the consequences of entering or not entering an appearance.

SECTION 8

Examination as to jurisdiction and admissibility

Article 27

Where a court of a Member State is seised of a claim which is principally concerned with a matter over which the courts of another Member State have exclusive jurisdiction by virtue of Article 24, it shall declare of its own motion that it has no jurisdiction.

Article 28

1. Where a defendant domiciled in one Member State is sued in a court of another Member State and does not enter an appearance, the court shall declare of its own motion that it has no jurisdiction unless its jurisdiction is derived from the provisions of this Regulation.

2. The court shall stay the proceedings so long as it is not shown that the defendant has been able to receive the document instituting the proceedings or an equivalent document in sufficient time to enable him to arrange for his defence, or that all necessary steps have been taken to this end.

3. Article 19 of Regulation (EC) No 1393/2007 of the European Parliament and of the Council of 13 November 2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) (15) shall apply instead of paragraph 2 of this Article if the document instituting the proceedings or an equivalent document had to be transmitted from one Member State to another pursuant to that Regulation.

4. Where Regulation (EC) No 1393/2007 is not applicable, Article 15 of the Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters shall apply if the document instituting the proceedings or an equivalent document had to be transmitted abroad pursuant to that Convention.

SECTION 9

Lis pendens — related actions

Article 29

1. Without prejudice to Article 31(2), where proceedings involving the same cause of action and between the same parties are brought in the courts of different Member States, any court other than the court first seised shall of its own motion stay its proceedings until such time as the jurisdiction of the court first seised is established.

2. In cases referred to in paragraph 1, upon request by a court seised of the dispute, any other court seised shall without delay inform the former court of the date when it was seised in accordance with Article 32.

3. Where the jurisdiction of the court first seised is established, any court other than the court first seised shall decline jurisdiction in favour of that court.

Article 30

1. Where related actions are pending in the courts of different Member States, any court other than the court first seised may stay its proceedings.

2. Where the action in the court first seised is pending at first instance, any other court may also, on the application of one of the parties, decline jurisdiction if the court first seised has jurisdiction over the actions in question and its law permits the consolidation thereof.

3. For the purposes of this Article, actions are deemed to be related where they are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.

Article 31

1. Where actions come within the exclusive jurisdiction of several courts, any court other than the court first seised shall decline jurisdiction in favour of that court.

2. Without prejudice to Article 26, where a court of a Member State on which an agreement as referred to in Article 25 confers exclusive jurisdiction is seised, any court of another Member State shall stay the proceedings until such time as the court seised on the basis of the agreement declares that it has no jurisdiction under the agreement.

3. Where the court designated in the agreement has established jurisdiction in accordance with the agreement, any court of another Member State shall decline jurisdiction in favour of that court.

4. Paragraphs 2 and 3 shall not apply to matters referred to in Sections 3, 4 or 5 where the policyholder, the insured, a beneficiary of the insurance contract, the injured party, the consumer or the employee is the claimant and the agreement is not valid under a provision contained within those Sections.

Article 32

1. For the purposes of this Section, a court shall be deemed to be seised:

(a) at the time when the document instituting the proceedings or an equivalent document is lodged with the court, provided that the claimant has not subsequently failed to take the steps he was required to take to have service effected on the defendant; or

(b) if the document has to be served before being lodged with the court, at the time when it is received by the authority responsible for service, provided that the claimant has not subsequently failed to take the steps he was required to take to have the document lodged with the court.

The authority responsible for service referred to in point (b) shall be the first authority receiving the documents to be served.

2. The court, or the authority responsible for service, referred to in paragraph 1, shall note, respectively, the date of the lodging of the document instituting the proceedings or the equivalent document, or the date of receipt of the documents to be served.

Article 33

1. Where jurisdiction is based on Article 4 or on Articles 7, 8 or 9 and proceedings are pending before a court of a third State at the time when a court in a Member State is seised of an action involving the same cause of action and between the same parties as the proceedings in the court of the third State, the court of the Member State may stay the proceedings if:

(a) it is expected that the court of the third State will give a judgment capable of recognition and, where applicable, of enforcement in that Member State; and

(b) the court of the Member State is satisfied that a stay is necessary for the proper administration of justice.

2. The court of the Member State may continue the proceedings at any time if:

(a) the proceedings in the court of the third State are themselves stayed or discontinued;

(b) it appears to the court of the Member State that the proceedings in the court of the third State are unlikely to be concluded within a reasonable time; or

(c) the continuation of the proceedings is required for the proper administration of justice.

3. The court of the Member State shall dismiss the proceedings if the proceedings in the court of the third State are concluded and have resulted in a judgment capable of recognition and, where applicable, of enforcement in that Member State.

4. The court of the Member State shall apply this Article on the application of one of the parties or, where possible under national law, of its own motion.

Article 34

1. Where jurisdiction is based on Article 4 or on Articles 7, 8 or 9 and an action is pending before a court of a third State at the time when a court in a Member State is seised of an action which is related to the action in the court of the third State, the court of the Member State may stay the proceedings if:

(a) it is expedient to hear and determine the related actions together to avoid the risk of irreconcilable judgments resulting from separate proceedings;

(b) it is expected that the court of the third State will give a judgment capable of recognition and, where applicable, of enforcement in that Member State; and

(c) the court of the Member State is satisfied that a stay is necessary for the proper administration of justice.

2. The court of the Member State may continue the proceedings at any time if:

(a) it appears to the court of the Member State that there is no longer a risk of irreconcilable judgments;

(b) the proceedings in the court of the third State are themselves stayed or discontinued;

(c) it appears to the court of the Member State that the proceedings in the court of the third State are unlikely to be concluded within a reasonable time; or

(d) the continuation of the proceedings is required for the proper administration of justice.

3. The court of the Member State may dismiss the proceedings if the proceedings in the court of the third State are concluded and have resulted in a judgment capable of recognition and, where applicable, of enforcement in that Member State.

4. The court of the Member State shall apply this Article on the application of one of the parties or, where possible under national law, of its own motion.

SECTION 10

Provisional, including protective, measures

Article 35

Application may be made to the courts of a Member State for such provisional, including protective, measures as may be available under the law of that Member State, even if the courts of another Member State have jurisdiction as to the substance of the matter.

CHAPTER III

RECOGNITION AND ENFORCEMENT

SECTION 1

Recognition

Article 36

1. A judgment given in a Member State shall be recognised in the other Member States without any special procedure being required.

2. Any interested party may, in accordance with the procedure provided for in Subsection 2 of Section 3, apply for a decision that there are no grounds for refusal of recognition as referred to in Article 45.

3. If the outcome of proceedings in a court of a Member State depends on the determination of an incidental question of refusal of recognition, that court shall have jurisdiction over that question.

Article 37

1. A party who wishes to invoke in a Member State a judgment given in another Member State shall produce:

(a) a copy of the judgment which satisfies the conditions necessary to establish its authenticity; and

(b) the certificate issued pursuant to Article 53.

2. The court or authority before which a judgment given in another Member State is invoked may, where necessary, require the party invoking it to provide, in accordance with Article 57, a translation or a transliteration of the contents of the certificate referred to in point (b) of paragraph 1. The court or authority may require the party to provide a translation of the judgment instead of a translation of the contents of the certificate if it is unable to proceed without such a translation.

Article 38

The court or authority before which a judgment given in another Member State is invoked may suspend the proceedings, in whole or in part, if:

- (a) the judgment is challenged in the Member State of origin; or
- (b) an application has been submitted for a decision that there are no grounds for refusal of recognition as referred to in Article 45 or for a decision that the recognition is to be refused on the basis of one of those grounds.

SECTION 2

Enforcement

Article 39

A judgment given in a Member State which is enforceable in that Member State shall be enforceable in the other Member States without any declaration of enforceability being required.

Article 40

An enforceable judgment shall carry with it by operation of law the power to proceed to any protective measures which exist under the law of the Member State addressed.

Article 41

1. Subject to the provisions of this Section, the procedure for the enforcement of judgments given in another Member State shall be governed by the law of the Member State addressed. A judgment given in a Member State which is enforceable in the Member State addressed shall be enforced there under the same conditions as a judgment given in the Member State addressed.

2. Notwithstanding paragraph 1, the grounds for refusal or of suspension of enforcement under the law of the Member State addressed shall apply in so far as they are not incompatible with the grounds referred to in Article 45.

3. The party seeking the enforcement of a judgment given in another Member State shall not be required to have a postal address in the Member State addressed. Nor shall that party be required to have an authorised representative in the Member State addressed unless such a representative is mandatory irrespective of the nationality or the domicile of the parties.

Article 42

1. For the purposes of enforcement in a Member State of a judgment given in another Member State, the applicant shall provide the competent enforcement authority with:

- (a) a copy of the judgment which satisfies the conditions necessary to establish its authenticity; and
- (b) the certificate issued pursuant to Article 53, certifying that the judgment is enforceable and containing an extract of the judgment as well as, where appropriate, relevant information on the recoverable costs of the proceedings and the calculation of interest.

2. For the purposes of enforcement in a Member State of a judgment given in another Member State ordering a provisional, including a protective, measure, the applicant shall provide the competent enforcement authority with:

- (a) a copy of the judgment which satisfies the conditions necessary to establish its authenticity;
- (b) the certificate issued pursuant to Article 53, containing a description of the measure and certifying that:
 - (i) the court has jurisdiction as to the substance of the matter;
 - (ii) the judgment is enforceable in the Member State of origin; and
- (c) where the measure was ordered without the defendant being summoned to appear, proof of service of the judgment.

3. The competent enforcement authority may, where necessary, require the applicant to provide, in accordance with Article 57, a translation or a transliteration of the contents of the certificate.

4. The competent enforcement authority may require the applicant to provide a translation of the judgment only if it is unable to proceed without such a translation.

Article 43

1. Where enforcement is sought of a judgment given in another Member State, the certificate issued pursuant to Article 53 shall be served on the person against whom the enforcement is sought prior to the first enforcement measure. The certificate shall be accompanied by the judgment, if not already served on that person.

2. Where the person against whom enforcement is sought is domiciled in a Member State other than the Member State of origin, he may request a translation of the judgment in order to contest the enforcement if the judgment is not written in or accompanied by a translation into either of the following languages:

- (a) a language which he understands; or
- (b) the official language of the Member State in which he is domiciled or, where there are several official languages in that Member State, the official language or one of the official languages of the place where he is domiciled.

Where a translation of the judgment is requested under the first subparagraph, no measures of enforcement may be taken other than protective measures until that translation has been provided to the person against whom enforcement is sought. This paragraph shall not apply if the judgment has already been served on the person against whom enforcement is sought in one of the languages referred to in the first subparagraph or is accompanied by a translation into one of those languages.

3. This Article shall not apply to the enforcement of a protective measure in a judgment or where the person seeking enforcement proceeds to protective measures in accordance with Article 40.

Article 44

1. In the event of an application for refusal of enforcement of a judgment pursuant to Subsection 2 of Section 3, the court in the Member State addressed may, on the application of the person against whom enforcement is sought:

- (a) limit the enforcement proceedings to protective measures;
- (b) make enforcement conditional on the provision of such security as it shall determine; or
- (c) suspend, either wholly or in part, the enforcement proceedings.

2. The competent authority in the Member State addressed shall, on the application of the person against whom enforcement is sought, suspend the enforcement proceedings where the enforceability of the judgment is suspended in the Member State of origin.

SECTION 3

Refusal of recognition and enforcement

Subsection 1

Refusal of recognition

Article 45

1. On the application of any interested party, the recognition of a judgment shall be refused:

- (a) if such recognition is manifestly contrary to public policy (ordre public) in the Member State addressed;
- (b) where the judgment was given in default of appearance, if the defendant was not served with the document which instituted the proceedings or with an equivalent document in sufficient time and in such a way as to enable him to arrange for his defence, unless the defendant failed to commence proceedings to challenge the judgment when it was possible for him to do so;
- (c) if the judgment is irreconcilable with a judgment given between the same parties in the Member State addressed;
- (d) if the judgment is irreconcilable with an earlier judgment given in another Member State or in a third State involving the same cause of action and between the same parties, provided that the earlier judgment fulfils the conditions necessary for its recognition in the Member State addressed; or
- (e) if the judgment conflicts with:
 - (i) Sections 3, 4 or 5 of Chapter II where the policyholder, the insured, a beneficiary of the insurance contract, the injured party, the consumer or the employee was the defendant; or

(ii) Section 6 of Chapter II.

2. In its examination of the grounds of jurisdiction referred to in point (e) of paragraph 1, the court to which the application was submitted shall be bound by the findings of fact on which the court of origin based its jurisdiction.

3. Without prejudice to point (e) of paragraph 1, the jurisdiction of the court of origin may not be reviewed. The test of public policy referred to in point (a) of paragraph 1 may not be applied to the rules relating to jurisdiction.

4. The application for refusal of recognition shall be made in accordance with the procedures provided for in Subsection 2 and, where appropriate, Section 4.

Subsection 2 Refusal of enforcement

Article 46

On the application of the person against whom enforcement is sought, the enforcement of a judgment shall be refused where one of the grounds referred to in Article 45 is found to exist.

Article 47

1. The application for refusal of enforcement shall be submitted to the court which the Member State concerned has communicated to the Commission pursuant to point (a) of Article 75 as the court to which the application is to be submitted.

2. The procedure for refusal of enforcement shall, in so far as it is not covered by this Regulation, be governed by the law of the Member State addressed.

3. The applicant shall provide the court with a copy of the judgment and, where necessary, a translation or transliteration of it.

The court may dispense with the production of the documents referred to in the first subparagraph if it already possesses them or if it considers it unreasonable to require the applicant to provide them. In the latter case, the court may require the other party to provide those documents.

4. The party seeking the refusal of enforcement of a judgment given in another Member State shall not be required to have a postal address in the Member State addressed. Nor shall that party be required to have an authorised representative in the Member State addressed unless such a representative is mandatory irrespective of the nationality or the domicile of the parties.

Article 48

The court shall decide on the application for refusal of enforcement without delay.

Article 49

1. The decision on the application for refusal of enforcement may be appealed against by either party.

2. The appeal is to be lodged with the court which the Member State concerned has communicated to the Commission pursuant to point (b) of Article 75 as the court with which such an appeal is to be lodged.

Article 50

The decision given on the appeal may only be contested by an appeal where the courts with which any further appeal is to be lodged have been communicated by the Member State concerned to the Commission pursuant to point (c) of Article 75.

Article 51

1. The court to which an application for refusal of enforcement is submitted or the court which hears an appeal lodged under Article 49 or Article 50 may stay the proceedings if an ordinary appeal has been lodged against the judgment in the Member State of origin or if the time for such an appeal has not yet expired. In the latter case, the court may specify the time within which such an appeal is to be lodged.

2. Where the judgment was given in Ireland, Cyprus or the United Kingdom, any form of appeal available in the Member State of origin shall be treated as an ordinary appeal for the purposes of paragraph 1.

SECTION 4 Common provisions

Article 52

Under no circumstances may a judgment given in a Member State be reviewed as to its substance in the Member State addressed.

Article 53

The court of origin shall, at the request of any interested party, issue the certificate using the form set out in Annex I.

Article 54

1. If a judgment contains a measure or an order which is not known in the law of the Member State addressed, that measure or order shall, to the extent possible, be adapted to a measure or an order known in the law of that Member State which has equivalent effects attached to it and which pursues similar aims and interests.

Such adaptation shall not result in effects going beyond those provided for in the law of the Member State of origin.

2. Any party may challenge the adaptation of the measure or order before a court.

3. If necessary, the party invoking the judgment or seeking its enforcement may be required to provide a translation or a transliteration of the judgment.

Article 55

A judgment given in a Member State which orders a payment by way of a penalty shall be enforceable in the Member State addressed only if the amount of the payment has been finally determined by the court of origin.

Article 56

No security, bond or deposit, however described, shall be required of a party who in one Member State applies for the enforcement of a judgment given in another Member State on the ground that he is a foreign national or that he is not domiciled or resident in the Member State addressed.

Article 57

1. When a translation or a transliteration is required under this Regulation, such translation or transliteration shall be into the official language of the Member State concerned or, where there are several official languages in that Member State, into the official language or one of the official languages of court proceedings of the place where a judgment given in another Member State is invoked or an application is made, in accordance with the law of that Member State.

2. For the purposes of the forms referred to in Articles 53 and 60, translations or transliterations may also be into any other official language or languages of the institutions of the Union that the Member State concerned has indicated it can accept.

3. Any translation made under this Regulation shall be done by a person qualified to do translations in one of the Member States.

CHAPTER IV AUTHENTIC INSTRUMENTS AND COURT SETTLEMENTS

Article 58

1. An authentic instrument which is enforceable in the Member State of origin shall be enforceable in the other Member States without any declaration of enforceability being required. Enforcement of the authentic instrument may be refused only if such enforcement is manifestly contrary to public policy (*ordre public*) in the Member State addressed.

The provisions of Section 2, Subsection 2 of Section 3, and Section 4 of Chapter III shall apply as appropriate to authentic instruments.

2. The authentic instrument produced must satisfy the conditions necessary to establish its authenticity in the Member State of origin.

Article 59

A court settlement which is enforceable in the Member State of origin shall be enforced in the other Member States under the same conditions as authentic instruments.

Article 60

The competent authority or court of the Member State of origin shall, at the request of any interested party, issue the certificate using the form set out in Annex II containing a summary of the enforceable obligation recorded in the authentic instrument or of the agreement between the parties recorded in the court settlement.

CHAPTER V

GENERAL PROVISIONS

Article 61

No legalisation or other similar formality shall be required for documents issued in a Member State in the context of this Regulation.

Article 62

1. In order to determine whether a party is domiciled in the Member State whose courts are seised of a matter, the court shall apply its internal law.

2. If a party is not domiciled in the Member State whose courts are seised of the matter, then, in order to determine whether the party is domiciled in another Member State, the court shall apply the law of that Member State.

Article 63

1. For the purposes of this Regulation, a company or other legal person or association of natural or legal persons is domiciled at the place where it has its:

- (a) statutory seat;
- (b) central administration; or
- (c) principal place of business.

2. For the purposes of Ireland, Cyprus and the United Kingdom, 'statutory seat' means the registered office or, where there is no such office anywhere, the place of incorporation or, where there is no such place anywhere, the place under the law of which the formation took place.

3. In order to determine whether a trust is domiciled in the Member State whose courts are seised of the matter, the court shall apply its rules of private international law.

Article 64

Without prejudice to any more favourable provisions of national laws, persons domiciled in a Member State who are being prosecuted in the criminal courts of another Member State of which they are not nationals for an offence which was not intentionally committed may be defended by persons qualified to do so, even if they do not appear in person. However, the court seised of the matter may order appearance in person; in the case of failure to appear, a judgment given in the civil action without the person concerned having had the opportunity to arrange for his defence need not be recognised or enforced in the other Member States.

Article 65

1. The jurisdiction specified in point 2 of Article 8 and Article 13 in actions on a warranty or guarantee or in any other third-party proceedings may be resorted to in the Member States included in the list established by the Commission pursuant to point (b) of Article 76(1) and Article 76(2) only in so far as permitted under national law. A person domiciled in another Member State may be invited to join the proceedings before the courts of those Member States pursuant to the rules on third-party notice referred to in that list.

2. Judgments given in a Member State by virtue of point 2 of Article 8 or Article 13 shall be recognised and enforced in accordance with Chapter III in any other Member State. Any effects which judgments given in the Member States included in the list referred to in paragraph 1 may have, in accordance with the law of those Member States, on third parties by application of paragraph 1 shall be recognised in all Member States.

3. The Member States included in the list referred to in paragraph 1 shall, within the framework of the European Judicial Network in civil and commercial matters established by Council Decision 2001/470/EC (16) ('the European Judicial Network') provide information on how to determine, in accordance with their national law, the effects of the judgments referred to in the second sentence of paragraph 2.

CHAPTER VI

TRANSITIONAL PROVISIONS

Article 66

1. This Regulation shall apply only to legal proceedings instituted, to authentic instruments formally drawn up or registered and to court settlements approved or concluded on or after 10 January 2015.

2. Notwithstanding Article 80, Regulation (EC) No 44/2001 shall continue to apply to judgments given in legal proceedings instituted, to authentic instruments formally drawn up or registered and to court settlements approved or concluded before 10 January 2015 which fall within the scope of that Regulation.

CHAPTER VII

RELATIONSHIP WITH OTHER INSTRUMENTS

Article 67

This Regulation shall not prejudice the application of provisions governing jurisdiction and the recognition and enforcement of judgments in specific matters which are contained in instruments of the Union or in national legislation harmonised pursuant to such instruments.

Article 68

1. This Regulation shall, as between the Member States, supersede the 1968 Brussels Convention, except as regards the territories of the Member States which fall within the territorial scope of that Convention and which are excluded from this Regulation pursuant to Article 355 of the TFEU.

2. In so far as this Regulation replaces the provisions of the 1968 Brussels Convention between the Member States, any reference to that Convention shall be understood as a reference to this Regulation.

Article 69

Subject to Articles 70 and 71, this Regulation shall, as between the Member States, supersede the conventions that cover the same matters as those to which this Regulation applies. In particular, the conventions included in the list established by the Commission pursuant to point (c) of Article 76(1) and Article 76(2) shall be superseded.

Article 70

1. The conventions referred to in Article 69 shall continue to have effect in relation to matters to which this Regulation does not apply.

2. They shall continue to have effect in respect of judgments given, authentic instruments formally drawn up or registered and court settlements approved or concluded before the date of entry into force of Regulation (EC) No 44/2001.

Article 71

1. This Regulation shall not affect any conventions to which the Member States are parties and which, in relation to particular matters, govern jurisdiction or the recognition or enforcement of judgments.

2. With a view to its uniform interpretation, paragraph 1 shall be applied in the following manner:

(a) this Regulation shall not prevent a court of a Member State which is party to a convention on a particular matter from assuming jurisdiction in accordance with that convention, even where the defendant is domiciled in another Member State which is not party to that convention. The court hearing the action shall, in any event, apply Article 28 of this Regulation;

(b) judgments given in a Member State by a court in the exercise of jurisdiction provided for in a convention on a particular matter shall be recognised and enforced in the other Member States in accordance with this Regulation.

Where a convention on a particular matter to which both the Member State of origin and the Member State addressed are parties lays down conditions for the recognition or enforcement of judgments, those conditions shall apply. In any event, the provisions of this Regulation on recognition and enforcement of judgments may be applied.

Article 72

This Regulation shall not affect agreements by which Member States, prior to the entry into force of Regulation (EC) No 44/2001, undertook pursuant to Article 59 of the 1968 Brussels Convention not to recognise judgments given, in particular in other Contracting States to that Convention, against defendants domiciled or habitually resident in a third State where, in cases provided for in Article 4 of that Convention, the judgment could only be founded on a ground of jurisdiction specified in the second paragraph of Article 3 of that Convention.

Article 73

1. This Regulation shall not affect the application of the 2007 Lugano Convention.
2. This Regulation shall not affect the application of the 1958 New York Convention.
3. This Regulation shall not affect the application of bilateral conventions and agreements between a third State and a Member State concluded before the date of entry into force of Regulation (EC) No 44/2001 which concern matters governed by this Regulation.

**CHAPTER VIII
FINAL PROVISIONS**

Article 74

The Member States shall provide, within the framework of the European Judicial Network and with a view to making the information available to the public, a description of national rules and procedures concerning enforcement, including authorities competent for enforcement, and information on any limitations on enforcement, in particular debtor protection rules and limitation or prescription periods.

The Member States shall keep this information permanently updated.

Article 75

By 10 January 2014, the Member States shall communicate to the Commission:

- (a) the courts to which the application for refusal of enforcement is to be submitted pursuant to Article 47(1);
- (b) the courts with which an appeal against the decision on the application for refusal of enforcement is to be lodged pursuant to Article 49(2);
- (c) the courts with which any further appeal is to be lodged pursuant to Article 50; and
- (d) the languages accepted for translations of the forms as referred to in Article 57(2).

The Commission shall make the information publicly available through any appropriate means, in particular through the European Judicial Network.

Article 76

1. The Member States shall notify the Commission of:

- (a) the rules of jurisdiction referred to in Articles 5(2) and 6(2);
- (b) the rules on third-party notice referred to in Article 65; and
- (c) the conventions referred to in Article 69.

2. The Commission shall, on the basis of the notifications by the Member States referred to in paragraph 1, establish the corresponding lists.

3. The Member States shall notify the Commission of any subsequent amendments required to be made to those lists. The Commission shall amend those lists accordingly.

4. The Commission shall publish the lists and any subsequent amendments made to them in the *Official Journal of the European Union*.

5. The Commission shall make all information notified pursuant to paragraphs 1 and 3 publicly available through any other appropriate means, in particular through the European Judicial Network.

Article 77

The Commission shall be empowered to adopt delegated acts in accordance with Article 78 concerning the amendment of Annexes I and II.

Article 78

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 77 shall be conferred on the Commission for an indeterminate period of time from 9 January 2013.

3. The delegation of power referred to in Article 77 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 77 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 79

By 11 January 2022 the Commission shall present a report to the European Parliament, to the Council and to the European Economic and Social Committee on the application of this Regulation. That report shall include an evaluation of the possible need for a further extension of the rules on jurisdiction to defendants not domiciled in a Member State, taking into account the operation of this Regulation and possible developments at international level. Where appropriate, the report shall be accompanied by a proposal for amendment of this Regulation.

Article 80

This Regulation shall repeal Regulation (EC) No 44/2001. References to the repealed Regulation shall be construed as references to this Regulation and shall be read in accordance with the correlation table set out in Annex III.

Article 81

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 10 January 2015, with the exception of Articles 75 and 76, which shall apply from 10 January 2014.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Strasbourg, 12 December 2012.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

A. D. MAVROYIANNIS

(1) OJ C 218, 23.7.2011, p. 78.

(2) Position of the European Parliament of 20 November 2012 (not yet published in the Official Journal) and decision of the Council of 6 December 2012.

(3) OJ L 12, 16.1.2001, p. 1.

(4) OJ C 115, 4.5.2010, p. 1.

(5) OJ L 299, 31.12.1972, p. 32, OJ L 304, 30.10.1978, p. 1, OJ L 388, 31.12.1982, p. 1, OJ L 285, 3.10.1989, p. 1, OJ C 15, 15.1.1997, p. 1. For a consolidated text, see OJ C 27, 26.1.1998, p. 1.

(6) OJ L 319, 25.11.1988, p. 9.

(7) OJ L 120, 5.5.2006, p. 22.

(8) OJ L 147, 10.6.2009, p. 5.

(9) OJ L 7, 10.1.2009, p. 1.

(10) OJ L 74, 27.3.1993, p. 74.

(11) OJ L 157, 30.4.2004, p. 45.

(12) OJ L 174, 27.6.2001, p. 1.

(13) OJ L 299, 16.11.2005, p. 62.

(14) OJ L 335, 17.12.2009, p. 1.

(15) OJ L 324, 10.12.2007, p. 79.

(16) OJ L 174, 27.6.2001, p. 25.

Relevant Case Law on the repealed council Regulation no 44/2001

C-478/12 Maletic

Circumstances:

11. The Maletics are domiciled in Bludesch (Austria), which lies within the jurisdiction of the Bezirksgericht Bludenz (District Court, Bludenz). On 30 December 2011, they booked and paid for themselves, as private individuals, a package holiday to Egypt on the website of lastminute.com for EUR 1 858 from 10 to 24 January 2012. On its website, lastminute.com, a company whose registered office is in Munich (Germany), stated that it acted as the travel agent and that the trip would be operated by TUI, which has its registered office in Vienna (Austria).

12 The booking made by the applicants in the main proceedings concerned the Jaz Makadi Golf & Spa hotel in Hurghada (Egypt). That booking was confirmed by lastminute.com, which passed it on to TUI. Subsequently, the Maletics received a 'confirmation/invoice' of 5 January 2012 from TUI which, while it confirmed the information concerning the trip booked with lastminute.com, mentioned the name of another hotel, the Jaz Makadi Star Resort Spa in Hurghada.

13 It was only on their arrival in Hurghada that the applicants in the main proceedings noticed the mistake concerning the hotel and paid a surcharge of EUR 1 036 to be able to stay in the hotel initially booked on lastminute.com's website.

14 On 13 April 2012, in order to recover the surcharge paid and to be compensated for the inconvenience which affected their holiday, the applicants in the main proceedings brought an action before the Bezirksgericht Bludenz seeking payment from lastminute.com and TUI, jointly and severally of the sum of EUR 1 201.38 together with interest and costs.

21 In those circumstances, the Landgericht Feldkirch (Regional Court, Feldkirch) decided to stay the proceedings before it and to refer the following question to the Court for a preliminary ruling:

Preliminary question:

'Is Article 16(1) of [Regulation No 44/2001], which confers jurisdiction on the courts for the place where the consumer is domiciled, to be interpreted as meaning that, in the case where the other party to the contract (here, a travel agent having its seat abroad) has recourse to a contracting partner (here, a travel operator having its seat in the home country), Article 16(1) of Regulation No 44/2001 is, for the purpose of proceedings brought against those two parties, also applicable to the contracting partner in the home country?'

Judgement:

The concept of 'other party to the contract' laid down in Article 16(1) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning, in circumstances such as those at issue in the main proceedings, that it also covers the contracting partner of the operator with which the consumer concluded that contract and which has its registered office in the Member State in which the consumer is domiciled.

Joined Cases C-509/09 and C-161/10 eDate Advertising GmbH v X, Olivier Martinez, Robert Martinez v MGN Limited

Operative part of the judgment

1. Article 5(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that, in the event of an alleged infringement of personality rights by means of content placed online on an internet website, the person who considers that his rights have been infringed has the option of bringing an action for liability, in respect of all the damage caused, either before the courts of the Member State in which the publisher of that content is established or before the courts of the Member State in which the centre of his interests is based. That person may also, instead of an action for liability in respect of all the damage caused, bring his action before the courts of each Member State in the territory of which content placed online is or has been accessible. Those courts have jurisdiction only in respect of the damage caused in the territory of the Member State of the court seised.

2. Article 3 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), must be interpreted as not requiring transposition in the form of a specific conflict-of-laws rule. Nevertheless, in relation to the coordinated field, Member States must ensure that, subject to the derogations authorised in accordance with the conditions set out in Article 3(4) of Directive 2000/31, the provider of an electronic commerce service is not made subject to stricter requirements than those provided for by the substantive law applicable in the Member State in which that service provider is established.

Joined Cases C-585/08 and C-144/09, Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09)

Operative part of the judgment:

1. A contract concerning a voyage by freighter, such as that at issue in the main proceedings in C-585/08, is a contract of transport which, for an inclusive price, provides for a combination of travel and accommodation within the meaning of Article 15(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

2. In order to determine whether a trader whose activity is presented on its website or on that of an intermediary can be considered to be 'directing' its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of Regulation No 44/2001, it should be ascertained whether, before the conclusion of any contract with the consumer, it is apparent from those websites and the trader's overall activity that the trader was envisaging doing business with consumers domiciled in one or more Member States,

including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with them.

The following matters, the list of which is not exhaustive, are capable of constituting evidence from which it may be concluded that the trader's activity is directed to the Member State of the consumer's domicile, namely the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States. It is for the national courts to ascertain whether such evidence exists.

On the other hand, the mere accessibility of the trader's or the intermediary's website in the Member State in which the consumer is domiciled is insufficient. The same is true of mention of an email address and of other contact details, or of use of a language or a currency which are the language and/or currency generally used in the Member State in which the trader is established.

***C-523/10, Wintersteiger AG v Products 4U
Sondermaschinenbau GmbH,***

Operative part of the judgment:

Article 5(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that an action relating to infringement of a trade mark registered in a Member State because of the use, by an advertiser, of a keyword identical to that trade mark on a search engine website operating under a country-specific top-level domain of another Member State may be brought before either the courts of the Member State in which the trade mark is registered or the courts of the Member State of the place of establishment of the advertiser.

C-170/12, Peter Pinckney v KDG Mediatech AG,

Article 5(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that, in the event of alleged infringement of copyrights protected by the Member State of the court seised, the latter has jurisdiction to hear an action to establish liability brought by the author of a work against a company established in another Member State and which has, in the latter State, reproduced that work on a material support which is subsequently sold by companies established in a third Member State through an internet site also accessible with the jurisdiction of the court seised. That court has jurisdiction only to determine the damage caused in the Member State within which it is situated.

C-190/11, Daniela Mühlleitner v Ahmad Yusufi, Wadat Yusufi,

11 According to the order for reference and the documents in the case-file, Ms Mühlleitner, domiciled in Austria, searched on the internet for a car of a German make which she wished to acquire for her private use. After connecting to the German search platform www.mobile.de, she entered the make and type of vehicle she wanted, thereby obtaining a list of vehicles corresponding to the characteristics specified.

12 After selecting the vehicle which corresponded best to her search criteria, she was directed to an offer from the defendants, Mr A. Yusufi and Mr W. Yusufi, who operate a motor vehicle retail business via Autohaus Yusufi GbR ('Autohaus Yusufi'), a partnership established in Hamburg (Germany).

13 Wishing to obtain more information about the vehicle offered on the search platform, Ms Mühlleitner contacted the defendants, using the telephone number stated on the website of Autohaus Yusufi, which included an international dialling code. As the vehicle in question was no longer available, she was offered another vehicle, details of which were subsequently sent by email. She was also informed that her Austrian nationality would not prevent her from acquiring a vehicle from the defendants.

14 Ms Mühlleitner then went to Germany and, by a contract of sale signed on 21 September 2009 in Hamburg, bought the vehicle from Mr A. Yusufi and Mr W. Yusufi at a price of EUR 11 500, taking immediate delivery of it.

15 On her return to Austria Ms Mühlleitner discovered that the vehicle she had purchased was defective, and consequently asked the defendants to repair it.

16 When the defendants refused to repair the vehicle, Ms Mühlleitner brought proceedings in the court of her place of domicile, the Landesgericht Wels (Regional Court, Wels) (Austria), for rescission of the contract for the sale of the vehicle, which she claims to have concluded as a consumer with an undertaking directing its commercial or professional activities to Austria, a case falling within Article 15(1)(c) of the Brussels I Regulation.

17 The defendants contested Ms Mühlleitner's status of 'consumer' and the international jurisdiction of the Austrian courts, arguing that the dispute should be brought before the competent German courts. They also submitted that they did not direct their activities to Austria and that Ms Mühlleitner had concluded the contract at the seat of their undertaking in Germany.

.....

25 In those circumstances, the Oberster Gerichtshof decided to stay the proceedings and refer the following question to the Court for a preliminary ruling:

'Does the application of Article 15(1)(c) of [the Brussels I Regulation] presuppose that the contract between the consumer and the undertaking has been concluded at a distance?'

....

On those grounds, the Court (Fourth Chamber) hereby rules:

Article 15(1)(c) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as not requiring the contract between the consumer and the trader to be concluded at a distance.

Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)

Having regard to the Treaty establishing the European Community, and in particular Article 61(c) and the second indent of Article 67(5) thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (2),

Whereas:

(1) The Community has set itself the objective of maintaining and developing an area of freedom, security and justice. For the progressive establishment of such an area, the Community is to adopt measures relating to judicial cooperation in civil matters with a cross-border impact to the extent necessary for the proper functioning of the internal market.

(2) According to Article 65, point (b) of the Treaty, these measures are to include those promoting the compatibility of the rules applicable in the Member States concerning the conflict of laws and of jurisdiction.

(3) The European Council meeting in Tampere on 15 and 16 October 1999 endorsed the principle of mutual recognition of judgments and other decisions of judicial authorities as the cornerstone of judicial cooperation in civil matters and invited the Council and the Commission to adopt a programme of measures to implement that principle.

(4) On 30 November 2000 the Council adopted a joint Commission and Council programme of measures for implementation of the principle of mutual recognition of decisions in civil and commercial matters (3). The programme identifies measures relating to the harmonisation of conflict-of-law rules as those facilitating the mutual recognition of judgments.

(5) The Hague Programme (4), adopted by the European Council on 5 November 2004, called for work to be pursued actively on the conflict-of-law rules regarding contractual obligations (Rome I).

(6) The proper functioning of the internal market creates a need, in order to improve the predictability of the outcome of litigation, certainty as to the law applicable and the free movement of judgments, for the conflict-of-law rules in the Member States to designate the same national law irrespective of the country of the court in which an action is brought.

(7) The substantive scope and the provisions of this Regulation should be consistent with Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (5) (Brussels I) and Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (6).

(8) Family relationships should cover parentage, marriage, affinity and collateral relatives. The reference in Article 1(2) to relationships having comparable effects to marriage and other family relationships should be interpreted in accordance with the law of the Member State in which the court is seised.

(9) Obligations under bills of exchange, cheques and promissory notes and other negotiable instruments should

also cover bills of lading to the extent that the obligations under the bill of lading arise out of its negotiable character.

(10) Obligations arising out of dealings prior to the conclusion of the contract are covered by Article 12 of Regulation (EC) No 864/2007. Such obligations should therefore be excluded from the scope of this Regulation.

(11) The parties' freedom to choose the applicable law should be one of the cornerstones of the system of conflict-of-law rules in matters of contractual obligations.

(12) An agreement between the parties to confer on one or more courts or tribunals of a Member State exclusive jurisdiction to determine disputes under the contract should be one of the factors to be taken into account in determining whether a choice of law has been clearly demonstrated.

(13) This Regulation does not preclude parties from incorporating by reference into their contract a non-State body of law or an international convention.

(14) Should the Community adopt, in an appropriate legal instrument, rules of substantive contract law, including standard terms and conditions, such instrument may provide that the parties may choose to apply those rules.

(15) Where a choice of law is made and all other elements relevant to the situation are located in a country other than the country whose law has been chosen, the choice of law should not prejudice the application of provisions of the law of that country which cannot be derogated from by agreement. This rule should apply whether or not the choice of law was accompanied by a choice of court or tribunal. Whereas no substantial change is intended as compared with Article 3(3) of the 1980 Convention on the Law Applicable to Contractual Obligations (7) (the Rome Convention), the wording of this Regulation is aligned as far as possible with Article 14 of Regulation (EC) No 864/2007.

(16) To contribute to the general objective of this Regulation, legal certainty in the European judicial area, the conflict-of-law rules should be highly foreseeable. The courts should, however, retain a degree of discretion to determine the law that is most closely connected to the situation.

(17) As far as the applicable law in the absence of choice is concerned, the concept of 'provision of services' and 'sale of goods' should be interpreted in the same way as when applying Article 5 of Regulation (EC) No 44/2001 in so far as sale of goods and provision of services are covered by that Regulation. Although franchise and distribution contracts are contracts for services, they are the subject of specific rules.

(18) As far as the applicable law in the absence of choice is concerned, multilateral systems should be those in which trading is conducted, such as regulated markets and multilateral trading facilities as referred to in Article 4 of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments (8), regardless of whether or not they rely on a central counterparty.

(19) Where there has been no choice of law, the applicable law should be determined in accordance with the rule specified for the particular type of contract. Where the contract cannot be categorised as being one of the specified types or where its elements fall within more than one of the specified types, it should be governed by the law of the country where the party required to effect the characteristic performance of the

contract has his habitual residence. In the case of a contract consisting of a bundle of rights and obligations capable of being categorised as falling within more than one of the specified types of contract, the characteristic performance of the contract should be determined having regard to its centre of gravity.

(20) Where the contract is manifestly more closely connected with a country other than that indicated in Article 4(1) or (2), an escape clause should provide that the law of that other country is to apply. In order to determine that country, account should be taken, inter alia, of whether the contract in question has a very close relationship with another contract or contracts.

(21) In the absence of choice, where the applicable law cannot be determined either on the basis of the fact that the contract can be categorised as one of the specified types or as being the law of the country of habitual residence of the party required to effect the characteristic performance of the contract, the contract should be governed by the law of the country with which it is most closely connected. In order to determine that country, account should be taken, inter alia, of whether the contract in question has a very close relationship with another contract or contracts.

(22) As regards the interpretation of contracts for the carriage of goods, no change in substance is intended with respect to Article 4(4), third sentence, of the Rome Convention. Consequently, single-voyage charter parties and other contracts the main purpose of which is the carriage of goods should be treated as contracts for the carriage of goods. For the purposes of this Regulation, the term 'consignor' should refer to any person who enters into a contract of carriage with the carrier and the term 'the carrier' should refer to the party to the contract who undertakes to carry the goods, whether or not he performs the carriage himself.

(23) As regards contracts concluded with parties regarded as being weaker, those parties should be protected by conflict-of-law rules that are more favourable to their interests than the general rules.

(24) With more specific reference to consumer contracts, the conflict-of-law rule should make it possible to cut the cost of settling disputes concerning what are commonly relatively small claims and to take account of the development of distance-selling techniques. Consistency with Regulation (EC) No 44/2001 requires both that there be a reference to the concept of directed activity as a condition for applying the consumer protection rule and that the concept be interpreted harmoniously in Regulation (EC) No 44/2001 and this Regulation, bearing in mind that a joint declaration by the Council and the Commission on Article 15 of Regulation (EC) No 44/2001 states that 'for Article 15(1)(c) to be applicable it is not sufficient for an undertaking to target its activities at the Member State of the consumer's residence, or at a number of Member States including that Member State; a contract must also be concluded within the framework of its activities'. The declaration also states that 'the mere fact that an Internet site is accessible is not sufficient for Article 15 to be applicable, although a factor will be that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means. In this respect, the language or currency which a website uses does not constitute a relevant factor'.

(25) Consumers should be protected by such rules of the country of their habitual residence that cannot be derogated from by agreement, provided that the consumer contract has been concluded as a result of the professional pursuing his commercial or professional activities in that particular country. The same protection should be guaranteed if the professional, while not pursuing his commercial or professional activities in the country where the consumer has his habitual residence, directs his activities by any means to that country or to several countries, including that country, and the contract is concluded as a result of such activities.

(26) For the purposes of this Regulation, financial services such as investment services and activities and ancillary

services provided by a professional to a consumer, as referred to in sections A and B of Annex I to Directive 2004/39/EC, and contracts for the sale of units in collective investment undertakings, whether or not covered by Council Directive 85/611/EEC of 20 December 1985 on the coordination of laws, Regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (9), should be subject to Article 6 of this Regulation. Consequently, when a reference is made to terms and conditions governing the issuance or offer to the public of transferable securities or to the subscription and redemption of units in collective investment undertakings, that reference should include all aspects binding the issuer or the offeror to the consumer, but should not include those aspects involving the provision of financial services.

(27) Various exceptions should be made to the general conflict-of-law rule for consumer contracts. Under one such exception the general rule should not apply to contracts relating to rights in rem in immovable property or tenancies of such property unless the contract relates to the right to use immovable property on a timeshare basis within the meaning of Directive 94/47/EC of the European Parliament and of the Council of 26 October 1994 on the protection of purchasers in respect of certain aspects of contracts relating to the purchase of the right to use immovable properties on a timeshare basis (10).

(28) It is important to ensure that rights and obligations which constitute a financial instrument are not covered by the general rule applicable to consumer contracts, as that could lead to different laws being applicable to each of the instruments issued, therefore changing their nature and preventing their fungible trading and offering. Likewise, whenever such instruments are issued or offered, the contractual relationship established between the issuer or the offeror and the consumer should not necessarily be subject to the mandatory application of the law of the country of habitual residence of the consumer, as there is a need to ensure uniformity in the terms and conditions of an issuance or an offer. The same rationale should apply with regard to the multilateral systems covered by Article 4(1)(h), in respect of which it should be ensured that the law of the country of habitual residence of the consumer will not interfere with the rules applicable to contracts concluded within those systems or with the operator of such systems.

(29) For the purposes of this Regulation, references to rights and obligations constituting the terms and conditions governing the issuance, offers to the public or public take-over bids of transferable securities and references to the subscription and redemption of units in collective investment undertakings should include the terms governing, inter alia, the allocation of securities or units, rights in the event of over-subscription, withdrawal rights and similar matters in the context of the offer as well as those matters referred to in Articles 10, 11, 12 and 13, thus ensuring that all relevant contractual aspects of an offer binding the issuer or the offeror to the consumer are governed by a single law.

(30) For the purposes of this Regulation, financial instruments and transferable securities are those instruments referred to in Article 4 of Directive 2004/39/EC.

(31) Nothing in this Regulation should prejudice the operation of a formal arrangement designated as a system under Article 2(a) of Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (11).

(32) Owing to the particular nature of contracts of carriage and insurance contracts, specific provisions should ensure an adequate level of protection of passengers and policy holders. Therefore, Article 6 should not apply in the context of those particular contracts.

(33) Where an insurance contract not covering a large risk covers more than one risk, at least one of which is situated in a Member State and at least one of which is situated in a third country, the special rules on insurance contracts in this

Regulation should apply only to the risk or risks situated in the relevant Member State or Member States.

(34) The rule on individual employment contracts should not prejudice the application of the overriding mandatory provisions of the country to which a worker is posted in accordance with Directive 96/71/EC of the European Parliament and of the Council of 16 December 1996 concerning the posting of workers in the framework of the provision of services (12).

(35) Employees should not be deprived of the protection afforded to them by provisions which cannot be derogated from by agreement or which can only be derogated from to their benefit.

(36) As regards individual employment contracts, work carried out in another country should be regarded as temporary if the employee is expected to resume working in the country of origin after carrying out his tasks abroad. The conclusion of a new contract of employment with the original employer or an employer belonging to the same group of companies as the original employer should not preclude the employee from being regarded as carrying out his work in another country temporarily.

(37) Considerations of public interest justify giving the courts of the Member States the possibility, in exceptional circumstances, of applying exceptions based on public policy and overriding mandatory provisions. The concept of 'overriding mandatory provisions' should be distinguished from the expression 'provisions which cannot be derogated from by agreement' and should be construed more restrictively.

(38) In the context of voluntary assignment, the term 'relationship' should make it clear that Article 14(1) also applies to the property aspects of an assignment, as between assignor and assignee, in legal orders where such aspects are treated separately from the aspects under the law of obligations. However, the term 'relationship' should not be understood as relating to any relationship that may exist between assignor and assignee. In particular, it should not cover preliminary questions as regards a voluntary assignment or a contractual subrogation. The term should be strictly limited to the aspects which are directly relevant to the voluntary assignment or contractual subrogation in question.

(39) For the sake of legal certainty there should be a clear definition of habitual residence, in particular for companies and other bodies, corporate or unincorporated. Unlike Article 60(1) of Regulation (EC) No 44/2001, which establishes three criteria, the conflict-of-law rule should proceed on the basis of a single criterion; otherwise, the parties would be unable to foresee the law applicable to their situation.

(40) A situation where conflict-of-law rules are dispersed among several instruments and where there are differences between those rules should be avoided. This Regulation, however, should not exclude the possibility of inclusion of conflict-of-law rules relating to contractual obligations in provisions of Community law with regard to particular matters.

This Regulation should not prejudice the application of other instruments laying down provisions designed to contribute to the proper functioning of the internal market in so far as they cannot be applied in conjunction with the law designated by the rules of this Regulation. The application of provisions of the applicable law designated by the rules of this Regulation should not restrict the free movement of goods and services as regulated by Community instruments, such as Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (13).

(41) Respect for international commitments entered into by the Member States means that this Regulation should not affect international conventions to which one or more Member States are parties at the time when this Regulation is adopted. To make the rules more accessible, the Commission

should publish the list of the relevant conventions in the Official Journal of the European Union on the basis of information supplied by the Member States.

(42) The Commission will make a proposal to the European Parliament and to the Council concerning the procedures and conditions according to which Member States would be entitled to negotiate and conclude, on their own behalf, agreements with third countries in individual and exceptional cases, concerning sectoral matters and containing provisions on the law applicable to contractual obligations.

(43) Since the objective of this Regulation cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Regulation, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary to attain its objective.

(44) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland, annexed to the Treaty on European Union and to the Treaty establishing the European Community, Ireland has notified its wish to take part in the adoption and application of the present Regulation.

(45) In accordance with Articles 1 and 2 of the Protocol on the position of the United Kingdom and Ireland, annexed to the Treaty on European Union and to the Treaty establishing the European Community, and without prejudice to Article 4 of the said Protocol, the United Kingdom is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(46) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark, annexed to the Treaty on European Union and to the Treaty establishing the European Community, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

SCOPE

Article 1

Material scope

1. This Regulation shall apply, in situations involving a conflict of laws, to contractual obligations in civil and commercial matters.

It shall not apply, in particular, to revenue, customs or administrative matters.

2. The following shall be excluded from the scope of this Regulation:

(a) questions involving the status or legal capacity of natural persons, without prejudice to Article 13;

(b) obligations arising out of family relationships and relationships deemed by the law applicable to such relationships to have comparable effects, including maintenance obligations;

(c) obligations arising out of matrimonial property regimes, property regimes of relationships deemed by the law applicable to such relationships to have comparable effects to marriage, and wills and succession;

(d) obligations arising under bills of exchange, cheques and promissory notes and other negotiable instruments to the extent that the obligations under such other negotiable instruments arise out of their negotiable character;

(e) arbitration agreements and agreements on the choice of court;

(f) questions governed by the law of companies and other bodies, corporate or unincorporated, such as the creation, by registration or otherwise, legal capacity, internal organisation or winding-up of companies and other bodies, corporate or unincorporated, and the personal liability of officers and members as such for the obligations of the company or body;

(g) the question whether an agent is able to bind a principal, or an organ to bind a company or other body corporate or unincorporated, in relation to a third party;
(h) the constitution of trusts and the relationship between settlors, trustees and beneficiaries;
(i) obligations arising out of dealings prior to the conclusion of a contract;
(j) insurance contracts arising out of operations carried out by organisations other than undertakings referred to in Article 2 of Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance (14) the object of which is to provide benefits for employed or self-employed persons belonging to an undertaking or group of undertakings, or to a trade or group of trades, in the event of death or survival or of discontinuance or curtailment of activity, or of sickness related to work or accidents at work.
3. This Regulation shall not apply to evidence and procedure, without prejudice to Article 18.
4. In this Regulation, the term 'Member State' shall mean Member States to which this Regulation applies. However, in Article 3(4) and Article 7 the term shall mean all the Member States.

Article 2 Universal application

Any law specified by this Regulation shall be applied whether or not it is the law of a Member State.

CHAPTER II UNIFORM RULES

Article 3 Freedom of choice

1. A contract shall be governed by the law chosen by the parties. The choice shall be made expressly or clearly demonstrated by the terms of the contract or the circumstances of the case. By their choice the parties can select the law applicable to the whole or to part only of the contract.
2. The parties may at any time agree to subject the contract to a law other than that which previously governed it, whether as a result of an earlier choice made under this Article or of other provisions of this Regulation. Any change in the law to be applied that is made after the conclusion of the contract shall not prejudice its formal validity under Article 11 or adversely affect the rights of third parties.
3. Where all other elements relevant to the situation at the time of the choice are located in a country other than the country whose law has been chosen, the choice of the parties shall not prejudice the application of provisions of the law of that other country which cannot be derogated from by agreement.
4. Where all other elements relevant to the situation at the time of the choice are located in one or more Member States, the parties' choice of applicable law other than that of a Member State shall not prejudice the application of provisions of Community law, where appropriate as implemented in the Member State of the forum, which cannot be derogated from by agreement.
5. The existence and validity of the consent of the parties as to the choice of the applicable law shall be determined in accordance with the provisions of Articles 10, 11 and 13.

Article 4 Applicable law in the absence of choice

1. To the extent that the law applicable to the contract has not been chosen in accordance with Article 3 and without prejudice to Articles 5 to 8, the law governing the contract shall be determined as follows:
(a)

a contract for the sale of goods shall be governed by the law of the country where the seller has his habitual residence;
(b) a contract for the provision of services shall be governed by the law of the country where the service provider has his habitual residence;
(c) a contract relating to a right in rem in immovable property or to a tenancy of immovable property shall be governed by the law of the country where the property is situated;
(d) notwithstanding point (c), a tenancy of immovable property concluded for temporary private use for a period of no more than six consecutive months shall be governed by the law of the country where the landlord has his habitual residence, provided that the tenant is a natural person and has his habitual residence in the same country;
(e) a franchise contract shall be governed by the law of the country where the franchisee has his habitual residence;
(f) a distribution contract shall be governed by the law of the country where the distributor has his habitual residence;
(g) a contract for the sale of goods by auction shall be governed by the law of the country where the auction takes place, if such a place can be determined;
(h) a contract concluded within a multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments, as defined by Article 4(1), point (17) of Directive 2004/39/EC, in accordance with non-discretionary rules and governed by a single law, shall be governed by that law.
2. Where the contract is not covered by paragraph 1 or where the elements of the contract would be covered by more than one of points (a) to (h) of paragraph 1, the contract shall be governed by the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence.
3. Where it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply.
4. Where the law applicable cannot be determined pursuant to paragraphs 1 or 2, the contract shall be governed by the law of the country with which it is most closely connected.

Article 5 Contracts of carriage

1. To the extent that the law applicable to a contract for the carriage of goods has not been chosen in accordance with Article 3, the law applicable shall be the law of the country of habitual residence of the carrier, provided that the place of receipt or the place of delivery or the habitual residence of the consignor is also situated in that country. If those requirements are not met, the law of the country where the place of delivery as agreed by the parties is situated shall apply.
2. To the extent that the law applicable to a contract for the carriage of passengers has not been chosen by the parties in accordance with the second subparagraph, the law applicable shall be the law of the country where the passenger has his habitual residence, provided that either the place of departure or the place of destination is situated in that country. If these requirements are not met, the law of the country where the carrier has his habitual residence shall apply.
The parties may choose as the law applicable to a contract for the carriage of passengers in accordance with Article 3 only the law of the country where:

(a) the passenger has his habitual residence; or
(b) the carrier has his habitual residence; or

- (c) the carrier has his place of central administration; or
- (d) the place of departure is situated; or
- (e) the place of destination is situated.

3. Where it is clear from all the circumstances of the case that the contract, in the absence of a choice of law, is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply.

Article 6 Consumer contracts

1. Without prejudice to Articles 5 and 7, a contract concluded by a natural person for a purpose which can be regarded as being outside his trade or profession (the consumer) with another person acting in the exercise of his trade or profession (the professional) shall be governed by the law of the country where the consumer has his habitual residence, provided that the professional:

(a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or

(b) by any means, directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities.

2. Notwithstanding paragraph 1, the parties may choose the law applicable to a contract which fulfils the requirements of paragraph 1, in accordance with Article 3. Such a choice may not, however, have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law which, in the absence of choice, would have been applicable on the basis of paragraph 1.

3. If the requirements in points (a) or (b) of paragraph 1 are not fulfilled, the law applicable to a contract between a consumer and a professional shall be determined pursuant to Articles 3 and 4.

4. Paragraphs 1 and 2 shall not apply to:

(a) a contract for the supply of services where the services are to be supplied to the consumer exclusively in a country other than that in which he has his habitual residence;

(b) a contract of carriage other than a contract relating to package travel within the meaning of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours (15);

(c) a contract relating to a right in rem in immovable property or a tenancy of immovable property other than a contract relating to the right to use immovable properties on a timeshare basis within the meaning of Directive 94/47/EC;

(d) rights and obligations which constitute a financial instrument and rights and obligations constituting the terms and conditions governing the issuance or offer to the public and public take-over bids of transferable securities, and the subscription and redemption of units in collective investment undertakings in so far as these activities do not constitute provision of a financial service;

(e) a contract concluded within the type of system falling within the scope of Article 4(1)(h).

Article 7 Insurance contracts

1. This Article shall apply to contracts referred to in paragraph 2, whether or not the risk covered is situated in a Member State, and to all other insurance contracts covering risks situated inside the territory of the Member States. It shall not apply to reinsurance contracts.

2. An insurance contract covering a large risk as defined in Article 5(d) of the First Council Directive 73/239/EEC of 24 July 1973 on the coordination of laws, Regulations and administrative provisions relating to the taking-up and pursuit of the business of direct insurance other than life assurance (16) shall be governed by the law chosen by the parties in accordance with Article 3 of this Regulation.

To the extent that the applicable law has not been chosen by the parties, the insurance contract shall be governed by the law of the country where the insurer has his habitual residence. Where it is clear from all the circumstances of the case that the contract is manifestly more closely connected with another country, the law of that other country shall apply.

3. In the case of an insurance contract other than a contract falling within paragraph 2, only the following laws may be chosen by the parties in accordance with Article 3:

(a) the law of any Member State where the risk is situated at the time of conclusion of the contract;

(b) the law of the country where the policy holder has his habitual residence;

(c) in the case of life assurance, the law of the Member State of which the policy holder is a national;

(d) for insurance contracts covering risks limited to events occurring in one Member State other than the Member State where the risk is situated, the law of that Member State;

(e) where the policy holder of a contract falling under this paragraph pursues a commercial or industrial activity or a liberal profession and the insurance contract covers two or more risks which relate to those activities and are situated in different Member States, the law of any of the Member States concerned or the law of the country of habitual residence of the policy holder.

Where, in the cases set out in points (a), (b) or (e), the Member States referred to grant greater freedom of choice of the law applicable to the insurance contract, the parties may take advantage of that freedom.

To the extent that the law applicable has not been chosen by the parties in accordance with this paragraph, such a contract shall be governed by the law of the Member State in which the risk is situated at the time of conclusion of the contract.

4. The following additional rules shall apply to insurance contracts covering risks for which a Member State imposes an obligation to take out insurance:

(a) the insurance contract shall not satisfy the obligation to take out insurance unless it complies with the specific provisions relating to that insurance laid down by the Member State that imposes the obligation. Where the law of the Member State in which the risk is situated and the law of the Member State imposing the obligation to take out insurance contradict each other, the latter shall prevail;

(b) by way of derogation from paragraphs 2 and 3, a Member State may lay down that the insurance contract shall be governed by the law of the Member State that imposes the obligation to take out insurance.

5. For the purposes of paragraph 3, third subparagraph, and paragraph 4, where the contract covers risks situated in more than one Member State, the contract shall be considered as constituting several contracts each relating to only one Member State.

6. For the purposes of this Article, the country in which the risk is situated shall be determined in accordance with Article 2(d) of the Second Council Directive 88/357/EEC of 22 June 1988 on the coordination of laws, Regulations and administrative provisions relating to direct insurance other than life assurance and laying down provisions to facilitate the effective exercise of freedom to provide services (17) and,

in the case of life assurance, the country in which the risk is situated shall be the country of the commitment within the meaning of Article 1(1)(g) of Directive 2002/83/EC.

Article 8

Individual employment contracts

1. An individual employment contract shall be governed by the law chosen by the parties in accordance with Article 3. Such a choice of law may not, however, have the result of depriving the employee of the protection afforded to him by provisions that cannot be derogated from by agreement under the law that, in the absence of choice, would have been applicable pursuant to paragraphs 2, 3 and 4 of this Article.
2. To the extent that the law applicable to the individual employment contract has not been chosen by the parties, the contract shall be governed by the law of the country in which or, failing that, from which the employee habitually carries out his work in performance of the contract. The country where the work is habitually carried out shall not be deemed to have changed if he is temporarily employed in another country.
3. Where the law applicable cannot be determined pursuant to paragraph 2, the contract shall be governed by the law of the country where the place of business through which the employee was engaged is situated.
4. Where it appears from the circumstances as a whole that the contract is more closely connected with a country other than that indicated in paragraphs 2 or 3, the law of that other country shall apply.

Article 9

Overriding mandatory provisions

1. Overriding mandatory provisions are provisions the respect for which is regarded as crucial by a country for safeguarding its public interests, such as its political, social or economic organisation, to such an extent that they are applicable to any situation falling within their scope, irrespective of the law otherwise applicable to the contract under this Regulation.
2. Nothing in this Regulation shall restrict the application of the overriding mandatory provisions of the law of the forum.
3. Effect may be given to the overriding mandatory provisions of the law of the country where the obligations arising out of the contract have to be or have been performed, in so far as those overriding mandatory provisions render the performance of the contract unlawful. In considering whether to give effect to those provisions, regard shall be had to their nature and purpose and to the consequences of their application or non-application.

Article 10

Consent and material validity

1. The existence and validity of a contract, or of any term of a contract, shall be determined by the law which would govern it under this Regulation if the contract or term were valid.
2. Nevertheless, a party, in order to establish that he did not consent, may rely upon the law of the country in which he has his habitual residence if it appears from the circumstances that it would not be reasonable to determine the effect of his conduct in accordance with the law specified in paragraph 1.

Article 11

Formal validity

1. A contract concluded between persons who, or whose agents, are in the same country at the time of its conclusion is formally valid if it satisfies the formal requirements of the law which governs it in substance under this Regulation or of the law of the country where it is concluded.
2. A contract concluded between persons who, or whose agents, are in different countries at the time of its conclusion is formally valid if it satisfies the formal requirements of the

law which governs it in substance under this Regulation, or of the law of either of the countries where either of the parties or their agent is present at the time of conclusion, or of the law of the country where either of the parties had his habitual residence at that time.

3. A unilateral act intended to have legal effect relating to an existing or contemplated contract is formally valid if it satisfies the formal requirements of the law which governs or would govern the contract in substance under this Regulation, or of the law of the country where the act was done, or of the law of the country where the person by whom it was done had his habitual residence at that time.
4. Paragraphs 1, 2 and 3 of this Article shall not apply to contracts that fall within the scope of Article 6. The form of such contracts shall be governed by the law of the country where the consumer has his habitual residence.
5. Notwithstanding paragraphs 1 to 4, a contract the subject matter of which is a right in rem in immovable property or a tenancy of immovable property shall be subject to the requirements of form of the law of the country where the property is situated if by that law:
 - (a) those requirements are imposed irrespective of the country where the contract is concluded and irrespective of the law governing the contract; and
 - (b) those requirements cannot be derogated from by agreement.

Article 12

Scope of the law applicable

1. The law applicable to a contract by virtue of this Regulation shall govern in particular:
 - (a) interpretation;
 - (b) performance;
 - (c) within the limits of the powers conferred on the court by its procedural law, the consequences of a total or partial breach of obligations, including the assessment of damages in so far as it is governed by rules of law;
 - (d) the various ways of extinguishing obligations, and prescription and limitation of actions;
 - (e) the consequences of nullity of the contract.
2. In relation to the manner of performance and the steps to be taken in the event of defective performance, regard shall be had to the law of the country in which performance takes place.

Article 13

Incapacity

In a contract concluded between persons who are in the same country, a natural person who would have capacity under the law of that country may invoke his incapacity resulting from the law of another country, only if the other party to the contract was aware of that incapacity at the time of the conclusion of the contract or was not aware thereof as a result of negligence.

Article 14

Voluntary assignment and contractual subrogation

1. The relationship between assignor and assignee under a voluntary assignment or contractual subrogation of a claim against another person (the debtor) shall be governed by the law that applies to the contract between the assignor and assignee under this Regulation.
2. The law governing the assigned or subrogated claim shall determine its assignability, the relationship between the assignee and the debtor, the conditions under which the

assignment or subrogation can be invoked against the debtor and whether the debtor's obligations have been discharged.

3. The concept of assignment in this Article includes outright transfers of claims, transfers of claims by way of security and pledges or other security rights over claims.

Article 15

Legal subrogation

Where a person (the creditor) has a contractual claim against another (the debtor) and a third person has a duty to satisfy the creditor, or has in fact satisfied the creditor in discharge of that duty, the law which governs the third person's duty to satisfy the creditor shall determine whether and to what extent the third person is entitled to exercise against the debtor the rights which the creditor had against the debtor under the law governing their relationship.

Article 16

Multiple liability

If a creditor has a claim against several debtors who are liable for the same claim, and one of the debtors has already satisfied the claim in whole or in part, the law governing the debtor's obligation towards the creditor also governs the debtor's right to claim recourse from the other debtors. The other debtors may rely on the defences they had against the creditor to the extent allowed by the law governing their obligations towards the creditor.

Article 17

Set-off

Where the right to set-off is not agreed by the parties, set-off shall be governed by the law applicable to the claim against which the right to set-off is asserted.

Article 18

Burden of proof

1. The law governing a contractual obligation under this Regulation shall apply to the extent that, in matters of contractual obligations, it contains rules which raise presumptions of law or determine the burden of proof.

2. A contract or an act intended to have legal effect may be proved by any mode of proof recognised by the law of the forum or by any of the laws referred to in Article 11 under which that contract or act is formally valid, provided that such mode of proof can be administered by the forum.

CHAPTER III

OTHER PROVISIONS

Article 19

Habitual residence

1. For the purposes of this Regulation, the habitual residence of companies and other bodies, corporate or unincorporated, shall be the place of central administration.

The habitual residence of a natural person acting in the course of his business activity shall be his principal place of business.

2. Where the contract is concluded in the course of the operations of a branch, agency or any other establishment, or if, under the contract, performance is the responsibility of such a branch, agency or establishment, the place where the branch, agency or any other establishment is located shall be treated as the place of habitual residence.

3. For the purposes of determining the habitual residence, the relevant point in time shall be the time of the conclusion of the contract.

Article 20

Exclusion of renvoi

The application of the law of any country specified by this Regulation means the application of the rules of law in force in that country other than its rules of private international law, unless provided otherwise in this Regulation.

Article 21

Public policy of the forum

The application of a provision of the law of any country specified by this Regulation may be refused only if such application is manifestly incompatible with the public policy (ordre public) of the forum.

Article 22

States with more than one legal system

1. Where a State comprises several territorial units, each of which has its own rules of law in respect of contractual obligations, each territorial unit shall be considered as a country for the purposes of identifying the law applicable under this Regulation.

2. A Member State where different territorial units have their own rules of law in respect of contractual obligations shall not be required to apply this Regulation to conflicts solely between the laws of such units.

Article 23

Relationship with other provisions of Community law

With the exception of Article 7, this Regulation shall not prejudice the application of provisions of Community law which, in relation to particular matters, lay down conflict-of-law rules relating to contractual obligations.

Article 24

Relationship with the Rome Convention

1. This Regulation shall replace the Rome Convention in the Member States, except as regards the territories of the Member States which fall within the territorial scope of that Convention and to which this Regulation does not apply pursuant to Article 299 of the Treaty.

2. In so far as this Regulation replaces the provisions of the Rome Convention, any reference to that Convention shall be understood as a reference to this Regulation.

Article 25

Relationship with existing international conventions

1. This Regulation shall not prejudice the application of international conventions to which one or more Member States are parties at the time when this Regulation is adopted and which lay down conflict-of-law rules relating to contractual obligations.

2. However, this Regulation shall, as between Member States, take precedence over conventions concluded exclusively between two or more of them in so far as such conventions concern matters governed by this Regulation.

Article 26

List of Conventions

1. By 17 June 2009, Member States shall notify the Commission of the conventions referred to in Article 25(1). After that date, Member States shall notify the Commission of all denunciations of such conventions.

2. Within six months of receipt of the notifications referred to in paragraph 1, the Commission shall publish in the Official Journal of the European Union:

(a)

a list of the conventions referred to in paragraph 1;

(b)

the denunciations referred to in paragraph 1.

Article 27
Review clause

1. By 17 June 2013, the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee a report on the application of this Regulation. If appropriate, the report shall be accompanied by proposals to amend this Regulation. The report shall include:

- (a)
a study on the law applicable to insurance contracts and an assessment of the impact of the provisions to be introduced, if any; and
(b)
an evaluation on the application of Article 6, in particular as regards the coherence of Community law in the field of consumer protection.

2. By 17 June 2010, the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee a report on the question of the effectiveness of an assignment or subrogation of a claim against third parties and the priority of the assigned or subrogated claim over a right of another person. The report shall be accompanied, if appropriate, by a proposal to amend this Regulation and an assessment of the impact of the provisions to be introduced.

Article 28
Application in time

This Regulation shall apply to contracts concluded after 17 December 2009.

CHAPTER IV
FINAL PROVISIONS

Article 29
Entry into force and application

This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

It shall apply from 17 December 2009 except for Article 26 which shall apply from 17 June 2009.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaty establishing the European Community.

Done at Strasbourg, 17 June 2008.

For the European Parliament

The President

H.-G. PÖTTERING

For the Council

The President

J. LENARČIČ

(1) OJ C 318, 23.12.2006, p. 56.

(2) Opinion of the European Parliament of 29 November 2007 (not yet published in the Official Journal) and Council Decision of 5 June 2008.

(3) OJ C 12, 15.1.2001, p. 1.

(4) OJ C 53, 3.3.2005, p. 1.

(5) OJ L 12, 16.1.2001, p. 1. Regulation as last amended by Regulation (EC) No 1791/2006 (OJ L 363, 20.12.2006, p. 1).

(6) OJ L 199, 31.7.2007, p. 40.

(7) OJ C 334, 30.12.2005, p. 1.

(8) OJ L 145, 30.4.2004, p. 1. Directive as last amended by Directive 2008/10/EC (OJ L 76, 19.3.2008, p. 33).

(9) OJ L 375, 31.12.1985, p. 3. Directive as last amended by Directive 2008/18/EC of the European Parliament and of the Council (OJ L 76, 19.3.2008, p. 42).

(10) OJ L 280, 29.10.1994, p. 83.

(11) OJ L 166, 11.6.1998, p. 45.

(12) OJ L 18, 21.1.1997, p. 1.

(13) OJ L 178, 17.7.2000, p. 1.

(14) OJ L 345, 19.12.2002, p. 1. Directive as last amended by Directive 2008/19/EC (OJ L 76, 19.3.2008, p. 44).

(15) OJ L 158, 23.6.1990, p. 59.

(16) OJ L 228, 16.8.1973, p. 3. Directive as last amended by Directive 2005/68/EC of the European Parliament and of the Council (OJ L 323, 9.12.2005, p. 1).

(17) OJ L 172, 4.7.1988, p. 1. Directive as last amended by Directive 2005/14/EC of the European Parliament and of the Council (OJ L 149, 11.6.2005, p. 14).

Regulation (EC) No 864/2007 of the European parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 61(c) and 67 thereof,
Having regard to the proposal from the Commission,
Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the procedure laid down in Article 251 of the Treaty in the light of the joint text approved by the Conciliation Committee on 25 June 2007 (2),

Whereas:

(1) The Community has set itself the objective of maintaining and developing an area of freedom, security and justice. For the progressive establishment of such an area, the Community is to adopt measures relating to judicial cooperation in civil matters with a cross-border impact to the extent necessary for the proper functioning of the internal market.

(2) According to Article 65(b) of the Treaty, these measures are to include those promoting the compatibility of the rules applicable in the Member States concerning the conflict of laws and of jurisdiction.

(3) The European Council meeting in Tampere on 15 and 16 October 1999 endorsed the principle of mutual recognition of judgments and other decisions of judicial authorities as the cornerstone of judicial cooperation in civil matters and invited the Council and the Commission to adopt a programme of measures to implement the principle of mutual recognition.

(4) On 30 November 2000, the Council adopted a joint Commission and Council programme of measures for implementation of the principle of mutual recognition of decisions in civil and commercial matters (3). The programme identifies measures relating to the harmonisation of conflict-of-law rules as those facilitating the mutual recognition of judgments.

(5)The Hague Programme (4), adopted by the European Council on 5 November 2004, called for work to be pursued actively on the rules of conflict of laws regarding non-contractual obligations (Rome II).

(6)The proper functioning of the internal market creates a need, in order to improve the predictability of the outcome of litigation, certainty as to the law applicable and the free movement of judgments, for the conflict-of-law rules in the Member States to designate the same national law irrespective of the country of the court in which an action is brought.

(7)The substantive scope and the provisions of this Regulation should be consistent with Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (5) (Brussels I) and the instruments dealing with the law applicable to contractual obligations.

(8)This Regulation should apply irrespective of the nature of the court or tribunal seised.

(9)Claims arising out of *acta iure imperii* should include claims against officials who act on behalf of the State and liability for acts of public authorities, including liability of publicly appointed office-holders. Therefore, these matters should be excluded from the scope of this Regulation.

(10)Family relationships should cover parentage, marriage, affinity and collateral relatives. The reference in Article 1(2) to relationships having comparable effects to marriage and other family relationships should be interpreted in accordance with the law of the Member State in which the court is seised.

(11)The concept of a non-contractual obligation varies from one Member State to another. Therefore for the purposes of this Regulation non-contractual obligation should be understood as an autonomous concept. The conflict-of-law rules set out in this Regulation should also cover non-contractual obligations arising out of strict liability.

(12)The law applicable should also govern the question of the capacity to incur liability in tort/delict.

(13)Uniform rules applied irrespective of the law they designate may avert the risk of distortions of competition between Community litigants.

(14)The requirement of legal certainty and the need to do justice in individual cases are essential elements of an area of justice. This Regulation provides for the connecting factors which are the most appropriate to achieve these objectives. Therefore, this Regulation provides for a general rule but also for specific rules and, in certain provisions, for an 'escape clause' which allows a departure from these rules where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with another country. This set of rules thus creates a flexible framework of conflict-of-law rules. Equally, it enables the court seised to treat individual cases in an appropriate manner.

(15)The principle of the *lex loci delicti commissi* is the basic solution for non-contractual obligations in virtually all the Member States, but the practical application of the principle where the component factors of the case are spread over several countries varies. This situation engenders uncertainty as to the law applicable.

(16)Uniform rules should enhance the foreseeability of court decisions and ensure a reasonable balance between the interests of the person claimed to be liable and the person who has sustained damage. A connection with the country where the direct damage occurred (*lex loci damni*) strikes a fair balance between the interests of the person claimed to be liable and the person sustaining the damage, and also reflects the modern approach to civil liability and the development of systems of strict liability.

(17)The law applicable should be determined on the basis of where the damage occurs, regardless of the country or countries in which the indirect consequences could occur. Accordingly, in cases of personal injury or damage to property, the country in which the damage occurs should be

the country where the injury was sustained or the property was damaged respectively.

(18)The general rule in this Regulation should be the *lex loci damni* provided for in Article 4(1). Article 4(2) should be seen as an exception to this general principle, creating a special connection where the parties have their habitual residence in the same country. Article 4(3) should be understood as an 'escape clause' from Article 4(1) and (2), where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with another country.

(19)Specific rules should be laid down for special torts/delicts where the general rule does not allow a reasonable balance to be struck between the interests at stake.

(20)The conflict-of-law rule in matters of product liability should meet the objectives of fairly spreading the risks inherent in a modern high-technology society, protecting consumers' health, stimulating innovation, securing undistorted competition and facilitating trade. Creation of a cascade system of connecting factors, together with a foreseeability clause, is a balanced solution in regard to these objectives. The first element to be taken into account is the law of the country in which the person sustaining the damage had his or her habitual residence when the damage occurred, if the product was marketed in that country. The other elements of the cascade are triggered if the product was not marketed in that country, without prejudice to Article 4(2) and to the possibility of a manifestly closer connection to another country.

(21)The special rule in Article 6 is not an exception to the general rule in Article 4(1) but rather a clarification of it. In matters of unfair competition, the conflict-of-law rule should protect competitors, consumers and the general public and ensure that the market economy functions properly. The connection to the law of the country where competitive relations or the collective interests of consumers are, or are likely to be, affected generally satisfies these objectives.

(22)The non-contractual obligations arising out of restrictions of competition in Article 6(3) should cover infringements of both national and Community competition law. The law applicable to such non-contractual obligations should be the law of the country where the market is, or is likely to be, affected. In cases where the market is, or is likely to be, affected in more than one country, the claimant should be able in certain circumstances to choose to base his or her claim on the law of the court seised.

(23)For the purposes of this Regulation, the concept of restriction of competition should cover prohibitions on agreements between undertakings, decisions by associations of undertakings and concerted practices which have as their object or effect the prevention, restriction or distortion of competition within a Member State or within the internal market, as well as prohibitions on the abuse of a dominant position within a Member State or within the internal market, where such agreements, decisions, concerted practices or abuses are prohibited by Articles 81 and 82 of the Treaty or by the law of a Member State.

(24)'Environmental damage' should be understood as meaning adverse change in a natural resource, such as water, land or air, impairment of a function performed by that resource for the benefit of another natural resource or the public, or impairment of the variability among living organisms.

(25)Regarding environmental damage, Article 174 of the Treaty, which provides that there should be a high level of protection based on the precautionary principle and the principle that preventive action should be taken, the principle of priority for corrective action at source and the principle that the polluter pays, fully justifies the use of the principle of discriminating in favour of the person sustaining the damage. The question of when the person seeking compensation can make the choice of the law applicable should be determined in accordance with the law of the Member State in which the court is seised.

(26) Regarding infringements of intellectual property rights, the universally acknowledged principle of the *lex loci protectionis* should be preserved. For the purposes of this Regulation, the term 'intellectual property rights' should be interpreted as meaning, for instance, copyright, related rights, the *sui generis* right for the protection of databases and industrial property rights.

(27) The exact concept of industrial action, such as strike action or lock-out, varies from one Member State to another and is governed by each Member State's internal rules. Therefore, this Regulation assumes as a general principle that the law of the country where the industrial action was taken should apply, with the aim of protecting the rights and obligations of workers and employers.

(28) The special rule on industrial action in Article 9 is without prejudice to the conditions relating to the exercise of such action in accordance with national law and without prejudice to the legal status of trade unions or of the representative organisations of workers as provided for in the law of the Member States.

(29) Provision should be made for special rules where damage is caused by an act other than a tort/delict, such as unjust enrichment, *negotiorum gestio* and *culpa in contrahendo*.

(30) *Culpa in contrahendo* for the purposes of this Regulation is an autonomous concept and should not necessarily be interpreted within the meaning of national law. It should include the violation of the duty of disclosure and the breakdown of contractual negotiations. Article 12 covers only non-contractual obligations presenting a direct link with the dealings prior to the conclusion of a contract. This means that if, while a contract is being negotiated, a person suffers personal injury, Article 4 or other relevant provisions of this Regulation should apply.

(31) To respect the principle of party autonomy and to enhance legal certainty, the parties should be allowed to make a choice as to the law applicable to a non-contractual obligation. This choice should be expressed or demonstrated with reasonable certainty by the circumstances of the case. Where establishing the existence of the agreement, the court has to respect the intentions of the parties. Protection should be given to weaker parties by imposing certain conditions on the choice.

(32) Considerations of public interest justify giving the courts of the Member States the possibility, in exceptional circumstances, of applying exceptions based on public policy and overriding mandatory provisions. In particular, the application of a provision of the law designated by this Regulation which would have the effect of causing non-compensatory exemplary or punitive damages of an excessive nature to be awarded may, depending on the circumstances of the case and the legal order of the Member State of the court seised, be regarded as being contrary to the public policy (*ordre public*) of the forum.

(33) According to the current national rules on compensation awarded to victims of road traffic accidents, when quantifying damages for personal injury in cases in which the accident takes place in a State other than that of the habitual residence of the victim, the court seised should take into account all the relevant actual circumstances of the specific victim, including in particular the actual losses and costs of after-care and medical attention.

(34) In order to strike a reasonable balance between the parties, account must be taken, in so far as appropriate, of the rules of safety and conduct in operation in the country in which the harmful act was committed, even where the non-contractual obligation is governed by the law of another country. The term 'rules of safety and conduct' should be interpreted as referring to all Regulations having any relation to safety and conduct, including, for example, road safety rules in the case of an accident.

(35) A situation where conflict-of-law rules are dispersed among several instruments and where there are differences between those rules should be avoided. This Regulation, however, does not exclude the possibility of inclusion of

conflict-of-law rules relating to non-contractual obligations in provisions of Community law with regard to particular matters.

This Regulation should not prejudice the application of other instruments laying down provisions designed to contribute to the proper functioning of the internal market in so far as they cannot be applied in conjunction with the law designated by the rules of this Regulation. The application of provisions of the applicable law designated by the rules of this Regulation should not restrict the free movement of goods and services as regulated by Community instruments, such as Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (6).

(36) Respect for international commitments entered into by the Member States means that this Regulation should not affect international conventions to which one or more Member States are parties at the time this Regulation is adopted. To make the rules more accessible, the Commission should publish the list of the relevant conventions in the Official Journal of the European Union on the basis of information supplied by the Member States.

(37) The Commission will make a proposal to the European Parliament and the Council concerning the procedures and conditions according to which Member States would be entitled to negotiate and conclude on their own behalf agreements with third countries in individual and exceptional cases, concerning sectoral matters, containing provisions on the law applicable to non-contractual obligations.

(38) Since the objective of this Regulation cannot be sufficiently achieved by the Member States, and can therefore, by reason of the scale and effects of this Regulation, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity set out in Article 5 of the Treaty. In accordance with the principle of proportionality set out in that Article, this Regulation does not go beyond what is necessary to attain that objective.

(39) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on European Union and to the Treaty establishing the European Community, the United Kingdom and Ireland are taking part in the adoption and application of this Regulation.

(40) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark, annexed to the Treaty on European Union and to the Treaty establishing the European Community, Denmark does not take part in the adoption of this Regulation, and is not bound by it or subject to its application,

HAVE ADOPTED THIS REGULATION:

CHAPTER I
SCOPE

Article 1
Scope

1. This Regulation shall apply, in situations involving a conflict of laws, to non-contractual obligations in civil and commercial matters. It shall not apply, in particular, to revenue, customs or administrative matters or to the liability of the State for acts and omissions in the exercise of State authority (*acta iure imperii*).

2. The following shall be excluded from the scope of this Regulation:

(a) non-contractual obligations arising out of family relationships and relationships deemed by the law applicable to such relationships to have comparable effects including maintenance obligations;

(b) non-contractual obligations arising out of matrimonial property regimes, property regimes of relationships deemed by the law applicable to such relationships to have comparable effects to marriage, and wills and succession;

(c) non-contractual obligations arising under bills of exchange, cheques and promissory notes and other negotiable instruments to the extent that the obligations under such other negotiable instruments arise out of their negotiable character;

(d) non-contractual obligations arising out of the law of companies and other bodies corporate or unincorporated regarding matters such as the creation, by registration or otherwise, legal capacity, internal organisation or winding-up of companies and other bodies corporate or unincorporated, the personal liability of officers and members as such for the obligations of the company or body and the personal liability of auditors to a company or to its members in the statutory audits of accounting documents;

(e) non-contractual obligations arising out of the relations between the settlors, trustees and beneficiaries of a trust created voluntarily;

(f) non-contractual obligations arising out of nuclear damage;

(g) non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation.

3. This Regulation shall not apply to evidence and procedure, without prejudice to Articles 21 and 22.

4. For the purposes of this Regulation, 'Member State' shall mean any Member State other than Denmark.

Article 2

Non-contractual obligations

1. For the purposes of this Regulation, damage shall cover any consequence arising out of tort/delict, unjust enrichment, negotiorum gestio or culpa in contrahendo.

2. This Regulation shall apply also to non-contractual obligations that are likely to arise.

3. Any reference in this Regulation to:

(a) an event giving rise to damage shall include events giving rise to damage that are likely to occur; and

(b) damage shall include damage that is likely to occur.

Article 3

Universal application

Any law specified by this Regulation shall be applied whether or not it is the law of a Member State.

CHAPTER II

TORTS/DELICTS

Article 4

General rule

1. Unless otherwise provided for in this Regulation, the law applicable to a non-contractual obligation arising out of a tort/delict shall be the law of the country in which the damage occurs irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur.

2. However, where the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply.

3. Where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question.

Article 5

Product liability

1. Without prejudice to Article 4(2), the law applicable to a non-contractual obligation arising out of damage caused by a product shall be:

(a) the law of the country in which the person sustaining the damage had his or her habitual residence when the damage occurred, if the product was marketed in that country; or, failing that,

(b) the law of the country in which the product was acquired, if the product was marketed in that country; or, failing that,

(c) the law of the country in which the damage occurred, if the product was marketed in that country.

However, the law applicable shall be the law of the country in which the person claimed to be liable is habitually resident if he or she could not reasonably foresee the marketing of the product, or a product of the same type, in the country the law of which is applicable under (a), (b) or (c).

2. Where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in paragraph 1, the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question.

Article 6

Unfair competition and acts restricting free competition

1. The law applicable to a non-contractual obligation arising out of an act of unfair competition shall be the law of the country where competitive relations or the collective interests of consumers are, or are likely to be, affected.

2. Where an act of unfair competition affects exclusively the interests of a specific competitor, Article 4 shall apply.

3.

(a) The law applicable to a non-contractual obligation arising out of a restriction of competition shall be the law of the country where the market is, or is likely to be, affected.

(b) When the market is, or is likely to be, affected in more than one country, the person seeking compensation for damage who sues in the court of the domicile of the defendant, may instead choose to base his or her claim on the law of the court seised, provided that the market in that Member State is amongst those directly and substantially affected by the restriction of competition out of which the non-contractual obligation on which the claim is based arises; where the claimant sues, in accordance with the applicable rules on jurisdiction, more than one defendant in that court, he or she can only choose to base his or her claim on the law of that court if the restriction of competition on which the claim against each of these defendants relies directly and substantially affects also the market in the Member State of that court.

4. The law applicable under this Article may not be derogated from by an agreement pursuant to Article 14.

Article 7

Environmental damage

The law applicable to a non-contractual obligation arising out of environmental damage or damage sustained by persons or property as a result of such damage shall be the law determined pursuant to Article 4(1), unless the person seeking compensation for damage chooses to base his or her claim on the law of the country in which the event giving rise to the damage occurred.

Article 8

Infringement of intellectual property rights

1. The law applicable to a non-contractual obligation arising from an infringement of an intellectual property right shall be the law of the country for which protection is claimed.

2. In the case of a non-contractual obligation arising from an infringement of a unitary Community intellectual property

right, the law applicable shall, for any question that is not governed by the relevant Community instrument, be the law of the country in which the act of infringement was committed.

3. The law applicable under this Article may not be derogated from by an agreement pursuant to Article 14.

Article 9 Industrial action

Without prejudice to Article 4(2), the law applicable to a non-contractual obligation in respect of the liability of a person in the capacity of a worker or an employer or the organisations representing their professional interests for damages caused by an industrial action, pending or carried out, shall be the law of the country where the action is to be, or has been, taken.

CHAPTER III UNJUST ENRICHMENT, NEGOTIORUM GESTIO AND CULPA IN CONTRAHENDO

Article 10 Unjust enrichment

1. If a non-contractual obligation arising out of unjust enrichment, including payment of amounts wrongly received, concerns a relationship existing between the parties, such as one arising out of a contract or a tort/delict, that is closely connected with that unjust enrichment, it shall be governed by the law that governs that relationship.

2. Where the law applicable cannot be determined on the basis of paragraph 1 and the parties have their habitual residence in the same country when the event giving rise to unjust enrichment occurs, the law of that country shall apply.

3. Where the law applicable cannot be determined on the basis of paragraphs 1 or 2, it shall be the law of the country in which the unjust enrichment took place.

4. Where it is clear from all the circumstances of the case that the non-contractual obligation arising out of unjust enrichment is manifestly more closely connected with a country other than that indicated in paragraphs 1, 2 and 3, the law of that other country shall apply.

Article 11 Negotiorum gestio

1. If a non-contractual obligation arising out of an act performed without due authority in connection with the affairs of another person concerns a relationship existing between the parties, such as one arising out of a contract or a tort/delict, that is closely connected with that non-contractual obligation, it shall be governed by the law that governs that relationship.

2. Where the law applicable cannot be determined on the basis of paragraph 1, and the parties have their habitual residence in the same country when the event giving rise to the damage occurs, the law of that country shall apply.

3. Where the law applicable cannot be determined on the basis of paragraphs 1 or 2, it shall be the law of the country in which the act was performed.

4. Where it is clear from all the circumstances of the case that the non-contractual obligation arising out of an act performed without due authority in connection with the affairs of another person is manifestly more closely connected with a country other than that indicated in paragraphs 1, 2 and 3, the law of that other country shall apply.

Article 12 Culpa in contrahendo

1. The law applicable to a non-contractual obligation arising out of dealings prior to the conclusion of a contract, regardless of whether the contract was actually concluded or not, shall

be the law that applies to the contract or that would have been applicable to it had it been entered into.

2. Where the law applicable cannot be determined on the basis of paragraph 1, it shall be:

(a) the law of the country in which the damage occurs, irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occurred; or

(b) where the parties have their habitual residence in the same country at the time when the event giving rise to the damage occurs, the law of that country; or

(c) where it is clear from all the circumstances of the case that the non-contractual obligation arising out of dealings prior to the conclusion of a contract is manifestly more closely connected with a country other than that indicated in points (a) and (b), the law of that other country.

Article 13 Applicability of Article 8

For the purposes of this Chapter, Article 8 shall apply to non-contractual obligations arising from an infringement of an intellectual property right.

CHAPTER IV FREEDOM OF CHOICE

Article 14 Freedom of choice

1. The parties may agree to submit non-contractual obligations to the law of their choice:

(a) by an agreement entered into after the event giving rise to the damage occurred;

or

(b) where all the parties are pursuing a commercial activity, also by an agreement freely negotiated before the event giving rise to the damage occurred.

The choice shall be expressed or demonstrated with reasonable certainty by the circumstances of the case and shall not prejudice the rights of third parties.

2. Where all the elements relevant to the situation at the time when the event giving rise to the damage occurs are located in a country other than the country whose law has been chosen, the choice of the parties shall not prejudice the application of provisions of the law of that other country which cannot be derogated from by agreement.

3. Where all the elements relevant to the situation at the time when the event giving rise to the damage occurs are located in one or more of the Member States, the parties' choice of the law applicable other than that of a Member State shall not prejudice the application of provisions of Community law, where appropriate as implemented in the Member State of the forum, which cannot be derogated from by agreement.

CHAPTER V COMMON RULES

Article 15 Scope of the law applicable

The law applicable to non-contractual obligations under this Regulation shall govern in particular:

(a) the basis and extent of liability, including the determination of persons who may be held liable for acts performed by them;

(b) the grounds for exemption from liability, any limitation of liability and any division of liability;

(c) the existence, the nature and the assessment of damage or the remedy claimed;

(d) within the limits of powers conferred on the court by its procedural law, the measures which a court may take to prevent or terminate injury or damage or to ensure the provision of compensation;

(e) the question whether a right to claim damages or a remedy may be transferred, including by inheritance;
(f) persons entitled to compensation for damage sustained personally;
(g) liability for the acts of another person;
(h) the manner in which an obligation may be extinguished and rules of prescription and limitation, including rules relating to the commencement, interruption and suspension of a period of prescription or limitation.

Article 16

Overriding mandatory provisions

Nothing in this Regulation shall restrict the application of the provisions of the law of the forum in a situation where they are mandatory irrespective of the law otherwise applicable to the non-contractual obligation.

Article 17

Rules of safety and conduct

In assessing the conduct of the person claimed to be liable, account shall be taken, as a matter of fact and in so far as is appropriate, of the rules of safety and conduct which were in force at the place and time of the event giving rise to the liability.

Article 18

Direct action against the insurer of the person liable

The person having suffered damage may bring his or her claim directly against the insurer of the person liable to provide compensation if the law applicable to the non-contractual obligation or the law applicable to the insurance contract so provides.

Article 19

Subrogation

Where a person (the creditor) has a non-contractual claim upon another (the debtor), and a third person has a duty to satisfy the creditor, or has in fact satisfied the creditor in discharge of that duty, the law which governs the third person's duty to satisfy the creditor shall determine whether, and the extent to which, the third person is entitled to exercise against the debtor the rights which the creditor had against the debtor under the law governing their relationship.

Article 20

Multiple liability

If a creditor has a claim against several debtors who are liable for the same claim, and one of the debtors has already satisfied the claim in whole or in part, the question of that debtor's right to demand compensation from the other debtors shall be governed by the law applicable to that debtor's non-contractual obligation towards the creditor.

Article 21

Formal validity

A unilateral act intended to have legal effect and relating to a non-contractual obligation shall be formally valid if it satisfies the formal requirements of the law governing the non-contractual obligation in question or the law of the country in which the act is performed.

Article 22

Burden of proof

1. The law governing a non-contractual obligation under this Regulation shall apply to the extent that, in matters of non-contractual obligations, it contains rules which raise presumptions of law or determine the burden of proof.

2. Acts intended to have legal effect may be proved by any mode of proof recognised by the law of the forum or by any of the laws referred to in Article 21 under which that act is formally valid, provided that such mode of proof can be administered by the forum.

CHAPTER VI

OTHER PROVISIONS

Article 23

Habitual residence

1. For the purposes of this Regulation, the habitual residence of companies and other bodies, corporate or unincorporated, shall be the place of central administration.

Where the event giving rise to the damage occurs, or the damage arises, in the course of operation of a branch, agency or any other establishment, the place where the branch, agency or any other establishment is located shall be treated as the place of habitual residence.

2. For the purposes of this Regulation, the habitual residence of a natural person acting in the course of his or her business activity shall be his or her principal place of business.

Article 24

Exclusion of renvoi

The application of the law of any country specified by this Regulation means the application of the rules of law in force in that country other than its rules of private international law.

Article 25

States with more than one legal system

1. Where a State comprises several territorial units, each of which has its own rules of law in respect of non-contractual obligations, each territorial unit shall be considered as a country for the purposes of identifying the law applicable under this Regulation.

2. A Member State within which different territorial units have their own rules of law in respect of non-contractual obligations shall not be required to apply this Regulation to conflicts solely between the laws of such units.

Article 26

Public policy of the forum

The application of a provision of the law of any country specified by this Regulation may be refused only if such application is manifestly incompatible with the public policy (ordre public) of the forum.

Article 27

Relationship with other provisions of Community law

This Regulation shall not prejudice the application of provisions of Community law which, in relation to particular matters, lay down conflict-of-law rules relating to non-contractual obligations.

Article 28

Relationship with existing international conventions

1. This Regulation shall not prejudice the application of international conventions to which one or more Member States are parties at the time when this Regulation is adopted and which lay down conflict-of-law rules relating to non-contractual obligations.

2. However, this Regulation shall, as between Member States, take precedence over conventions concluded exclusively between two or more of them in so far as such conventions concern matters governed by this Regulation.

CHAPTER VII

FINAL PROVISIONS

Article 29
List of conventions

1. By 11 July 2008, Member States shall notify the Commission of the conventions referred to in Article 28(1). After that date, Member States shall notify the Commission of all denunciations of such conventions.
2. The Commission shall publish in the Official Journal of the European Union within six months of receipt:
 - (i) a list of the conventions referred to in paragraph 1;
 - (ii) the denunciations referred to in paragraph 1.

Article 30

Review clause

1. Not later than 20 August 2011, the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee a report on the application of this Regulation. If necessary, the report shall be accompanied by proposals to adapt this Regulation. The report shall include:
 - (i) a study on the effects of the way in which foreign law is treated in the different jurisdictions and on the extent to which courts in the Member States apply foreign law in practice pursuant to this Regulation;
 - (ii) a study on the effects of Article 28 of this Regulation with respect to the Hague Convention of 4 May 1971 on the law applicable to traffic accidents.
2. Not later than 31 December 2008, the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee a study on the situation in the field of the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality, taking into account rules relating to freedom of the press and freedom of expression in the media, and conflict-of-law issues related to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (7).

Article 31
Application in time

This Regulation shall apply to events giving rise to damage which occur after its entry into force.

Article 32
Date of application

This Regulation shall apply from 11 January 2009, except for Article 29, which shall apply from 11 July 2008.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaty establishing the European Community.

Done at Strasbourg, 11 July 2007.

For the European Parliament

The President

H.-G. PÖTTERING

For the Council

The President

M. LOBO ANTUNES

(1) OJ C 241, 28.9.2004, p. 1.

(2) Opinion of the European Parliament of 6 July 2005 (OJ C 157 E, 6.7.2006, p. 371), Council Common Position of 25 September 2006 (OJ C 289 E, 28.11.2006, p. 68) and Position of the European Parliament of 18 January 2007 (not yet published in the Official Journal). European Parliament Legislative Resolution of 10 July 2007 and Council Decision of 28 June 2007.

(3) OJ C 12, 15.1.2001, p. 1.

(4) OJ C 53, 3.3.2005, p. 1.

(5) OJ L 12, 16.1.2001, p. 1. Regulation as last amended by Regulation (EC) No 1791/2006 (OJ L 363, 20.12.2006, p. 1).

(6) OJ L 178, 17.7.2000, p. 1.

(7) OJ L 281, 23.11.1995, p. 31.

Commission Statement on the review clause (Article 30)

The Commission, following the invitation by the European Parliament and the Council in the frame of Article 30 of the 'Rome II' Regulation, will submit, not later than December 2008, a study on the situation in the field of the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality. The Commission will take into consideration all aspects of the situation and take appropriate measures if necessary.