PROTECTION OF PERSONAL DATA

Introduction to GDPR

Certain aspects of protection of personal data in the health sector

GDPR

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**)

- Repealing Directive 95/46/EC

SCOPE OF GDPR

- Material: 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

- Territorial:
  - activities of an entity established in the Union, regardless of whether the processing takes place in the Union or not
  - activities of an entity established outside the EU, processing data of data subjects in the EU in the context of offering products or services in the EU or monitoring behavior of data subjects in the EU

- Does not apply to:
  - data of deceased people
  - anomymized data

PERSONAL DATA

- Any information relating to an identified or identifiable natural person
- Identifiable person = can be identified, directly or indirectly, by one or more factors specific to their identity
- name, an identification number, location data, factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity

PROCESSING

- 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

DATA PROTECTION PRINCIPLES

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- accountability

WHEN IS PROCESSING LAWFUL?

- Consent given by the data subject
- Processing based on the necessity to fulfill a contract
- Compliance with a legal obligation
- Vital interest of the data subject
- A task carried out in the public interest or in the exercise of official authority vested in the controller (on the basis of EU or National law)
- 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. (weighing of interests)

SPECIAL CATEGORIES OF PERSONAL DATA

Processing of personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- health
- sex life or sexual orientation

is **FORBIDEN!**

SPECIAL CATEGORIES OF PERSONAL DATA DEROGATIONS:

- consent
- carrying out rights and obligations under employment and social security and social protection law;
- vital interests of the data subject
- personal data of members
- data manifestly made public by the data subject
- establishment, exercise or defence of legal claims
- necessary for reasons of substantial public interest
- necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

SPECIAL CATEGORIES OF PERSONAL DATA DEROGATIONS:

- processing is necessary for the purposes **of preventive or occupational medicine**, for the assessment of the working capacity of the employee, **medical diagnosis**, the **provision of health or social care or treatment** or the **management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional
- 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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

CONSENT

- Freely given, which implies a real choice and control for data subjects.
- Specific, the purpose must be clear and covered by the consent.
- If the consent is given for more specific purposes, the data subject must have a choice in relation to each of them.
- Informed, meaning an appropriate notice on how the personal data are processed is provided.
- Unambiguous indication of the data subject's agreement to the processing of personal data relating to him/her.
- To be given through affirmative action.
- In addition, consent for processing health data must be explicit (Art.9).

CONTROLLER AND PROCESSOR

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

- Processors must provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of GDPR and ensure the protection of the rights of the data subject

- Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller.

JOINT CONTROLLERS

- Two or more controllers jointly determine the purposes and means of processing.
- They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under GDPR, by means of an **arrangement** between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law.
- The essence of the arrangement shall be made available to the data subject.
- The data subject may exercise his or her rights under GDPR in respect of and against each of the controllers.

DATA PROTECTION IMPACT ASSESSMENT

- Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a **high risk** to the rights and freedoms of natural persons
- By the controller prior to the processing
- In particular be required in the case of:
  - a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing
  - processing on a large scale of special categories of data
  - a systematic monitoring of a publicly accessible area on a large scale
- Lists of the kind of processing operations requiring DPIA published by supervisory authorities

THANK YOU FOR YOUR ATTENTION!