Personal data protection online II

Rights of the data subject, Duties of the data controller and processor

Jakub Míšek

15. 11. 2018

Recap: Basic concepts

I. Prevention

A. Broad application

B. Purpose limitation and Data Minimisation

Recap: Basic concepts

General Data Protection Regulation

II. Accountability of the data controller

Recap: 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.

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, 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

Legal Obligation and Public Interest

- Art. 6 para. 3:
  - Union law or Member State law to which the controller is subject
  - Law determines purposes
    - Should specify also general conditions 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
- Case C-465/00, C-138/01 and C-139/01 – Österreichischer Rundfunk

Consent

- Art 4, para 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
- Rec 42
  - Controller should be able to demonstrate that the data subject has given consent to the processing operation
- Data subject can withdraw at any time

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

Consent of Children (Art. 8)

- Information Society Service
  - Definition in Directive 2015/1535
- 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. 2Where 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
- More in your essays!

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

Reminder: 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

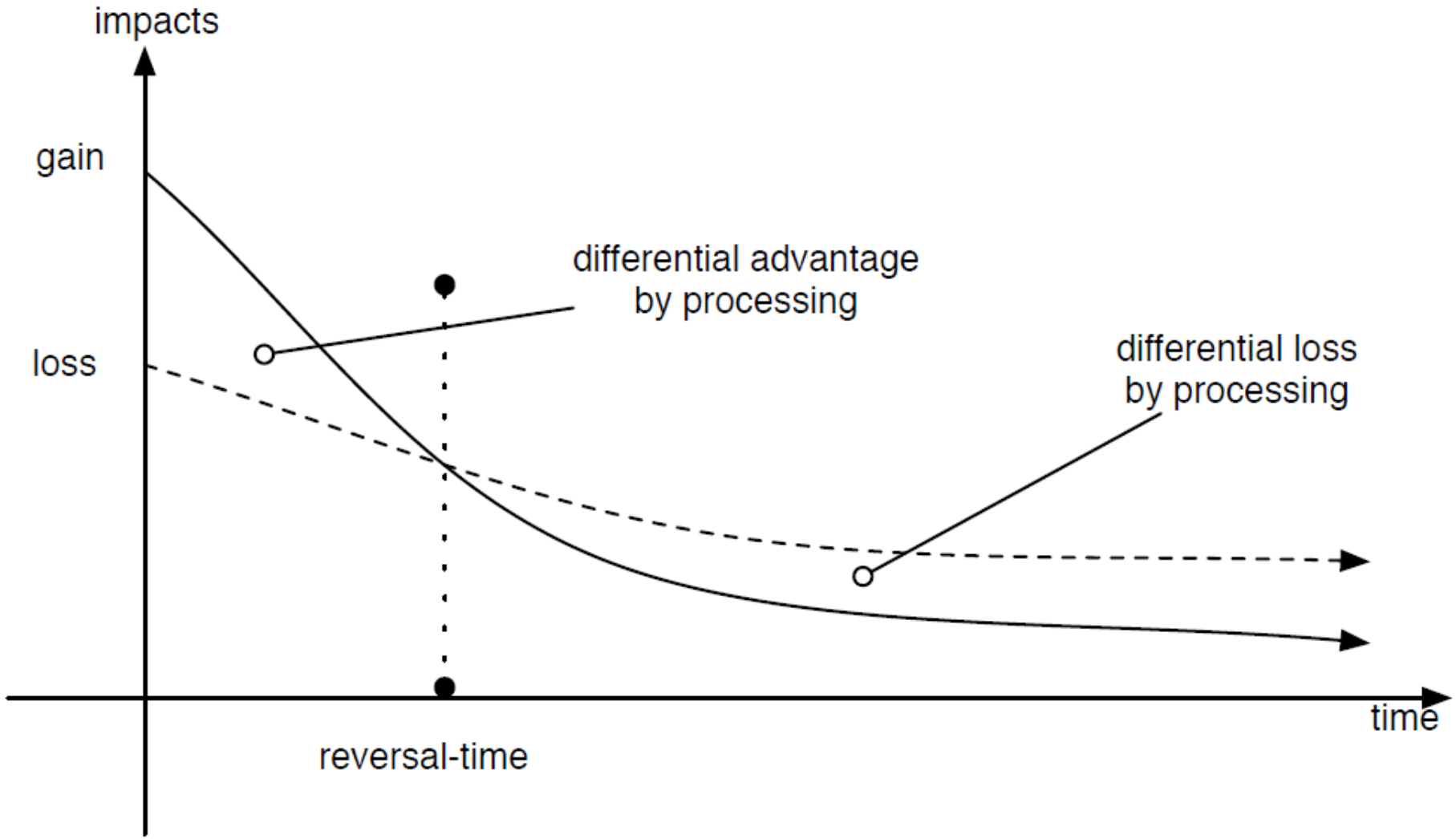

Figure 1 The impact of processing (line) and non-processing (dotted line) over time

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 Categhories

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

Examples / Exercise

Thank you for your attention.

Jakub Míšek
@jkb_misek