EUROPEAN COMMISSION

Brussels, 25.1.2012
SEC(2012) 73 final

COMMISSION STAFF WORKING PAPER

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
and
Directive of the European Parliament and of the Council on the protection of individuals 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

{COM(2012) 10 final}
{COM(2012) 11 final}
{SEC(2012) 72 final}

COMMISSION STAFF WORKING PAPER

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
and
Directive of the European Parliament and of the Council on the protection of individuals 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

1. INTRODUCTION

Since the adoption of the current EU legal framework on data protection in 1995, rapid technological and business developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally, without being fully aware of the risks involved.

Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services, including public e-government services. If not addressed, this lack of confidence will continue to slow down the development of innovative uses of new technologies, to act as an obstacle to economic growth and to block the public sector from reaping the potential benefits of digitisation of its services.

Moreover, the Lisbon Treaty has created, with Article 16 TFEU, a new legal basis for a modernised and comprehensive approach to data protection and the free movement of personal data, also covering police and judicial cooperation in criminal matters.

2. PROBLEM DEFINITION

The impact assessment presents and analyses three main problem areas:

2.1. Problem 1: Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement

Despite the Directive's objective to ensure an equivalent level of data protection within the EU, there is still considerable divergence in the rules across Member States. As a consequence, data controllers may have to deal with 27 different national laws and requirements within the EU. The result is a fragmented legal environment which has created legal uncertainty and unequal protection for individuals. This has caused unnecessary costs

and **administrative burdens** (amounting to **about € 3 billion per annum** in the baseline scenario) for businesses and constitutes a disincentive for enterprises, including SMES, operating in the single market who may wish to expand their operations cross-border.

Furthermore, the resources and powers of the national authorities responsible for data protection vary considerably between Member States. In some cases this means that they are unable to perform their enforcement tasks satisfactorily. Cooperation between these authorities at European level – via the existing Advisory Group (the Article 29 Working Party) – does not always lead to consistent enforcement and therefore also needs to be improved.

2.2. Problem 2: Difficulties for individuals to stay in control of their personal data

Given the lack of harmonisation in national legislations on data protection and the divergent powers of national data protection authorities, it is more difficult for individuals to exercise their rights in some Member States than in others, especially in online contexts.

Individuals have also lost control over their own data, due to the sheer volume of data being shared every day, and the fact that they are often not fully aware of their data being collected. Although many Europeans consider that the disclosure of personal data is increasingly a part of modern life[1], 72% of internet users in Europe still worry that they are asked for too much personal data online, and they often do not know how to exercise their rights online.

2.3. Problem 3: Gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in criminal matters

The scope of the Directive, based on an internal market legal basis, specifically excluded police and judicial cooperation in criminal matters. The Framework Decision adopted in 2008 to regulate data processing in the area of police cooperation and judicial cooperation in criminal matters reflects the specificities of the pre-Lisbon "pillar" structure of the EU and is characterised by **a limited scope and various other gaps,** often leading to legal uncertainty for individuals and law enforcement authorities, as well as to practical difficulties of implementation. Moreover, the Framework Decision provides for wide possibilities of derogating to general data protection principles at national level, thereby not harmonising them. This does not only risk emptying such principles of their very purpose – and thus negatively affecting the fundamental right of individuals to the protection of their personal data in this area - but also hinders the smooth exchange of personal data between relevant national authorities.

3. ANALYSIS OF SUBSIDIARITY AND PROPORTIONALITY

In light of the problems outlined above, the analysis of subsidiarity indicates the necessity of EU-level action on the following grounds:

- The right to the protection of personal data is enshrined in Article 8 of the Charter of Fundamental Rights. Article 16 TFEU is the legal basis for the adoption of EU rules on data protection ;
- Personal data can be transferred across national boundaries, both EU-internal borders and to third countries, at rapidly increasing rates. In addition, there are practical challenges to

[1] See Special Eurobarometer 359 – *Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011, p. 23.

enforcing data protection legislation and a need for cooperation between Member States and their authorities, which need to be organised at EU level to ensure the necessary coherence and a high level of protection within the Union;

- Member States cannot alone reduce the problems in the current situation. This is particularly the case for those problems that arise from the fragmentation in national legislations implementing the EU data protection regulatory framework;
- Whilst it would be possible for Member States to enact policies which ensure that this right is not breached, this would not be achieved in a uniform way in the absence of common EU rules and would create restrictions on cross-border flows of personal data.

The **envisaged actions are proportionate** as they are within the scope of the Union competences as defined by the Treaties and are necessary to ensure uniformity of application of EU legislation, ensuring effective and equal protection of individuals' fundamental rights. Action at EU level is essential to continue ensuring credibility and a high level of data protection in a globalised world, while maintaining the free flow of data. The proper functioning of the internal market requires that the provisions ensure a level playing field for economic operators.

4. OBJECTIVES

The three main **policy objectives** are:

- to **enhance the internal market dimension of data protection**, by reducing fragmentation, strengthening consistency and **simplifying** the regulatory environment, thus eliminating unnecessary costs and **reducing administrative burden**;
- to **increase the effectiveness of the fundamental right to data protection and put individuals in control of their data**;
- to **enhance the coherence of the EU data protection framework**, including in the field of police cooperation and judicial cooperation in criminal matters, taking full account of the entry into force of the Lisbon Treaty.

5. POLICY OPTIONS

5.1. Option 1: Soft action

This option would mainly consist of **interpretative Communications by the Commission, technical support tools and funding** – as well as **encouraging standardisation and self-regulation** – to strengthen practical implementation of existing rules by data controllers and raise individuals' awareness. The Commission would propose **only very limited legislative amendments** to clarify existing concepts of the Directive and target specific issues that cannot be addressed effectively in any other way. This policy option would only be relevant for problems 1 and 2.

The limited legislative changes would explicitly introduce the principles of transparency and data minimisation, as well as a legal basis for "Binding Corporate Rules" for international transfers.

5.2. Option 2: Modernised legal framework

The Commission would present **legislative proposals to further harmonise substantive rules**, clarify specific provisions, and address inconsistencies caused by differing approaches in Member States. These proposals would address problems 1 and 2 as they would, on the one hand, **facilitate data flows within the EU and from the EU to third countries** and, on the other hand, **clarify and strengthen individuals' rights** (e.g. right of access, "right to be forgotten", clearer modalities for consent and for notification of data breaches) **and reinforce responsibility – and "accountability" - of data controllers and processors** (e.g. by introducing, where appropriate, the obligation to appoint Data Protection Officers - DPOs or to carry out Data Protection Impact Assessment – DPIAs**)**. This option would set, in particular, a **"one stop shop"** for data controllers (i.e. one single law and one single DPA responsible). General notification requirements would be simplified (i.e. "basic registration"). It would also **reinforce DPAs independence and harmonise their powers.** Cooperation and mutual asssistance between DPAs would be strengthened, including via a new **"consistency mechanism"** involving both a - newly established – "European Data Protection Board" and the Commission.

As regards data protection in the area of police and judicial cooperation in criminal matters (problem 3), the Commission would present proposals to replace the Framework Decision with a **new instrument with extended scope** and would address **the most important gaps and shortcomings**, in order to both strengthen individuals' rights and facilitate cooperation between law enforcement authorities, while taking into account the specificities of the law enforcement sector.

5.3. Option 3: Detailed legal rules at EU level

This option would include most elements of Option 2 as well as **much more detailed EU legislation,** including sectoral one (e.g. in the health and medical sector), and a **centralised EU-level enforcement structure (**i.e. the setting up of an EU Data Protection Authority). It would also involve the elimination of general notification requirements (except for prior checking of risky processing), the setting up of an EU-wide certification scheme for data protection-compliant processes and products and the definition of harmonised EU-wide criminal sanctions for breaches of data protection rules. Consent would be defined as the "primary ground" for data processing.

Regarding police and judicial cooperation in criminal matters, in addition to the substantive measures under option 2, it would include the establishment of detailed rules for individuals' right of access (always direct). It would also involve **amending the relevant provisions of all existing ex-third pillar instruments**, to align them entirely with the new and extended harmonised rules.

6. ASSESSMENT OF IMPACTS

6.1. Policy Option 1: Soft action

Interpretative Commission Communications regarding provisions of the Directive would not be binding and therefore have **only limited impact on reducing legal uncertainty and costs**. More self-regulation at EU level could help to provide more legal clarity for data controllers

in specific sectors, but **would not be sufficient** to ensure effective and consistent application of the rules in the absence of an underlying clear and harmonised EU legal framework.

Awareness campaigns would help individuals to know better their data protection rights and to better understand practical ways to exercise them. This would however be **insufficient** for individuals to ascertain their rights where such rights are not clearly defined in the law. **Legislative clarifications** regarding the principles of transparency, data minimisation**,** adequacy and BCRs would increase harmonisation and legal certainty for individuals and businesses.

Regarding enforcement, Commission Communications would not overcome Member States' reluctance to change national rules to give greater independence and harmonised powers to DPAs. Enhanced coordination by WP29 and exchanges between DPAs would have a positive impact on more consistent enforcement of the rules; however, the **continuing divergences in national laws and their interpretation would limit the effect of improved cooperation between DPAs**.

The expected **financial and economic impacts of this policy option are limited** and the identified problems would largely remain unresolved.

6.2. Policy Option 2: Modernised legal framework

Legal uncertainty for private companies and public authorities **will be significantly reduced**. Problematic provisions will be clarified and consistency increased due to the reduced margin of interpretation, and implementing measures and/or delegated acts adopted by the Commission.

Replacing the general notification of data processing activities by a simplified **harmonised 'registration' system**, while keeping prior checks for sensitive data and risky processing, will relieve data controllers from an obligation currently implemented in a diverging manner. Strengthening data controllers' and data processors' responsibility by introducing – in certain cases and with clearly defined and targeted thresholds - DPOs and DPIAs and introducing the principle of data protection by design will offer easier ways to ensure and demonstrate compliance.

Clarifying and simplifying rules by defining one single law applicable throughout the EU and setting up a "one-stop shop" for data protection supervision will strengthen the internal market including by removing differences in DPAs' administrative formalities. This will allow for **an overall saving**, purely in terms of administrative burden, of about **€ 2.3 billion** per year.

Consistency of enforcement will also be fostered by reinforcing and harmonising DPAs' powers and creating a strong cooperation and mutual assistance mechanism for cases with an EU dimension, and harmonising offences subject to administrative sanctions.

An **EU-wide harmonised obligation to notify data breaches** will better protect individuals, ensure consistency across sectors and avoid competitive disadvantages.

Data subjects' rights and individuals' control over their data would be significantly strengthened by introducing new rights, as well as by improving and further clarifying existing ones. Children will benefit from measures specifically addressing their vulnerability.

Associations will have greater scope to support data subjects in the exercise of their rights, including in action before courts.

Applying general data protection principles to the area of police and judicial cooperation in criminal matters would enhance the overall coherence of the EU data protection framework, while respecting the inherent specificities of the law enforcement. Individuals' rights would in particular be strengthened by extending the scope of data protection rules in this area to 'domestic' processing, setting conditions for ensuring the right of access and providing stricter rules on purpose limitation.

In terms of **financial and economic impact**, the obligation for larger economic operators (more than 250 employees) to designate DPOs will not **create disproportionate costs**, as DPOs are already common in these companies. Compliance costs would amount to € 320 million per annum. The obligation would cover a necessary minimum segment of data controllers, as SMEs would be as a rule excluded from this obligation, unless their data processing activities entail significant data protection risks. Public authorities and bodies would be allowed to appoint one single DPO for several entities (e.g. covering several branches, departments, offices), taking account of their organisational structure.

Simplifying the rules for international transfers (for example, by extending the scope of "Binding Corporate Rules") would also have a positive impact on the international competitiveness of EU businesses.

Strengthening DPAs' independence and powers, together with the obligation for Member States to provide them with sufficient resources, would entail additional costs for public authorities that are currently not equipped with appropriate powers and adequate resources.

The new cooperation and mutual assistance mechanism between DPAs would also entail additional costs for national DPAs and the EDPS. For instance the additional tasks of the EDPS for providing the secretariat of the EU Data Protection Board - replacing the Article 29 Working Party - and in particular the involvement in the consistency mechanism are likely to require an increase of its current resources by an additional € 3 million per annum on average for the first six years, including credits for 10 additional human resources.

6.3. Policy Option 3: Detailed legal rules at EU level

Adding further detailed legal provisions, including sectoral ones, beyond the measures envisaged in option 2, would lead to a **maximum reduction of disparities between Member States**. However, there may not be enough flexibility for Member States to take account of national specificities.

The total abolition of notifications - except in case of prior checks - would greatly simplify the regulatory environment and reduce administrative burden.

Setting up an EU Data Protection Agency would greatly improve the **consistency of enforcement** and solve the inconsistencies for cases with a clear EU dimension but the powers of such an EU agency could go too far under EU law. However, this would be very costly for the EU budget. Harmonised criminal sanctions would also strengthen consistent enforcement, but would likewise be met with strong opposition by Member States.

Data subjects' rights, including the rights of children, would be further strengthened, for instance by extending the definition of sensitive data to include data of children, biometric

and financial data. The introduction of a right to "collective actions" could allow maximising rights by means of litigation. Additional strengthening of individual rights would be expected from harmonising the level of sanctions, including criminal ones, at EU level.

Explicit amendments of all instruments extending the general data protection rules to the area of police and judicial cooperation in criminal matters would have a positive impact in terms of consistency and coherence of the rules in this area and of strengthening individuals' rights. However, such a radical approach would encounter resistance from Member States' side and be politically difficult to achieve.

7. COMPARISON OF OPTIONS

Policy Option 1 would lead to low levels of compliance and administrative costs, especially for private data controllers, as most of the additional costs would fall on national and EU public authorities. At the same time it would only have a **limited positive impact on the identified problems and on achieving the policy objectives**.

In terms of political feasibility, though the proposals are not controversial, this policy option is likely to be met with resistance by stakeholders as a result of its limited scope and impact on the problems, and would be considered as not ambitious enough.

Policy Option 2 will lead to a **significant reduction of fragmentation and legal uncertainty**. It can be expected to have a much greater impact in addressing the identified problems and achieving the policy objectives. The balance of compliance and administrative **costs associated with this policy option are expected to be reasonable in view of the benefits and savings of about € 2.3 billion in administrative burden per annum – something which will be very important for enterprises**. This Option will ensure better and more consistent enforcement overall. The abolition of notifications in favour of a much simpler 'basic registration system' would also simplify the regulatory environment and reduce the administrative burden.

As to stakeholders' acceptance, this Option would generally be positively received by economic operators and public authorities as it would overall reduce their compliance costs, particularly those linked to the current fragmented regime. The strengthening of data protection rights would be welcomed by the data protection community and in particular DPAs. As regards the third general objective, this option would contribute to achieving the objectives of ensuring **more coherence and consistency of data protection rules in the area of police cooperation and judicial cooperation in criminal matters** by repealing and "lisbonising" the Framework Decision, thus eliminating its gaps, in particular by extending its scope to "domestic" processing.

Policy Option 3 includes most of the measures in Policy Option 2, while being more far-reaching under several aspects. It would therefore have a **high and positive impact in terms of both reducing costs linked to legal fragmentation and enhancing individuals' rights**. Moreover, it would maximise the consistency and coherence of data protection rules in the former third pillar and raise the data protection standards in that context. However, some of the measures included under this option either have an **excessively high compliance cost or are likely to encounter a strong opposition from stakeholders**. Furthermore, the simultaneous amendment of all former third pillar instruments would be very complex and politically controversial.

Preferred Option:

The ***Preferred Option*** consists of Option 2 combined with:

– the abolition of notification obligations from Option 3, and

– some 'soft measures' from Option 1: the encouragement of privacy-enhancing technologies and certification schemes, and awareness-raising campaigns

The Preferred Option is the most likely to achieve the policy objectives without excessive compliance costs, and with considerable reduction of administrative burden.

The strengthened data protection rules are expected to give rise to some additional compliance costs, in particular for controllers doing risky data processing activities. However, a strong data protection regime can offer a competitive advantage for the EU economy, as the higher level of protection and expected reduced number of data protection incident and breaches can increase consumer confidence. Requiring companies to adopt high standards of data protection can also lead to long-term improvements for European businesses, which could become world leaders in privacy enhancing technology or privacy by design solutions, drawing business, jobs and capital to the European Union.

Furthermore, for businesses operating within the EU internal market, the enhanced harmonisation will make the cross-border processing of personal data simpler and cheaper. This is expected to provide considerable incentives for such businesses to expand cross-border and reap the benefits of the internal market, with beneficial effects both for consumers and the European economy as a whole.

The Preferred Option includes a balanced solution also in relation to problem 3, as it strengthens individuals' rights, eliminates gaps and reduces inconsistencies as regards data protection in the area of police and judicial cooperation in criminal matters, while facilitating law enforcement cooperation and respecting the specificities of the sector and its operational needs.

8. MONITORING AND EVALUATION

Monitoring and evaluation of the impact of the preferred option will focus on elements such as the use of the new instruments introduced by the reform, the powers and resources of the national DPAs, the sanctions issued for breaches of data protection laws, the time and costs spent by data controllers for compliance, and the development of individuals' confidence in the protection of their personal data in the online environment.