Bringing Data to Life: Data Management for a better patient care

MAŠA KOJIĆ, MLAW, PHD CANDIDATE AT THE UNIVERSITY OF ZURICH

Universität Zürich[UZH]

Content

Introduction to Data Management

- Data Management lifecycle
- Data Management goals
- Data Management principles
- Data standards & procedures

Regulatory compliance

Europe vs. USA Data Protection legislation

iPC project and relevant legal issues according to the GDPR

- Key data protection roles
- Cloud Platform ⟶ Controller or Processor?
- Rights of the data subjects

GDPR compliance according to the Data Management lifecycle

Universität Zürich[UZH]

Data Management

What?

Who?

Why?

Introduction to Data Management

What is Data Management?

What are the key principles and components of Data Management?

What are the characteristics of data quality?

What is required for successful Data Management? *(e.g. technical infrastructure, policy & commitment, human infrastructure, Data Management Plan, etc.)*

What are the challenges of Data Management? *(i.e. how to make sense of collected data)*

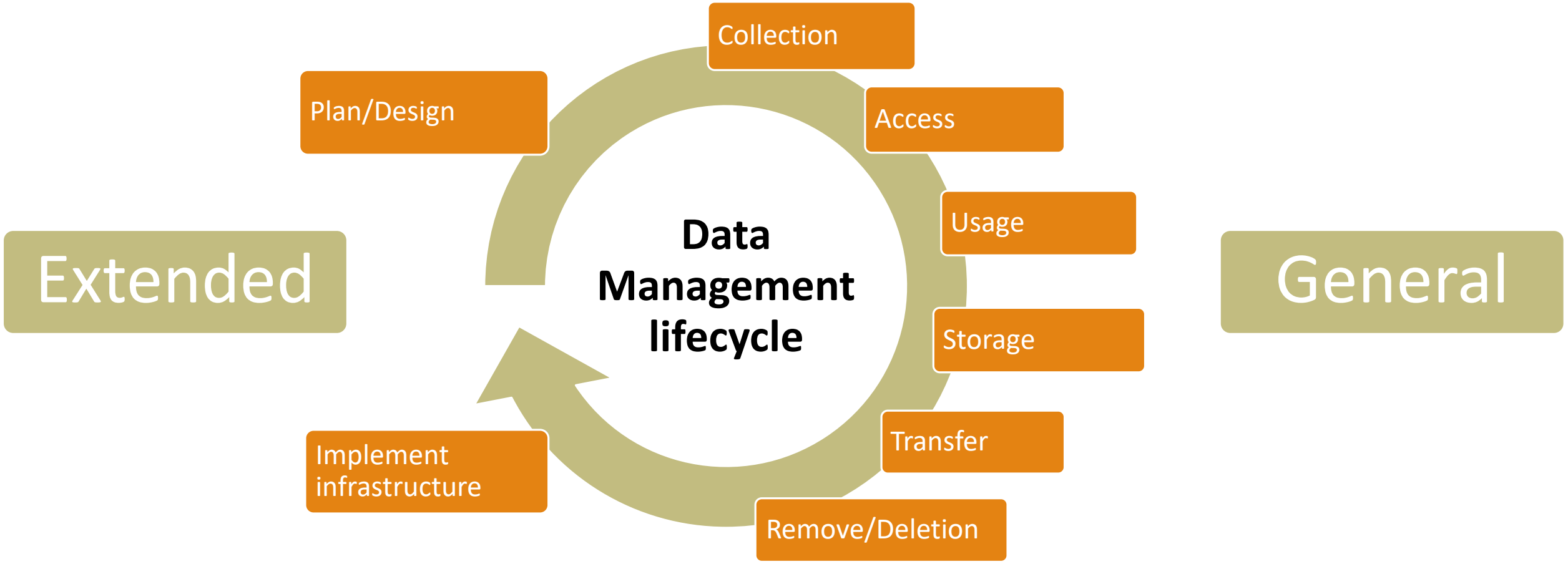
What are the best practices of Data Management? (*i.e. where should we strive)*

Who are the main actors within Data Management?

Why Data Management is important?

Universität Zürich[UZH]

Data Management lifecycle



Data Management goals

- primary goals -

- Understanding information needs
- Data Integrity
- Data Quality
- Data Security
- Effective use and value

- secondary goals -

- Control of Costs
- Understanding the value
- Information Management
- Allign with Platform Needs

Data Management principles

…policy

…ownership

…documentation and metadata compilation

…quality, standardisation and harmonisation

…lifecycle control

…stewardship

…access and dissemination

…audit

Data standards & procedures

Naming standards

Specification standards

Data modeling standards

Database design standards

Architecture standards

Procedural standards

(for each data management function)

Regulatory compliance
- relevant laws -

Switzerland (*Federal Data Protection Act , planned amendments, cantonal DPAs, Federal Act regarding Research on Humans, Federal Act on Human Genetic Testing, Federal Ordinance on Health Insurance, Federal Electronic Patient Records Act*)

EU (*European Convention on Human Rights and Fundamental Freedoms, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Convention ETS 108) and its additional protocol of 8 November 2001, GDPR*)

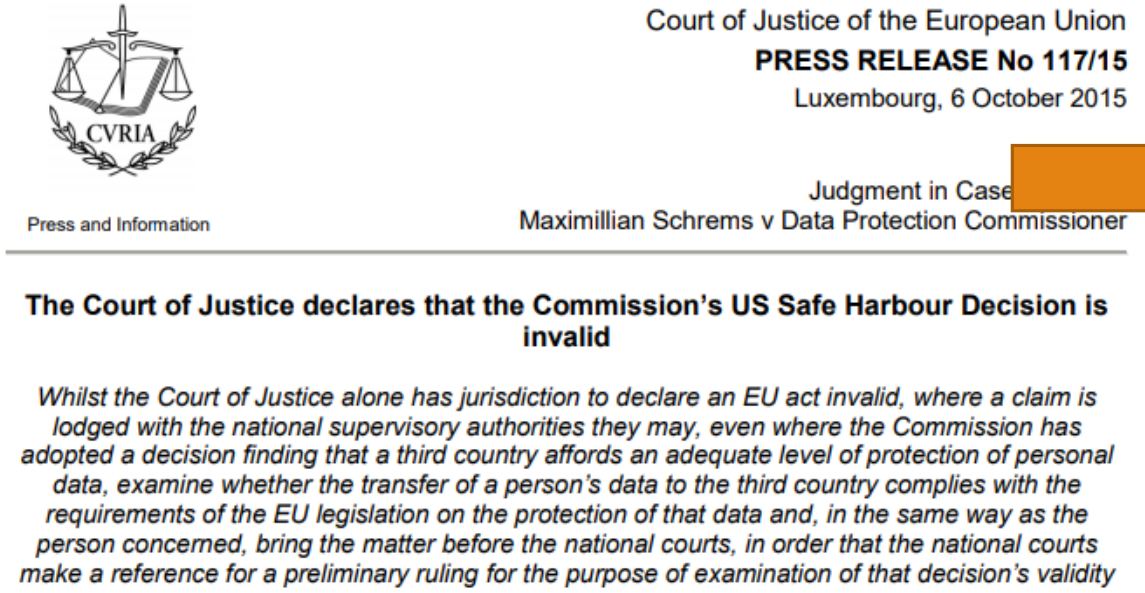
USA (*no central federal level privacy law, several vertically-focused federal privacy laws, as well as a new generation of consumer-oriented privacy laws coming from the states, instead, HIPAA*)

Australia (*Privacy Act 1988 Act No. 119 of 1988 as amended, Australian Privacy Principles, Privacy Regulation 2013*)

Europe vs USA
Data Protection legislation

The European Union's (*current*) approach to data privacy legislation (GDPR)

Data privacy legislation in the USA (HIPPA)



Court of Justice of the European Union
PRESS RELEASE No 117/15
Luxembourg, 6 October 2015

Press and Information

Judgment in Case
Maximillian Schrems v Data Protection Commissioner

The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid

Whilst the Court of Justice alone has jurisdiction to declare an EU act invalid, where a claim is lodged with the national supervisory authorities they may, even where the Commission has adopted a decision finding that a third country affords an adequate level of protection of personal data, examine whether the transfer of a person's data to the third country complies with the requirements of the EU legislation on the protection of that data and, in the same way as the person concerned, bring the matter before the national courts, in order that the national courts make a reference for a preliminary ruling for the purpose of examination of that decision's validity

iPC project and relevant legal issues according to the GDPR

Data Controler – who is the Data Controllor? What responsibilities it has?

Data Processor? – who is the Data Processor? What responsibilities it has?

Data Subjects? – who are the data subjects?

Data Protection Officer? Needed?

DPA? Needed?

Rights of the data subjects

Issues to think about:

- Necessary Platform Policies
- Platform – third parties relationship
- What about incidental findings?
- What about genetic data and impact on others?

Key data protection roles

…the 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

Data Controller

Article 4(7) GDPR

Data Processor

Article 4(8) GDPR

…a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

… 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

Data Subjects

Article 4(1) GDPR

Data Protection Officer

Articles 37-39 GDPR

…ensure that her organisation processes the personal data of its staff, customers, providers or any other individuals in compliance with the applicable data protection rules

Cloud Platform

Controller or Processor?

Who owns the Platform?

Who operates the Platform?

Only determines the purposes and means of the processing of personal data?

Processing the personal data as well?

Are third parties engaged in processing of personal data?

Is Data Protection Addendum needed for the Cloud Platform?

Rights of the data subjects

Rights (Art. 12 – 22 GDPR)

Transparent information, communication and modalities for the exercise of the rights of the data subject

Information to be provided where personal data are collected from the data subject

Information to be provided where personal data have not been obtained from the data subject

Right of access by the data subject

Right to rectification

Right to erasure (‘right to be forgotten’)

Right to restriction of processing

Notification obligation regarding rectification or erasure of personal data or restriction of processing

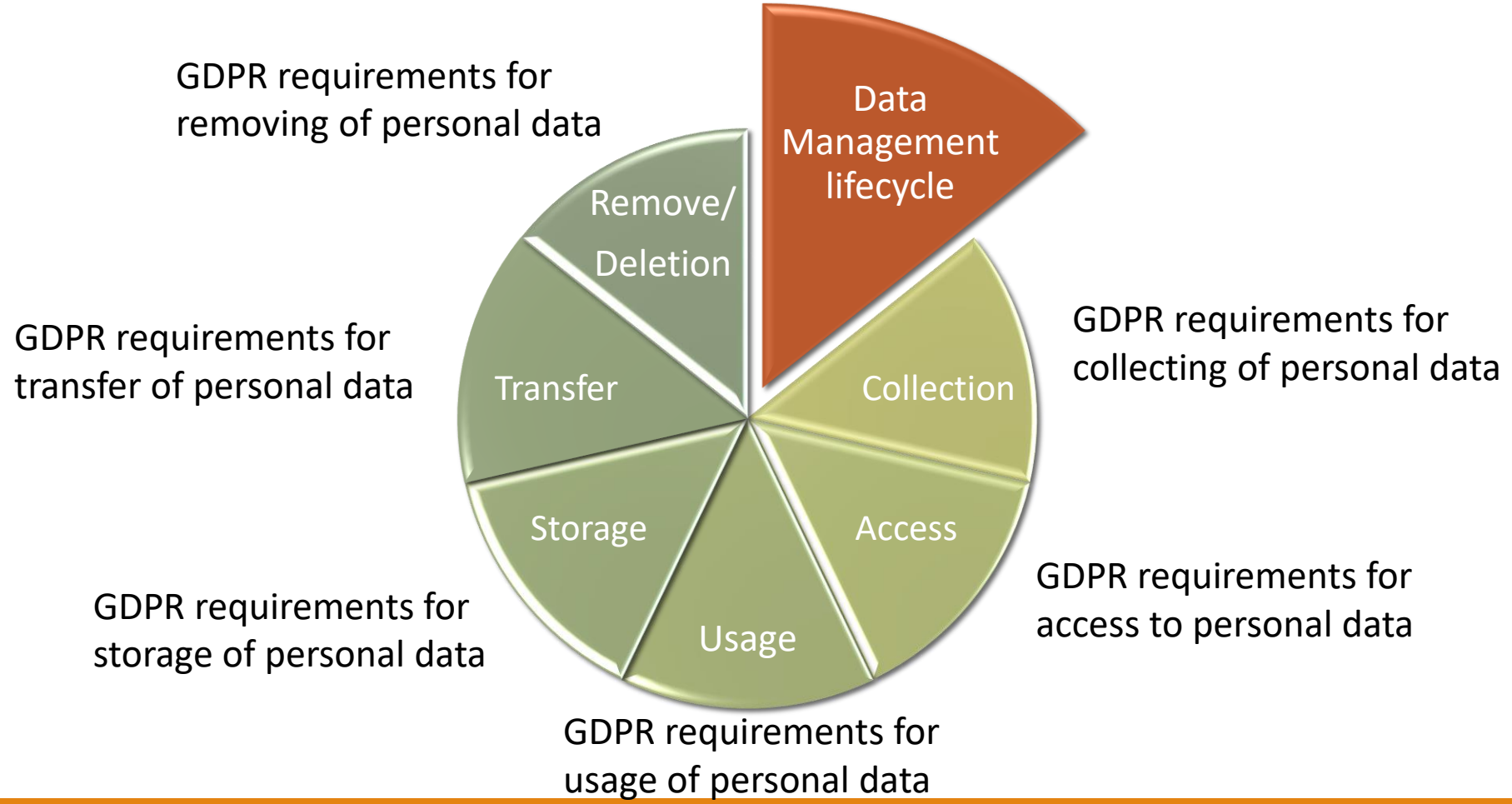
Right to data portability

Right to object

Automated individual decision-making, including profiling

Restrictions (Art. 23 GDPR)

GDPR compliance according to Data Management lifecycle



Issues to think about

- **Necessary Platform Policies** (access to the platform/information/content and access to the personal data → terms of use, terms of services…)
- **Platform – third parties relationship** (legal issues with regard to obtaining the data from third parties, f.e. hospitals, other databases…)
- **Incidental findings**?
  - Needed to be disclosed?
  - Legal or moral obligation?
  - To whom?
- **Genetic data**?
  - Ownership of genetic data?
  - Sharing of genetic data impacts others?

Key Points Summary

Cloud Platform

Controller & Processor

DPA

needed

DP Officer

needed

Rights of data subjects

to comply with

Collecting & Processing requirements

to comply with

THANK YOU FOR YOUR ATTENTION!

Contact: masa.kojic@uzh.ch