The Processing of Personal Data

Key features from a data protection perspective

DSI Data Day, 4th July 2018

Dr. Robert Weniger

Agenda

Part I - What is data protection?

Part II - Basic terms

Part III - EU General Data Protection Regulation 2016/679

Part IV - Questions

Part I - What is data protection?

Nothing to hide?

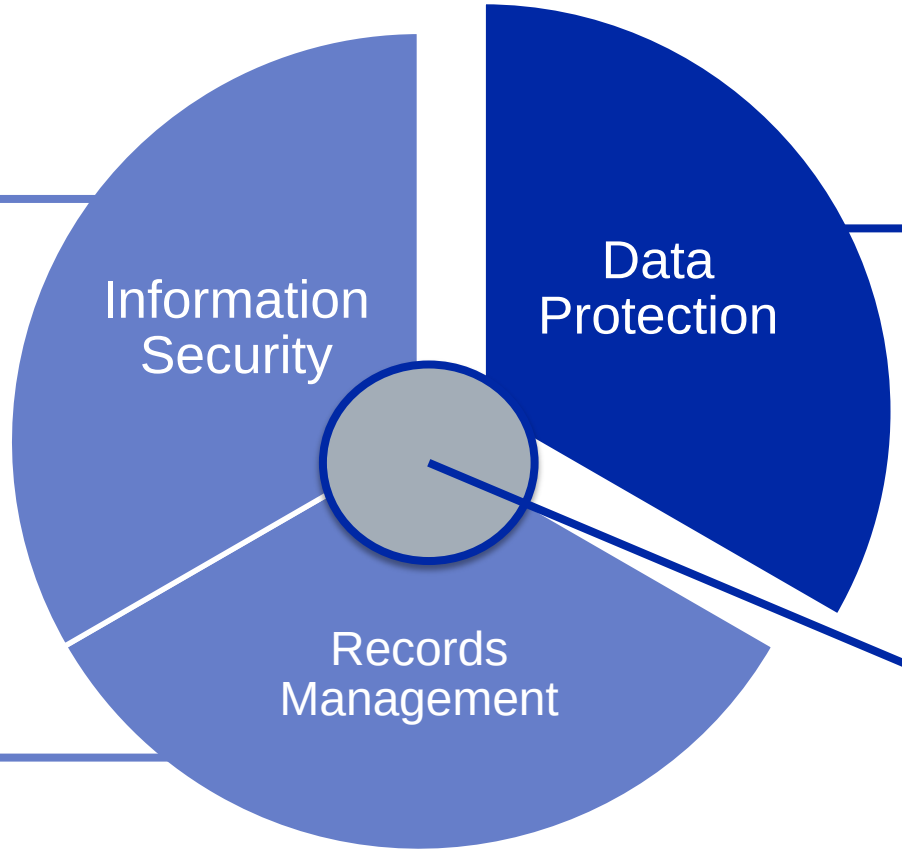
What is data protection?

- Data Protection (or «privacy») shall ensure, **that everyone has the right to decide for him-/herself**
  - **whether** and **who**
  - processes **which data** about his/her person
  - for **which purpose**
  - **where** the data is **stored**
  - **to whom** the data is **transferred** for which purpose
  - **when** the data is **deleted**

- Data protection is enshrined in the **fundamental right to informational self-determination**:
  - Art. 10 Abs. 2 und 13 Swiss Federal Constitution; Art. 10 Constitution of the Canton of Zürich

Interfaces to data protection in the area of information management

Subject matter:
Personal data and non-personal data
Objective:
To ensure the confidentiality, integrity and availability of data of authorities and companies



Subject matter:
Personal data
Objective:
To ensure personal rights, in particular the fundamental right to informational self-determination

Subject matter:
Business-relevant data (which may encompass both personal data and non-personal data)
Objective:
To ensure the legal obligation to properly collect, process, store, reproduce, transmit and destroy business-relevant data

Overlap: Technical-organisational measures

Part II - Basic terms

Law on Information and Data Protection of the Canton of Zurich (IDG)

- Applies to **public bodies** of the canton of Zurich (§ 1 Abs. 1 i.V.m. § 3 Abs. 1 IDG ZH), e.g.
  - University of Zurich (UZH)
  - Institutions of Higher Education (ZHAW, ZHdK, PHZH),
  - Power stations of the Canton of Zurich (EKZ)
  - University Hospital of Zurich (USZ)
- Regulates the handling of **information**, i.e.:
  - **Personal data**
  - **Special categories of personal data**
  - **Non-personal data**
- Persons are **natural persons as well as legal entities**

What are personal data?

- **Very broad term**:
  - All information relating to an “identified" or "identifiable" person (cf. § 3 para. 2 IDG ZH)

- A person is **identified** if his/her identity directly results from the available information:
  - Photo, passport, personal file, tax file, certificate

- A person is **identifiable** if his/her identity does not derive directly from the available information but only in combination with other information:
  - Account number, ID number, vehicle registration number, telephone number, e-mail address, IP address

Illustration of personal data

Name: Max Mustermann

Social insurance no.: 756.1234.5678.97

E-Mail address: muster@abc.ch

Current IP address: 192.0.2.42

Passport no.: ABC123EFG

Bank account no.: 123-456789.10A

Address: Musterstrasse 1, CH-1234 Musterdorf

Comment in blog XY: May 2018

Profession: Computer scientist

Credit card billing for account no. XYZ: May 2018

Downloads from music and filmstore XY: May 2018

Flight e-ticket no.: AB1CD23

Data communication on gaming platform XY: May 2018

Automatically transmitted data from fitness tracker XY about heart rate: May 2018

What are special categories of personal data?

- **Definition is settled in § 3 para. 4 IDG ZH**

- Information for which there is a **particular risk of an infringement of personal rights** due to its **importance** or due to the **way it is processed** or due to the possibility of **combining with other information**, such as information about:
  1. **religious**, **ideological**, **political** or **trade union** views or activities,
  2. **health**, **privacy**, **racial** or **ethnic origin**,
  3. **social assistance measures**,
  4. **administrative or criminal prosecutions or sanctions**

- **Compilations of information** which allow an **assessment of essential aspects of the personality** of natural persons

Restrictions on the processing of special categories of personal data

- Requirement for a **sufficiently specified regulation in a formal law** for the processing of the data (cf. § 8 para. 2 IDG ZH).
- Requirement to **explicitly inform** the data subject **when collecting the data** (cf. § 12 para. 2 IDG ZH).
- Requirement for an **explicit consent** of the data subject in the event of an information access requests, **otherwise rejection of the request** (cf. § 26 para. 2 IDG ZH).

Reference to a person, pseudonymization and anonymization

Allocation table
Patient: 4711
Name: Max Mustermann

Personal data / Special categories of personal data:

Max Mustermann
has a blood pressure of 160/100mmHg

Pseudonymised data

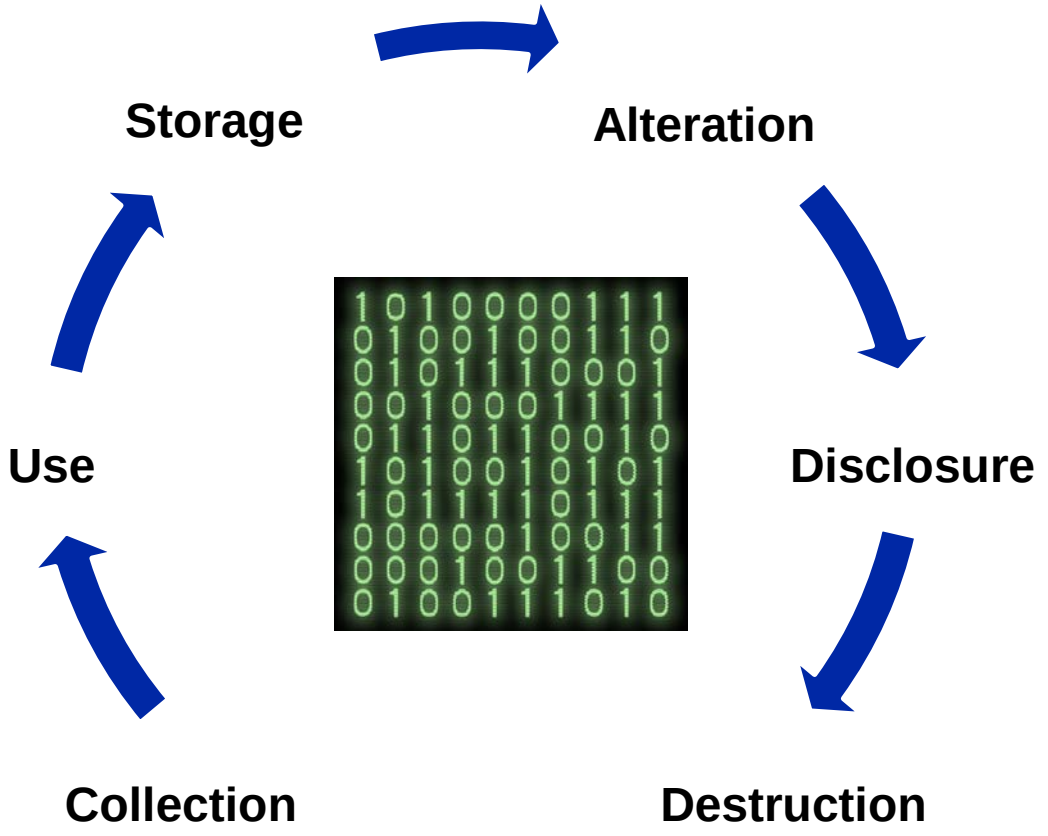
Patient 4711
has a blood pressure of 160/100mmHg

Anonymised data

A patient
has a blood pressure of 160/100mmHg

What is a processing of personal data?

- **Very broad term**
- **Includes any handling of personal data**, regardless of the used means and procedures
- § 3 para. 5 IDG ZH provides **an exemplary and not conclusive list** of single processing steps



Data protection principles

- Legality and proportionality (§ 8 IDG ZH)
- Data avoidance and data minimisation (§ 11 IDG ZH)
- Transparency (§ 12 IDG ZH)
- Purpose limitation (§ 9 Abs. 1 IDG ZH)
- Information security (7 IDG ZH)
- Commissioned processing of personal data (§ 6 IDG ZH)
- Cross-border data disclosure (§ 19 IDG ZH)
- Information access and data subjects rights (§ § 20, 21, 22, 28 IDG ZH)

Part III - EU General Data Protection Regulation 2016/679

How far are Swiss universities being affected?

- **Extraterritorial effect - Art. 3 (2)**
- The GDPR applies to the processing of personal data of a controller or a processor **not established in the EU**, **under condition** that the processing activities are related to:
  - the **offering of goods or services to data subjects in the EU** - Art. 3 (2) a; or
  - the **monitoring of data subjects' behaviour** as far as their behaviour takes place **within the EU** - Art. 3 (2) b.
- It is **sufficient that the stay** of the data subject in the EU **was temporary**, when the processing activity occurred
- Neither the **nationality** nor the **status as an EU citizen of the data subject** is relevant

Offering of goods or services to data subjects in the EU - Art. 3 (2) a

- Not relevant whether goods and services are subject to payment or are **free of charge**
- Goods or services **must be "intended" to be offered in the EU**
  - **Indications** are provided by **Recital 23**: "… factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union."
  - **However the question** whether or not goods or services are aimed at resp. offered to persons staying in the EU **must be determined in an overall view**, **in which other factors may play a role as well**
- **Possible cases**, where Swiss universities **may trigger** the applicability of the GDPR:
  - Contracted research
  - Cross-border service provided by an institute or hospital of the university, such as dental and microbiological examinations

Monitoring of data subjects' behaviour in the EU - Art. 3 (2) b

- Measures must be **intended to provide for a sustainable observation** of the data subject
  - **Indications** are provided by **Recital 24**: " … In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."
  - **Includes** social plugins and cookies, which enable individual traceability of users, which e.g. pursue the purpose of individual advertising (targeted advertising). **Does not include** measures which are intended only as a one-off activity, such as session cookies for the purpose of online shopping
- **Possible cases**, where Swiss universities **may trigger** the applicability of the GDPR:
  - Collection of personal data from test persons located in the EU e.g. **for surveys or measurements in research projects**, **in particular through questionnaires on websites** of the university or **through apps, provided by the university** for research projects
  - **Monitoring the progress in e-learning tools resp. online courses** offered to students in the EU

Impact: What are the keypoints?

- New obligations on **information to be provided to data subjects** - Art. 12, 13 and 14
- Data Protection **Impact Assessment** - Art. 35
- Conditions for **consent** - Art. 7
- **Right of data access** by the data subject - Art. 15
- **Right to be forgotten** - Art. 17
- **Data protection by design** and by default - Art. 25
- **Security** of processing - Art. 32
- **Data breach reporting** to supervisory authorities - Art. 33, and to affected data subjects - Art. 34
- **Fines** Art. 83 (4) a) and Art. 83 (5) b)
- **Liability for damages** suffered by the data subject - Art. 82

How far is scientific research privileged?

- **Consent**: data subjects **may give their consent** to the processing of their personal data **for one or more specific purposes** - Art. 6 (1) a
- **Purpose limitation**: further processing for scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes - Art. 5 (1) b
- **Storage limitation**: personal data may be stored for longer periods - Art. 5 (1) e
- **General prohibition of the processing of special categories of personal data**: special categories of personal data may be processed contrary to the general prohibition - Art. 9 (2) j
- **Information to be provided where personal data have not been obtained from the data subject**: data controllers may be exempted from their obligation to provide information to the data subjects - Art. 14 (5) b
- **Right to be forgotten**: data controllers may be exempted from their obligation to delete personal data - Art. 17 (3) d
- **Right to object**: Non-application of the right of objection if personal data are processed for scientific or historical research purposes and the processing is necessary for the performance of a task carried out for reasons of public interest - Art. 21 (6)
- All derogations **are subject to the condition**, that the **prerequisites and safeguards articulated in Recital 156 and stipulated by Art. 89 (1)** for the rights and freedoms of the data subjects are established

Part IV - Questions

Questions?

Contact details

Dr. iur. Robert Weniger
Delegate for Data Protection of the UZH
Stampfenbachstrasse 73
CH-8006 Zürich
Phone: +41 44 63 40177
E-Mail: robert.weniger@uzh.ch
Web: www.dsd.uzh.ch