Personal data protection I

Jakub Míšek

7. 11. 2019

Privacy v. Personal Data - recap

- 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
    - Distributive v. Non-distributive right

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.

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.

Constitutional Level

- Czech - Charter of Fundamental Rights and Freedoms
  - Art. 7 (Protection of privacy, person and household)
  - Art. 10 (Para. 3: Everyone has the right to be protected from the unauthorized gathering, public revelation, or other misuse of her personal data.)

Reminder - Informational self determination

- 1983 – Germany, Census case
- One of basic premises of personal data protection
  - Examples:
    - Accent on consent
    - Right to be forgotten
    - Right to object the processing

Legislation

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

Basic concepts

I. Prevention

Basic concepts

I. Prevention

A. Broad application

B. Purpose limitation and Data Minimisation

Basic concepts

General Data Protection Regulation

II. Accountability of the data controller

III. Risk-based regulation

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 – 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. […]

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
- Direct X Indirect Identification
- Objective v. Subjective approach
- Context is everything!

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.*"

Personal Data

- Cases of wrong anonymisation
  - AOL search data
- Sex, Date of Birth, ZIP cod
  - 87% of US citizens

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

Anonymisation

- Problems:
  - Anonymity v. Information value
- Anonymisation techniques - examples
  - Removal of direct identifiers
  - Lowering of granularity
  - Aggregation
  - Data exchange
- De-Anonymisation

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

Special categories of Personal Data

- 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

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. 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.

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

Material Scope of the Regulation

- Art. 2 para. 3 – exceptions:
  - processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EU) No 1725/2018 applies
- Art. 2 para. 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

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
- 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

Main Establishment

- Rec. 36:
  - […]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.[…] 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.

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.

Territorial Scope II

- Rec. 23
  - Offering of the services – is it apparent? Could the controller envisage that?
    - Inspiration by the consumer targeting case law of the CJEU (e.g. Pammer & Hotel Alpenhof Case C-585/08)
- Rec. 24
  - Monitoring Behaviour
    - Tracking
    - Profiling
    - Analysing or predicting of personal preferences etc.
- Example – Google Spain case and CNIL (French DPA)
- Problem?
  - Enforceability
  - Everything or nothing approach

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

Right to lodge a complaint with a supervisory authority

- Article 77:
  - […] 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.

- **One-Stop-Shop Principle**
  - If DPAs cannot Agree, the Board will decide

Right to an effective judicial remedy against a supervisory authority

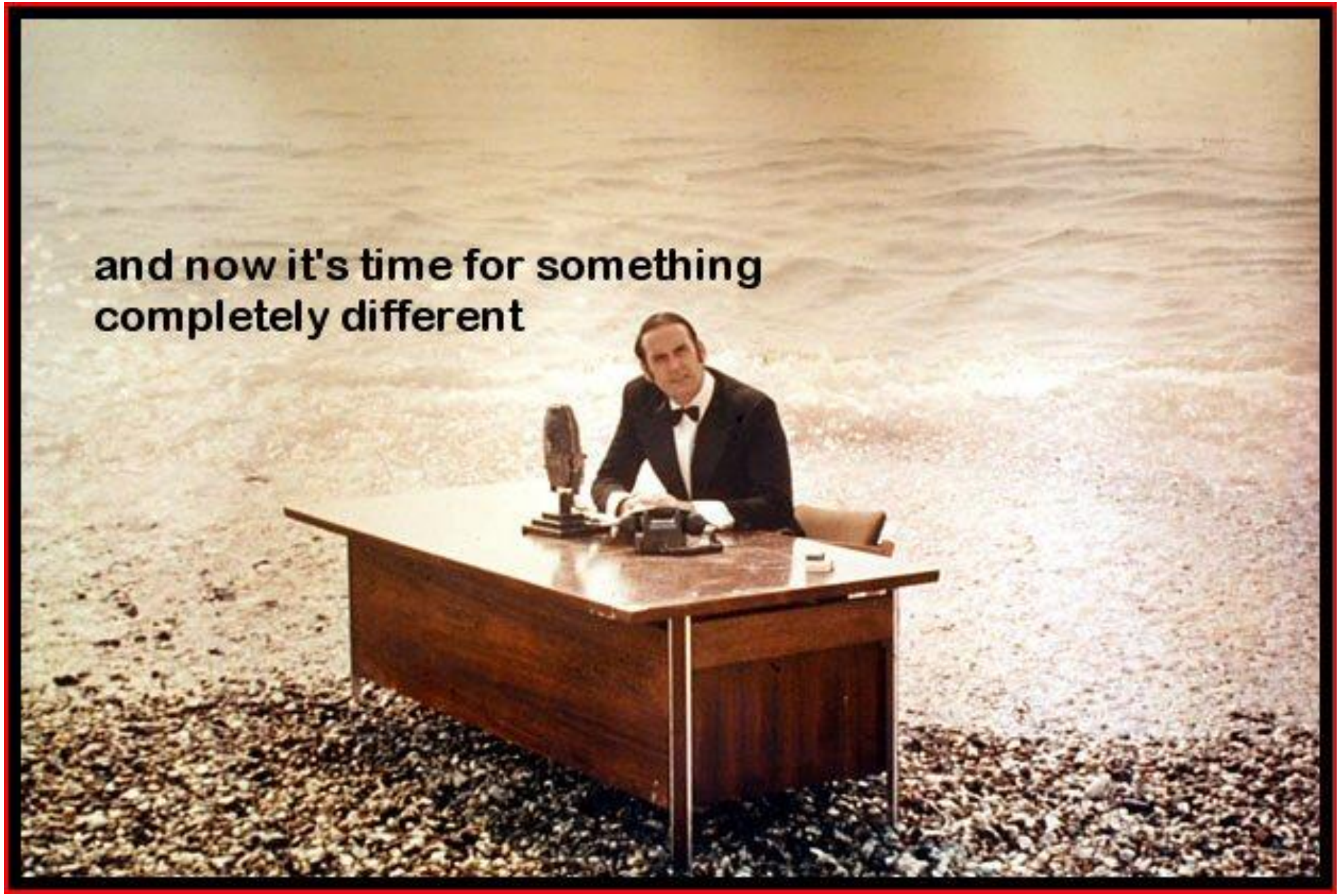
- Art. 78:
  - […] each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them
- Related proceedings
  - Rec. 144
    - Cooperation of courts in the case of the same processing
    - Court may stay its proceedings if there is a related proceedings elsewhere

Right to an effective judicial remedy against a controller or processor

- Art. 79
  - (1) […] 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.

Court action against decision of the Board

- Recital 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. […]
- Art. 263 TFEU


and now it's time for something
completely different

Art. 5 - principles to processing of PD

- 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

- Consent of the data subject
- Processing is necessary for the performance of a contract to which the data subject is party
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- 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
- 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
- **Balancing test!**

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

Further processing (Art. 6 para. 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 …, 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:
  - any link between the purposes for which the personal data have been collected and the purposes of the intended further processing
  - the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller
  - the nature of the personal data
  - the possible consequences of the intended further processing for data subjects
  - the existence of appropriate safeguards, which may include encryption or pseudonymisation

Art. 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.

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 Access (Art. 15)

- Data subject can actively ask for:
  - Basic information about processing:
    - Who, how, why (purpose), why (legal ground), how long, where…
  - Para 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.

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

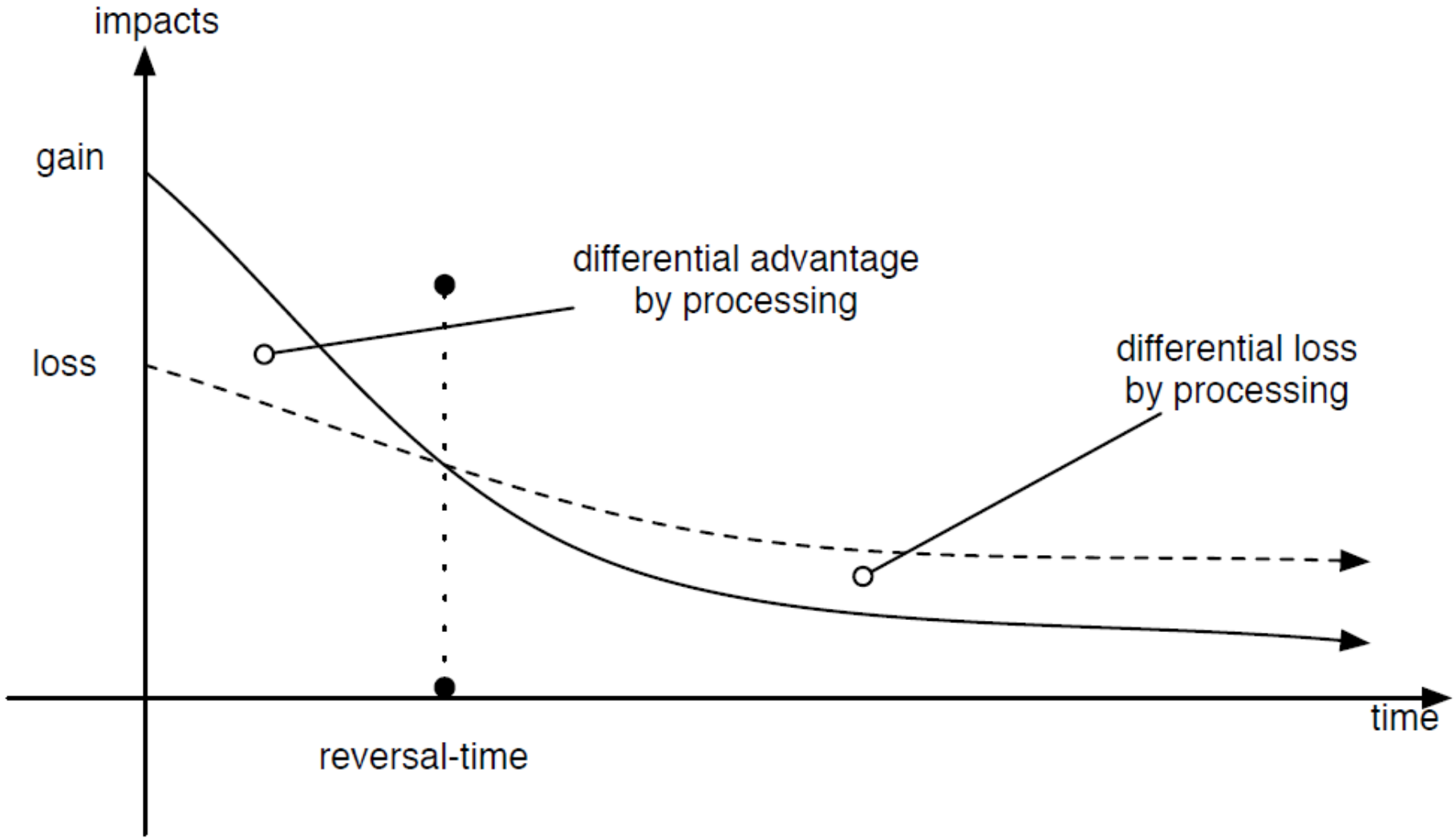


Figure 1 The impact of processing (line) and non-processing (dotted line) over time

Korenhof, Paulan, Jef Ausloos, Ivan Szekely, Meg Ambrose, Giovanni Sartor, and Ronald Leenes, 'Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data', in *Reforming European Data Protection Law*, ed. by Serge Gutwirth, Ronald Leenes, and Paul de Hert, Law, Governance and Technology Series, 20 (Dordrecht: Springer Netherlands, 2015), p. 191.

Right to restriction of processing (Art. 18)

- The data subject shall have the right to obtain from the controller restriction of processing when:
  - 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
  - the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead
  - 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
  - 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

Notification obligation of the controller

- Art. 19
  - Controller shall communicate any rectification or erasure of personal data or restriction of processing … 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.

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 protection impact assessment (Art. 35)

- Practical realisation of the Responsibility of the controller (Art. 24)
- Main purpose – to be sure that the controller fulfils all the duties arising from GDPR
  - Prevention principle
- Different to standard risk management
- Result of DPIA should be seen in the processing itself
- Para. 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.

Data protection impact assessment (Art. 35)

- Para. 3
  - A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of
    - 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
    - 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
    - a systematic monitoring of a publicly accessible area on a large scale
- WP 29 Guidelines
  - 9 Categories

Data protection impact assessment (Art. 35)

- WP 29 Guidelines
  - 9 Categories
    1. Evaluation or scoring
    2. Automated-decision making with legal or similar significant effect
    3. Systematic monitoring
    4. Sensitive data or data of a highly personal nature
    5. Data processed on a large scale
       - Number of subjects/ Volume of data/ Duration/ Geographical extent
    6. Matching or combining datasets
    7. Data concerning vulnerable data subjects
    8. Innovative use or applying new technological or organisational solutions
    9. When the processing in itself *“prevents data subjects from exercising a right or using a service or a contract”*

Data Protection Officer (Art. 37)

- Para 1 - The controller and the processor shall designate a data protection officer in any case where:
  - the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
  - 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
  - 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

Data Protection Officer (Art. 37)

- Rec. 97:
  - … 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

Thank you for your attention.

Questions?

Jakub Míšek
@jkb_misek