MUNI
LAW

Introduction to European Personal Data Protection Law

František Kasl, Ph.D., Jakub Míšek, Ph.D.
Institute of Law and Technology, Masaryk University

Privacy

Privacy

Judith Thomson (1975):

„*Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.“*

- Thomson, Judith Jarvis. ‘The Right to Privacy’. *Philosophy & Public Affairs* 4, no. 4 (1975): 295–314.

Serge Gutwirth (2013):

„*The notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as ‘our’ privacy, it still finds a way to remain elusive.“*

- GUTWIRTH, Serge. *Privacy and the information age*. Lanham, Md: Rowman & Littlefield Publishers, 2002

Grounds of privacy I - Freedom

- Right to freedom of thought and consciousness
- Right to freedom of religion or belief

- Example – surveillance
  - Big Brother
  - Big Other (Little brothers)
  - Chilling effect

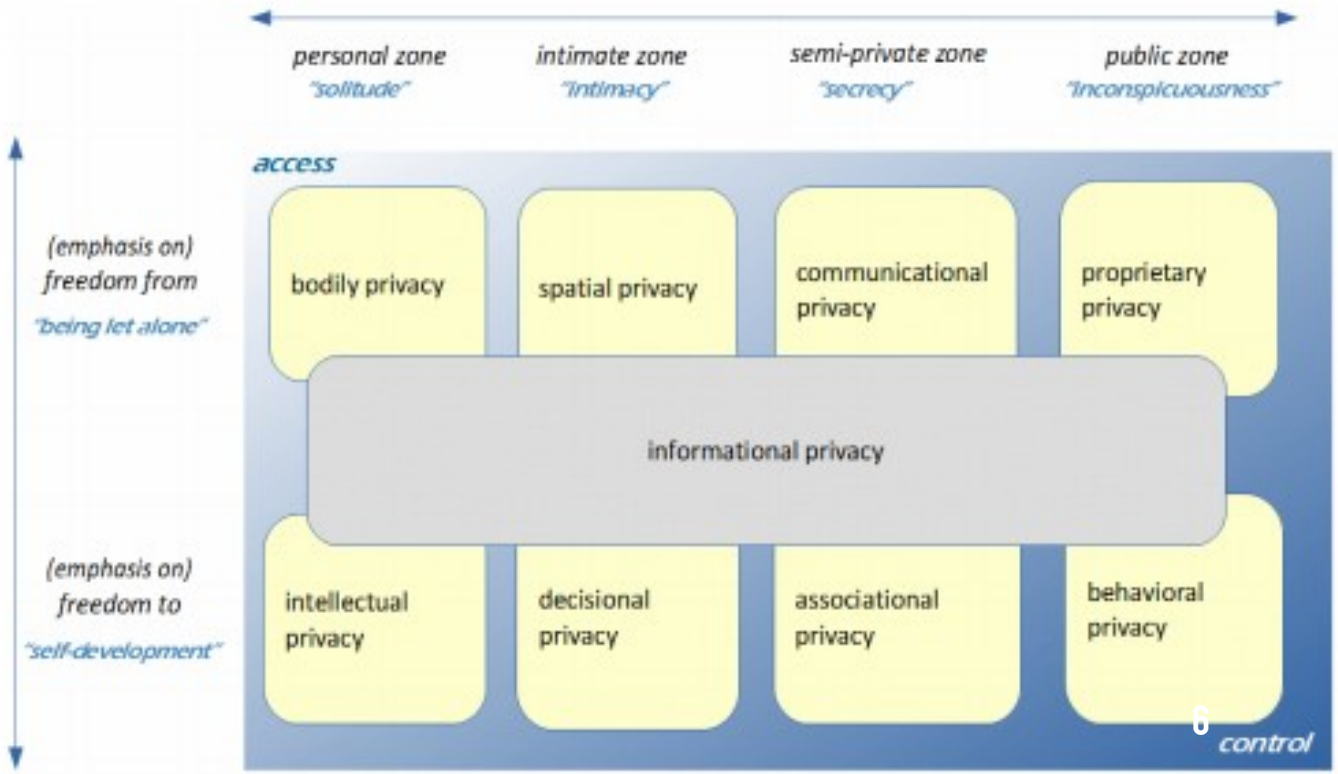
Grounds of privacy II
Informational self-determination

- 1983 – Germany, Census case
- The right to decide about information about one's privacy
- Freedom of speech and scientific work
- Protection of privacy, personality and right to a active family life

- Furthermore:
  - Right to education
  - Personal Data Protection
  - Public sector information

Informational Privacy

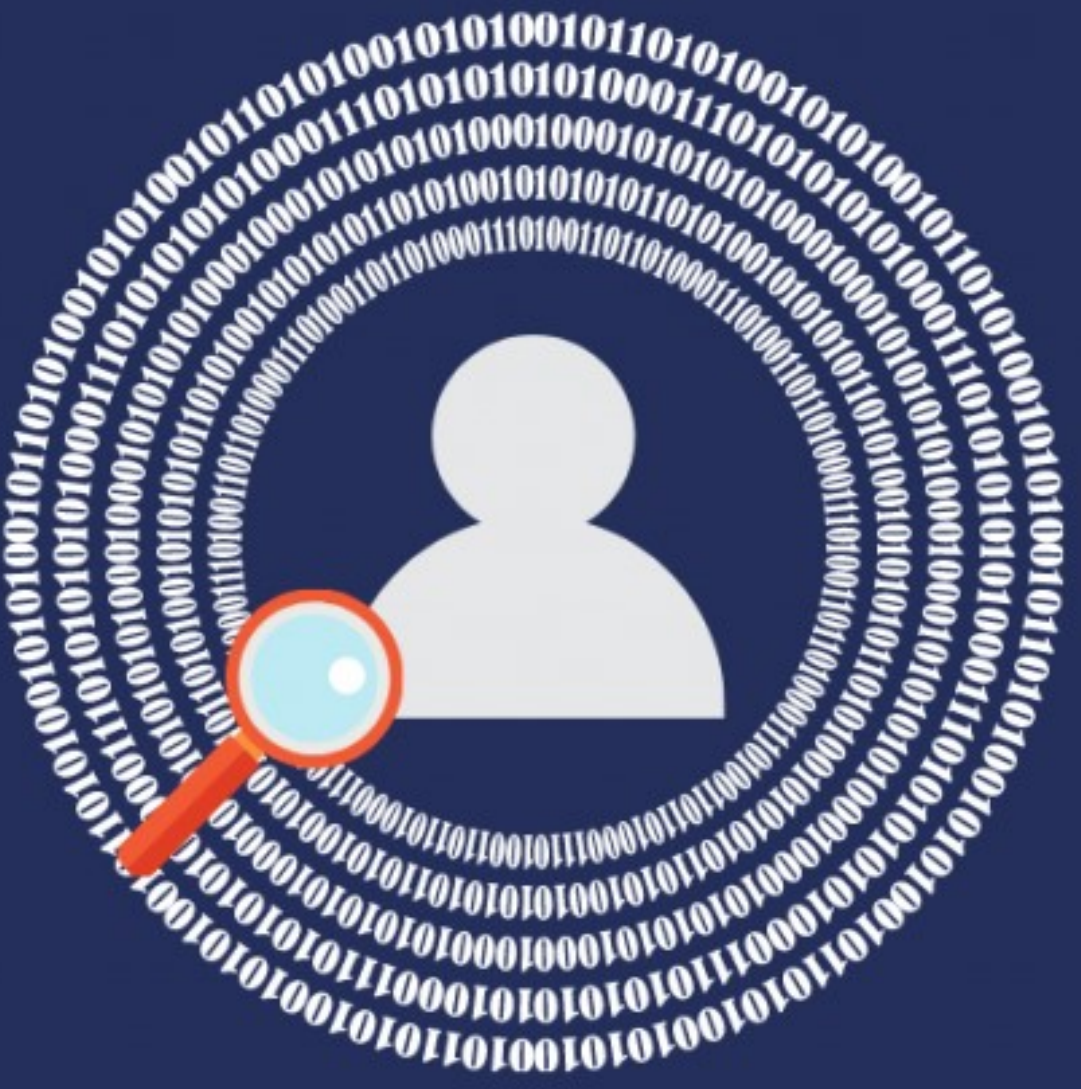
- Overlapping concept
- Virtualised image of other privacy spheres
- Connection with informational self-determination and personal data
- Bert Jaap-Koops et al. (2016)



Privacy v. Personal Data

- Personal data protection as an independent fundamental right
  - **Different purposes**
    - Protection of privacy v. Protection of rights and interests of natural persons in relation with processing of their personal data (+ purpose of enabling a fair processing)
  - **Different means of protection**
    - Private v. Public law
    - Restitutive v. Preventive
    - Court v. DPA

Personal data protection



History of data protection

- European Convention on Human Rights (1950)
- OECD Gudelines OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (**Convention 108**) (1981)
  - Recast – Convention 108+
- **Directive 95/46/EC**
  - Legislation started in summer 1990
  - Enacted 1995
- **General Data Protection Regulation (2016/679)**

Constitutional Level

- Art. 8 of the European Convention on Human Rights
  - **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.
  - Case law of ECHR

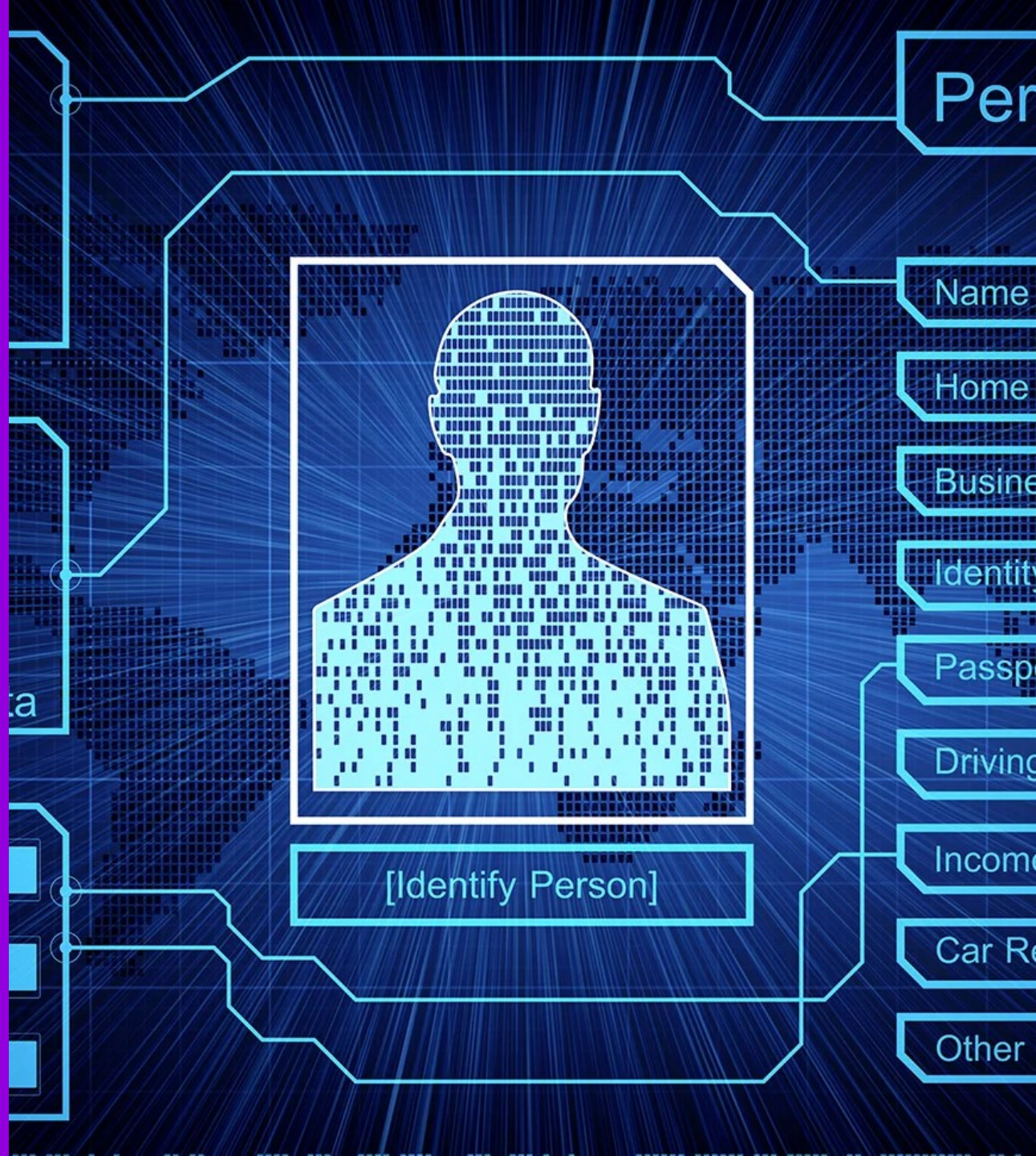
Constitutional Level

- Charter of Fundamental Rights of the European Union (2012/C 326/02)
- **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.

Legislation

- General Data Protection Regulation (2016/679)
- Police Directive (2016/680)
- In Czechia
  - Act No. 110/2019 Sb., on processing of personal data

Elements of personal data protection



Basic concepts

Prevention

A. Broad application

B. Purpose limitation and Data Minimisation

The cornerstone – Purpose of Processing

Almost everything in the personal data protection law (legality of processing) is evaluated in relation to the purpose of processing.

Basic concepts

General Data Protection Regulation

Accountability of the data controller

The principle of accountability of the data controller and the risk-based approach

- **Principle of accountability**
  - Art. 5 para 2 GDPR:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

  - Traditionally - "Keep your records."

Accountability

- Richard Mulgan: „*The concept of ‘account-ability’ includes an implication of potentiality, literally an ‘ability’ to be called to ‘account*’.“

- **To whom?**
  - DPA (Data protection authority)
  - Data subjects

- Preventive, proactive

Accountability

- Accountability – **Performance based rule**
  - “Adjust your processing of personal data to meet the needs of the specific situation so that you process personal data fairly.“
- Against what are duties measured?
- **Risk of data processing**

Art. 24 sec. 1 GDPR

“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.”

Risk based approach

- Combination of art. 5 sec. 2 and art. 24:
  - **“Adjust your processing of personal data to match the risks it creates.”**

- It applies to almost all duties under the Regulation
  - **Granularity and scalability** of data controller’s duties
  - The biggest news and the most significant change (for the better) of the GDPR compared to the Directive

  - Exception: Data subjects rights

Basic concepts

General Data Protection Regulation

Accountability of the data controller

Risk-based regulation

Basic concepts – Personal Data

- Art. 4 para. 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*

Basic concepts – Personal Data

- Recital 26:
  - […] 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. […]

Personal Data

- Breyer Case (CJEU) C-582/14
  - Dynamic IP Address is Personal Data
  - Para 46:
    - It is not personal data "*if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.*"

Anonymisation

- **Irreversible** modification of the dataset so that it no longer contains personal data
- Anonymisation techniques - examples
  - Removal of direct identifiers
  - Lowering of granularity
  - Aggregation
  - Data exchange
- Problems:
  - Anonymity v. Information value
  - De-Anonymisation

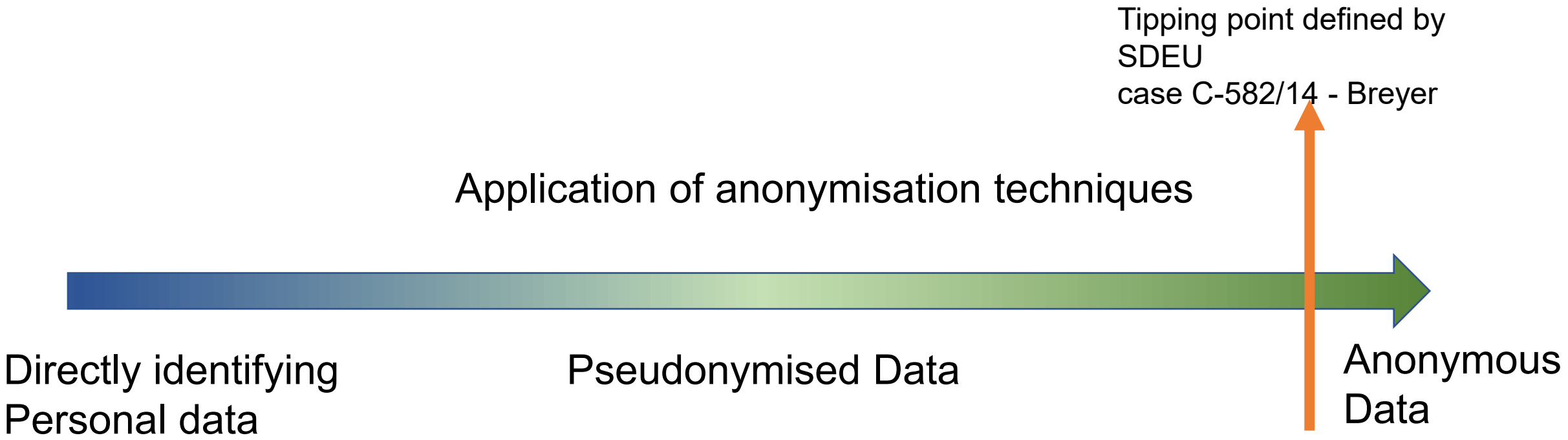
Anonymisation

- Recital 26:
  - *[…] 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.*
- Anonymous data – Ex-personal Data

Pseudonymisation

- Rec 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**. […]
- Art. 4 para 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

The scale of anonymity



Personal data processing

- Art 4, para 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

Material Scope of the Regulation

- Art. 2 para. 2 – exceptions:
  - activity which falls outside the scope of Union law
  - activities which fall within the scope of Chapter 2 of Title V of the TEU
    - Foreign and Security politics of MS
  - processing by a **natural person in the course of a purely personal or household activity**
    - E.g. Ryneš Case (C-212/13); Lindqvist Case (C-101/01)
  - Processing 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

Personal Data Controller

- **Controller**
  - = 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
  - Example – Google Search Engine
- Joint controllers
  - CJEU:
    - C-210/16 - Wirtschaftsakademie Schleswig-Holstein (5. 6. 2018)
    - C-25/17 - Jehovan todistajat (10. 7. 2018)
    - C-40/17 - Fashion ID (29. 7. 2019)
- **Processor**
  - = natural or legal person, public authority, agency or other body which processes personal data **on behalf of the controller**
  - A contract on data processing

Territorial scope

- Art. 3 para 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.
  - "Context of the activities"
    - Not where the controller is necessarily established, but where the establishment is involved in the activities related to the data processing
  - Location of the data is not important for the scope of application

Establishment

- Recital 22:
  - […] 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.
- CJEU Google Spain Case (C-131/12)
- CJEU Weltimmo Case (C-230/14)
  - Website, Stable Legal Representative, Bank Account

Territorial Scope II

- Art. 3, Para. 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.

Jurisdiction: Competent DPA

- Controller + Processor:
  - Recital 36:
    - The competent **lead supervisory authority** should remain the supervisory authority of the Member State **where the controller has its main establishment**
    - The supervisory authority of the processor (supervisory authority concerned) should participate in the cooperation procedure
- Controller has establishments or activities in more than one MS

  OR: processing of personal data which takes place in one MS but it substantially affects may affect data subjects in more than one EU MS
  - Recital 124
    - DPA of the Main Establishment = lead supervisory authority
    - It should cooperate with other DPAs

Rules for processing of personal data

Art. 5 - principles of personal data processing

- Principle of lawfulness, fairness and transparency
  - processed lawfully, fairly and in a transparent manner in relation to the data subject
- Principle of purpose limitation
- Principle of data minimalization
- Principle of accuracy
- Principle of storage limitation
- Principle of integrity and confidentiality
- Principle of accountability
  - The controller shall be responsible for, and be able to demonstrate compliance with rules

Legal grounds for processing – Art. 6 para. 1

a) Consent of the data subject

b) Processing is necessary for the performance of a contract to which the data subject is party

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

Consent

- **Freely given**
  - Real choice is necessary
  - no risk of deception, intimidation, coercion or significant negative consequences
  - Art. 7 para. 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.
- **Specific**
  - Scope and consequences of data processing are defined
  - Not open ended set of processing activities
- **Informed**
  - 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 (Rec. 42)
  - 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.(Rec. 58)
- **Unambiguous**
  - Leave no doubt

Legitimate interests pursued by the controller

- Art. 6 para. 1 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
- Rec. 47, Rec. 49

Legitimate interests pursued by the controller

- **Balancing test!**
  1. Criterion of suitability
     - Does the institute restricting a constitutional right allows the achievement of the desirable aim (protection of another constitutional right of public interest)?
  2. Criterion of necessity
     - Can the same objective be achieved by another less intruding method?
  3. Comparison of conflicting constitutional rights

- Examples:
  - Google Spain, IP Addresses in CySec
  - Open Data Applications

Duties of the controller

- Responsibility of the controller (Art. 24)
  - Controller must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation
- Data protection by design and by default (Art. 25)
- Records of processing activities (Art. 30)
  - Files and documents
- Cooperation with the supervisory authority (Art. 31)
- Security of processing (Art. 32)
- Notification of a personal data breach to the supervisory authority (Art. 33)
- Data protection impact assessment (Arts. 35)
- Data protection officer (Arts. 37 – 39)

Data subject rights

Rights of the data subject

- Right to information about processing
  - Art. 13 (when data collected from the subject)
  - Art. 14 (when data collected from a third person)
- Right of access by the data subject (Art. 15)
- Right to rectification (Art. 16)
- Right to erasure (‘right to be forgotten’) (Art. 17)
- Right to restriction of processing (Art. 18)
- Right to data portability (Art. 20)
- Right to object (Art. 21)
  - When: Legitimate interest OR Public interest OR Direct marketing
- Automated individual decision-making, including profiling (Art. 22)

Right to information about processing

- Basic information about processing:
  - Who, how, why (purpose), why (legal ground), how long, where…
- Art. 14 para. 5 – exception. Information duty not apply when:
  - the data subject **already has the information**
  - 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 … 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
  - **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
  - **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

Right to erasure (Right to be Forgotten)

- Google Spain Case
- 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, when:
  - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
  - the data subject withdraws consent on which the processing is based
  - the data subject objects to the processing pursuant to Article 21(1) (legitimate or public interest) and there are no overriding legitimate grounds for the processing
  - the personal data have been unlawfully processed
  - the personal data have to be erased for compliance with a legal obligation
  - Children consent

Right to erasure (Right to be Forgotten)

- Viral nature of the right (Art. 17 Para. 2)
  - If controller made public
- Exceptions (Art. 17 Para. 3) - Processing is necessary for:
  - exercising the right of freedom of expression and information
  - compliance with a legal obligation or for the performance of a task carried out in the public interest
  - reasons of public interest in the area of public health
  - archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)
  - the establishment, exercise or defence of legal claims

A problem with time

- Forgetting – natural and useful process
- Internet does not forget
  - Collective memory
  - Past made present
    - Streisand effect
    - Long past misconducts
- Furthermore!
  - The value of Data changes in time

International Data Transfers

Why do we deal with it

- Cross-border data flow (including personal) is essential
- Teritoriality
  - Different countries – different levels of protection
- Possible loophole – exported data might not be protected
- Data Transfers Rules - ensuring data are protected even when transferred abroad

- Conflict: adequate protection v. free flow of data (one of the origins of data protection law)

Data transfers under GDPR

- Free flows of data in the EU/EEA
  - + Convention 108(+)

- Transfers to “third countries”
  - Adequacy
  - Appropriate safeguards
  - Derogations

Adequacy

- Art. 45 GDPR

  „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.“
- Decision of European Commission on adequate level of protection in particular country/sector in country/international organization
- Not necessarily indefinite force - possible monitoring, amendment, repeal or suspension
- Example - Japan
  - Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance)

Adequacy

- Assessment of:
  - 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 …
  - 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
  - the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments

Adequacy

- States providing adequate protection (as recognized by EC decisions)
  - Andorra
  - Argentina
  - Canada (commercial organizations)
  - Israel
  - Japan
  - New Zealand
  - Switzerland
  - Uruguay
  - United Kingdom
  - Republic of Korea
  - ~~USA~~
    - CJEU Cases Schrems I (C-362/14) and Schrems II (C-311/18)
  - + smaller territories (Faroe Islands, Guernsey, Isle of Man, Jersey)

Appropriate safeguards

- Art. 46 and following GDPR
- Legally binding and enforceable instrument between public authorities or bodies
- Binding Corporate Rules
- Standard Contractual Clauses
- Codes of Conduct
- Certifications

- Subject to specific approval:
  - Ad hoc contractual clauses
  - Provisions to be inserted into administrative arrangements

Derogations

- Art. 49 GDPR
  - Explicit consent, „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“
  - Performance of a contract
    - between the data subject and the controller
    - concluded in the interest of the data subject between the controller and another natural or legal person
  - Important reasons of public interest
  - Establishment, exercise or defense of legal claims
  - Vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
  - Transfer is made from a register which according to Union or Member State law is intended to provide information to the public
  - **Escape clause** : necessary for the purposes of compelling legitimate interests only if transfer is not repetitive, concerns only a limited number of data subjects
    - The controller shall inform the supervisory authority and the data subject of the transfer.
- EDPB Guidelines 2/2018

MUNI
LAW

Thank you for your attention!