Personal data protection online I – Basic concepts, jurisdiction and applicable law

Jakub Míšek

8. 11. 2018

Recap: Privacy v. Personal Data Protection

- Scope of protection
  - DP – No legal persons, no dead persons
- Private v. Public law
- Restitutive v. Preventive
- Court v. DPA
- Distributive v. Non-distributive right

- Personal data
  - Disconnected from privacy protection
  - Disconnected from a man

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

- Directive 95/46/EC
- General Data Protection Regulation (2016/679)
- Police Directive (2016/680)
- In Czechia
  - Act No. 101/2000 Sb., on personal data protection

Legislation

- ~~Directive 95/46/EC~~
- General Data Protection Regulation (2016/679)
- Police Directive (2016/680)
- In Czechia
  - ~~Act No. 101/2000 Sb., on personal data protection~~
  - In the process: Act on personal data processing (Proposal No. 138)

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

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

- Cases of wrong anonymisation
  - AOL search data
  - Netflix
    - Movie reviews – 1-5 stars
      - 6 unusual movies – 84% uniqueness
      - With time stamp (2 weeks tolerance)
        - 6 random movies 99% uniqueness
- Sex, Date of Birth, ZIP cod
  - 87% of US citizens

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

- 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 (EC) No 45/2001 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 I

- 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 - Controller

- Art. 4 para. 16 a):
  - as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment

Main Establishment - Processor

- Art. 4 para. 16 b):
  - as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation

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.

Applicable Law

- 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"
- WP 29 (Opinion 179 on applicable law):
  - Location of the establishment of the controller is the main criterion. Neither the nationality or place of habitual residence of data subjects, nor the physical location of the personal data, are decisive for this purpose.

Applicable law – examples (WP29, O. No 179)

A) Establishment in Austria + processes personal data in Austria in the context of the activities of that establishment
   - the applicable law: law of Austria - that is, **where the establishment is situated**.

B) Establishment in Austria + processes in the context of activities of which he processes personal data collected via **its website**.
   - The website is accessible to users in various countries.
   - Applicable Law - still the law of Austria - that is, **where the establishment is situated** - independently of the location of users and of the data.

Applicable law – examples (WP29, O. No 179)

C) Establishment in Austria + processing done by a processor in Germany. The processing in Germany is in the context of the activities of the controller in Austria.

- Purpose and instructions are set by the Austrian company
- The applicable law for the processor: law of Austria

D) Establishment in Austria + opens representation in Italy which organizes all the Italian contents of the website and handles Italian users' requests

- Data processing by the Italian office is conducted in the context of Italian establishment.
- Applicable Law - the law of Italy

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?
  - Enforcebility
  - Everything or nothing approach

Jurisdiction

- Applicable law and Jurisdiction not always the same
- Generally – Competent Data Protection Authority (DPA) where the Establishment is

Jurisdiction II : 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

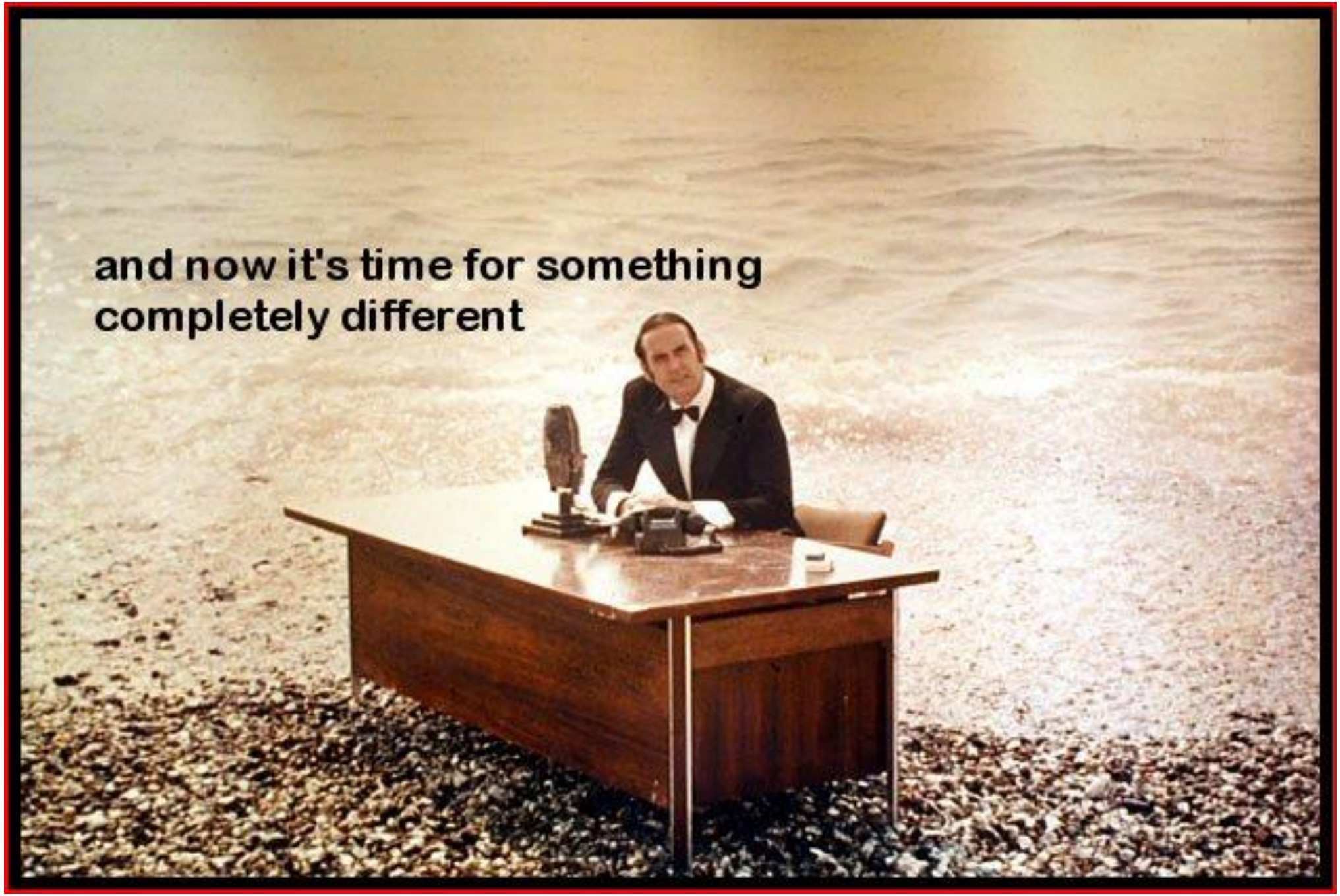
- Art. 78:
  - […] each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them
- Related proceedings
  - Rec. 144
    - Cooperation of courts in the case of the same processing
    - Court may stay its 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
- Specific
- Informed
- Unambiguous
- Rec 42
  - Controller should be able to demonstrate that the data subject has given consent to the processing operation
  - For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended
  - Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

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

- **Balancing test!**

More on this – next week.

Thank you for your attention.

Jakub Míšek
@jkb_misek