CHALLENGES OF ANONYMISED SHARING OF HEALTH DATA

Anna Zsófia Horváth LL.M.

Research Assistant

University of Goettingen, Institute for Business law

Chair of Civil Law, Commercial and Business Law, Comparative Law, Multimedia and Telecommunications Law

DATA PROTECTION OR DATA EXPLOITATION? LEGISLATIVE AND TECHNOLOGICAL LANDSCAPE

DATA PROTECTION

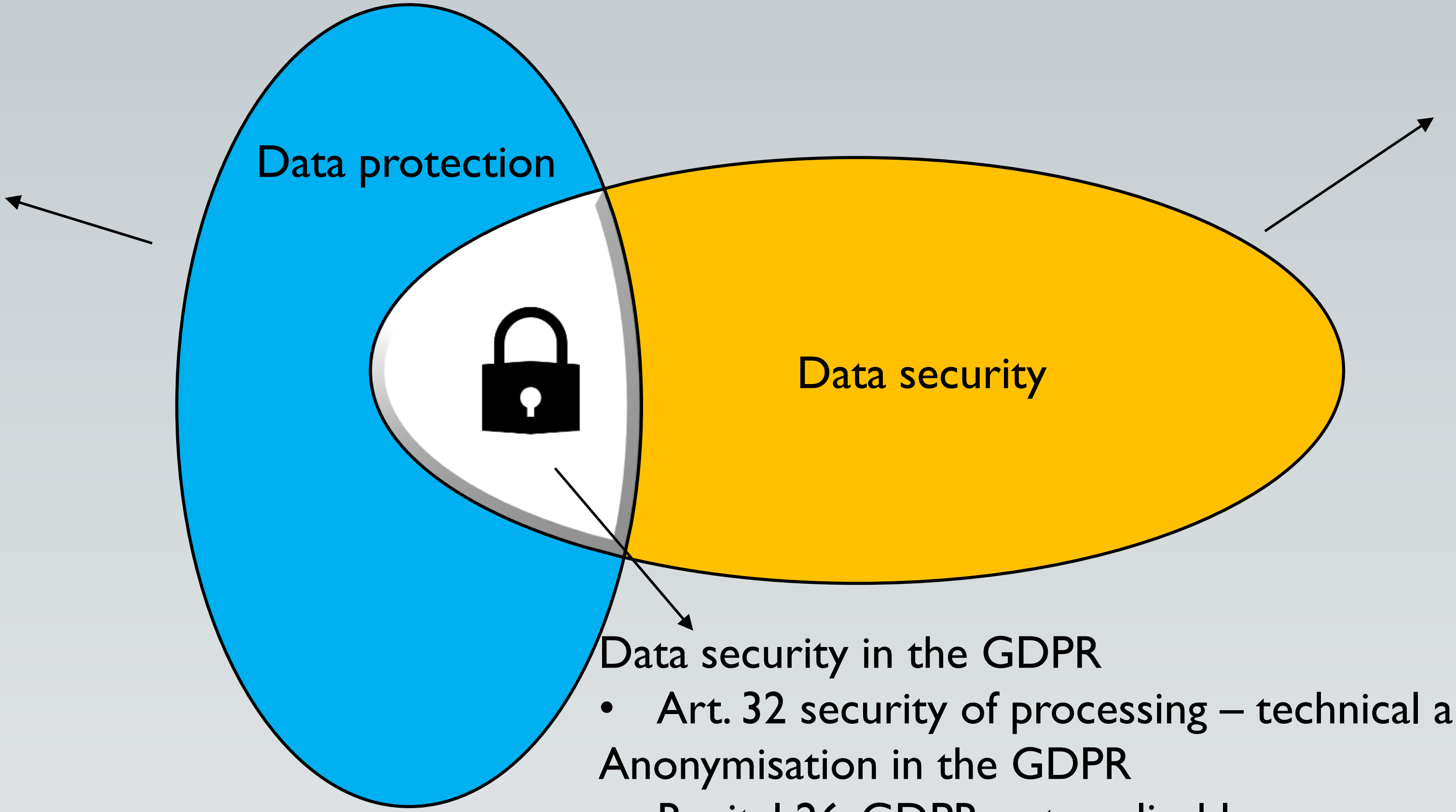
- right of informational self-determination
- risk of violation of fundamental rights
- GDPR:
  - stricter data protection requirements
  - draconian fines

BIG DATA

- Industry 4.0, enormous potential in research
- increase efficiency while reducing costs
- excessive regulation

ANONYMISATION IN THE DATA PROTECTION REGULATORY REGIME

- relationship between collection and dissemination of data
- legal underpinnings surrounding that data



- protecting data from destructive forces and unauthorised access
- confidentiality
- robustness

Data security in the GDPR

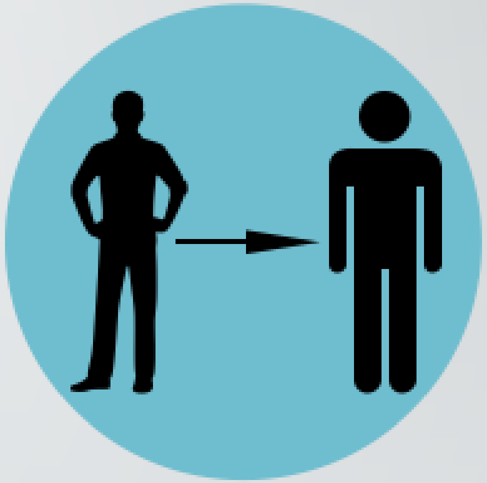
- Art. 32 security of processing – technical and organisational measures

Anonymisation in the GDPR

- Recital 26, GDPR not applicable

DEFINING ANONYMISATION I.

- **ISO** 15025237 on health informatics
  - process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party
- **Free medical dictionary**
  - „data from which the patient cannot be identified by the recipient of the information"



DEFINING ANONYMISATION II.
LEGAL STANDPOINT

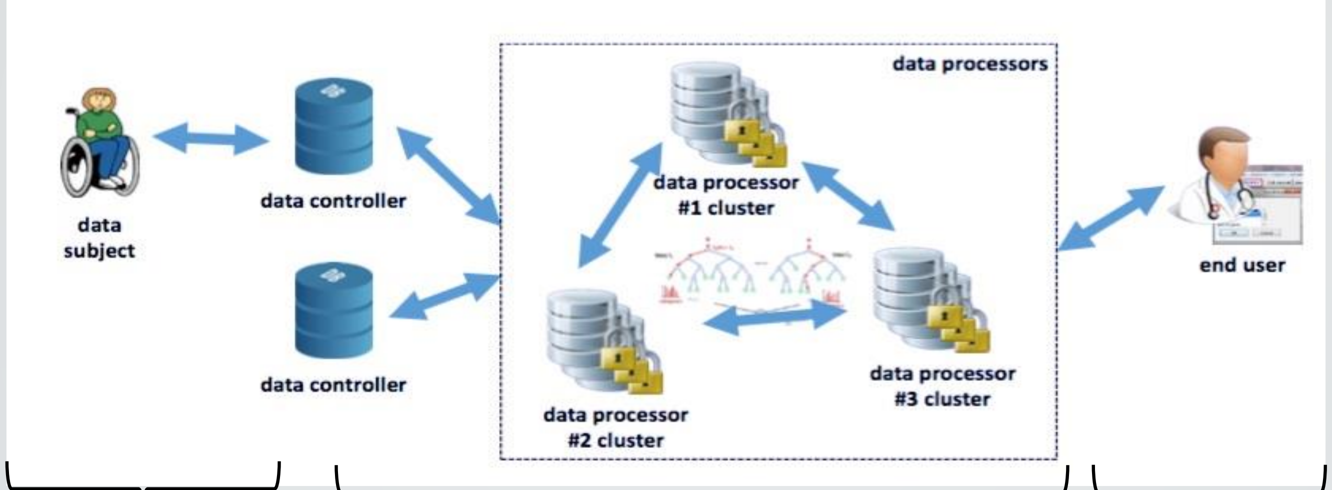
- GDPR does not define anonymisation / anonymous data
- Personal Data – Art. 4 Nr. 1
  - any information relating to an identified or *identifiable* natural person data without personal reference falls out of the GDPR‘s scope
- Question of identifiability
  - Absolute concept of identifiability
    - Anonymity only if all raw data has been deleted
  - Relative concept of identifiability
    - context-sensitive
    - additional knowledge necessary

DEFINING ANONYMISATION II.
GDPR

- 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”
    - costs
    - time
    - circumstances of any given processing
    - Indirect identification, e.g. by ”singling out".
  - Objective discretionary question
  - threshold of re-identification risk
  - no one-size fits all

ANONYMISATION THROUGH THE DATA LIFE CYCLE

data life span


data subject
data controller
data controller
data processors
data processor #1 cluster
data processor #2 cluster
data processor #3 cluster
end user

acquisition

analysis

Anonym, if no means reasonably likely to be used for re-identification

application

Anonym, if protected against: singling out, linkability, inference

FOUNDATION OF DATA ANONYMISATION I.

- Define the key concepts
  - data type
  - data processing setting
- Identify and anticipate risks
  - evaluate data protection and privacy situation
  - analysis and control of risks
  - impact management
- Map state-of-the-art
  - compare and assess already existing methods and best-practices

FOUNDATION OF DATA ANONYMISATION II.

- Factors to be taken into account:
  - Right algorithm
    - assurance of suitability
  - Right key size
    - sufficiently large to ensure that an attack remains a practical impossibility
    - over the entire lifetime of the data
  - Secure key management
  - Appropriate level of aggregation

- State of the art anonymisation in a technical sense
- anonymisation in a legal sense

SOLUTION APPROACH

relative anonymity, removal of personal reference

Context specific risk assessment

Application of appropriate methods of anonymisation and technical and organisational measures

Regular review, continuous evaluation, comprehensible documentation

THANK YOU FOR YOUR ATTENTION!