EL2: European legislation

GDPR, EHDS and DA

Legal part

- Today: European legislation (mainly GDPR!)
  - Lecture handouts main sourse for examination (seminair ES1 and possibly DISA exam).
  - Article [1]. Focus on the introduction, the section "GDPR-related enablers and barriers to cross-country health data exchange in Europe" (in the results section incl. figures and tables), discussion and conclusions. Examined as part of seminair ES1 (not the DISA exam).
- Next lecture: Swedish legislation (including associated reading). Examined as part of seminair ES1 (not the DISA exam).
- Consequence: [2, ch. 4]. Read the beginning. Skip "Medical Information Mart for Intensive Care". Read the "Synthea" section. The "Synthea" section does not have a legal focus but the legal parts explains why we use this data. Read for your own understanding (not examied).

European legislation

- **GDPR** (our focus)
  - Defines the legal conditions for **processing personal data**
  - Focuses on protection, safeguards, and accountability
- **European Health Data Space (EHDS)**
  - Establishes a European framework for access to health data for research, statistics, and policy.
  - Focuses on data access, governance, and interoperability
  - Increases opportunities for cross-national health statistics
- **EU Data Act**
  - Regulates who may access data and under what conditions, across sectors.
  - Indirectly relevant for health statistics through device-generated and digital service data.

> ! Important
>
> Legal and governance frameworks enable access to data, but **statistical expertise remains essential** for ensuring data quality, valid inference, and meaningful interpretation.

EU law vs Swedish law

- EU legislation tends to be more detailed in the legal text itself
- This is because EU law must be:
  - applied uniformly across many different legal systems
  - interpreted without relying on national preparatory works
- Interpretation of EU law relies mainly on:

    - the wording of the legislation
    - recitals (non-binding explanaitions before the articles describing the purpose and context).
- Swedish legislation is often:
    - shorter and less detailed in the statutory text
    - supplemented by extensive **preparatory works (förarbeten)**
- In Sweden, preparatory works are a central interpretative source for courts and authorities

➡️ The difference reflects **different legislative techniques**, not necessarily a difference in regulatory ambition.

> ℹ Source
>
> The GDPR is available in all official EU languages via EUR-Lex. Take a quick look to get a very brief overview. However, it is recommended reading only if you suffer from insomnia — it is not required for fulfilling the course requirements!

GDPR

- Regulation (EU) 2016/679 (GDPR)
- Enforced since May 25, 2018
- Regulates the **processing** of **personal data**
- Aims to protect the privacy and rights of individuals
- Sets out rules for data **controllers** and **processors**

European Union (EU)

- GDPR applies **directly and uniformly** as law
- No national implementation required
- Member States may:
    - introduce **supplementary legislation**
    - allow legal exceptions, e.g. for:
        - research
        - public interest
        - health data

European Economic Area (EEA)

Countries: Norway, Iceland and Liechtenstein

- GDPR applies via the **EEA Agreement**
- Implemented into national law
- In practice:
    - very similar application as within the EU
    - same core principles, rights, and obligations

United Kingdom (UK)

- EU GDPR no longer applies directly after Brexit
- Replaced by:
  - UK GDPR
  - Data Protection Act 2018

Switzerland

- Not part of EU or EEA
- GDPR does **not** apply as law
- Instead: Federal Act on Data Protection (FADP)
  - Revised to align closely with GDPR

International laws

- Note that other countries have different laws and regulations
- In USA, for example, HIPAA regulates the use and disclosure of protected health information (PHI)
  - Different states have different laws as well
- When collaborating internationally, compliance with all relevant laws is required

Definitions

GDPR article 4:

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.

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;

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;

Controller

means 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 [...]

Processor

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

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;

Personal data breach

means a breach of security leading to the accidental or unlawful destruction, loss, alteration, **unauthorised disclosure of, or access to, personal data** transmitted, stored or otherwise processed;

Data concerning health

means personal data related to the **physical or mental health** of a natural person, including the provision of **health care services**, which reveal information about his or her health status;

Legal grounds for processing personal data:

GDPR article 6 (1):

Processing shall be lawful only if and to the extent that at least one of the following applies:

a. the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes; ~~processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;~~
b. ~~processing is necessary for compliance with a legal obligation to which the controller is subject;~~
c. ~~processing is necessary in order to protect the vital interests of the data subject or of another natural person;~~
d. 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;
e. 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.
f. ~~processing is necessary for compliance with a legal obligation to which the controller is subject under Union or Member State law requiring the processing of personal data for a specific purpose.~~

Legal ground (d) is the most relevant if you work iwith secondary data in the public sector (research and reporting etc). (a) is relevant to collect primary data for research etc. (e) is a delicate one ...

Processing of special categories of personal data

GDPR Article 9 (1):

> Processing of 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**. 😱

But ...

> Paragraph 1 shall not apply if one of the following applies:

- (a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes [...]
- (i) processing is necessary for reasons of **public interest** in the area of **public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices [...]
- (j) processing is necessary for archiving purposes in the public interest, **scientific** or historical research purposes or **statistical purposes** (🥳) in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Safeguards

GDPR article 89:

> Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or **statistical purposes**

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or **statistical purposes**, shall be subject to **appropriate safeguards**, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that **technical and organisational measures are in place** in particular in order to ensure respect for the principle of **data minimisation**. Those measures may include **pseudonymisation** provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or **statistical purposes**, Union or Member State law may provide for derogations [...] so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

Technical Safeguards

Examples of technical safeguards include:

- Pseudonymisation
- Encryption of personal data
- Access controls and authentication
- Logging and monitoring of access
- Secure storage and transmission
- Use of secure software environments often enforced by organizational standards

Organisational Safeguards

Examples of organisational safeguards include:

- Defined roles and responsibilities
- Internal policies and procedures
- Staff training and confidentiality obligations
- Data protection by design and by default
- Incident and breach response procedures
- Documentation and accountability measures
- Working for a health care organization might require an agreement of secrecy

Data Minimisation and Purpose Limitation

- Only data that are **necessary** should be processed
- Data are processed **only for specified purposes**
- Access is limited to authorised personnel
- Retention periods are defined and respected

Pseudonymisation and Anonymisation

- **Pseudonymisation** reduces risks while allowing reuse of the data
  - Identifiers are kept separately and protected
- **Anonymisation** removes data from GDPR scope (if irreversible)

> ! Important
>
> - Pseudonymisation $\neq$ Anonymisation
> - Removing the Swedish personal identification number (PIN) is not a guarantee for pseudonymisation

Data Controller

- The entity that **determines the purposes and means** of the processing of personal data
- Bears the **primary legal responsibility**
- Responsible for:
  - Lawful basis
  - Compliance with GDPR principles
  - Transparency and information to data subjects
  - Appropriate technical and organisational measures
- Typical examples:
  - Public authorities
  - Universities
  - Regions and municipalities

Data Processor (PUB) under GDPR

- Processes personal data **on behalf of the controller**
- Acts **only on documented instructions** from the controller
- May **not** determine purposes of processing
- Has direct responsibilities for:
  - Security of processing (Article 32)
  - Confidentiality
- Must be governed by a **data processing agreement**

Controller–Processor Relationship

- A formal **Data Processing Agreement (DPA)** is required
- The agreement must specify:
  - Subject matter and duration
  - Nature and purpose of processing
  - Types of personal data
  - Categories of data subjects (patients, students, citizens, …)
  - Security measures
- The controller remains responsible even when processing is outsourced

Example: Sahlgrenska

- If a researcher work at the Sahlgrenska university hospital, VGR might be the data controller (personuppgiftsansvarig; PUA)
- If he/she asks for statistical consulting from the Sahlgrenska Academy, GU might be the data processor (personuppgiftsbiträde; PUB)

European Health Data Space (EHDS)

What is it?

- EHDS is an EU-wide legal and technical framework for the use and sharing of health data
- It aims to:

    - improve access to health data across borders
    - support healthcare, research, **statistics**, and policy-making
- Focuses on data access and governance

Two Main Pillars

- Primary use of health data
    - Use of data for individual patient care
    - Cross-border access to electronic health records
- Secondary use of health data for
    - statistics
    - scientific research
    - public health
    - policy evaluation and innovation

Implementation Timeline

- **2025**: EHDS regulation enters into force
- **2025–2027**: Development of implementing and technical acts
- **From ~2029 onwards**:
    - national infrastructures become operational
    - cross-border access for secondary use starts to function in practice

How EHDS Relates to GDPR

- EHDS does **not replace GDPR**
- GDPR continues to govern:
    - personal data protection
    - lawful bases
    - safeguards for health data
- EHDS provides **procedures and structures** for lawful data access under GDPR

➡️ GDPR defines *whether* data may be processed

➡️ EHDS defines *how* data can be made available

Why EHDS Matters for Statisticians

- EHDS explicitly recognises **statistics** as a legitimate purpose
- It facilitates access to:
    - large-scale health datasets
    - cross-national data sources
- It increases demand for:
    - data quality assessment
    - metadata interpretation
    - harmonisation and comparability analyses

EHDS Does *Not* Do This

- EHDS does not:

  - define statistical methods
  - ensure data quality automatically
  - guarantee comparability across countries
- Legal and technical access ≠ valid statistical inference

EU Data Act

What Is It?

- The Data Act is an EU regulation on access to and sharing of data
- Focuses mainly on:
  - data generated by connected products and digital services (IoT)
  - business-to-business (B2B) and business-to-government (B2G) data sharing
- It is **not a data protection regulation**

➡️ The Data Act is about *who may access data and under what conditions.*

How the Data Act Relates to Health Data

- The Data Act does not primarily target health registers
- However, it may affect:
  - data generated by medical devices
  - digital health services
  - health-related IoT data

➡️ Health data may fall under the Data Act depending on how it is generated.

Bibliography

[1] J. Vukovic, D. Ivankovic, C. Habl, and J. Dimnjakovic, "Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective," *Archives of Public Health*, vol. 80, no. 1, p. 115, Apr. 2022, doi: 10.1186/s13690-022-00866-7.

[2] A. Nguyen, *Hands-on healthcare data: taming the complexity of real-world data*, First edition. Beijing Boston Farnham Sebastopol Tokyo: O'Reilly, 2022.