The General Data Protection Regulation

Opportunities and challenges for IHE

Petra Wilson

Health Connect Partners
supporting trust in data

IHE Symposium
17th April 2018
The Hague

Do you process personal data ?

- **Any information**
- **relating to**
- **an identified or identifiable**
- **natural person**

Art 4 - definition & Art 29 Committee Guidance

General personal data

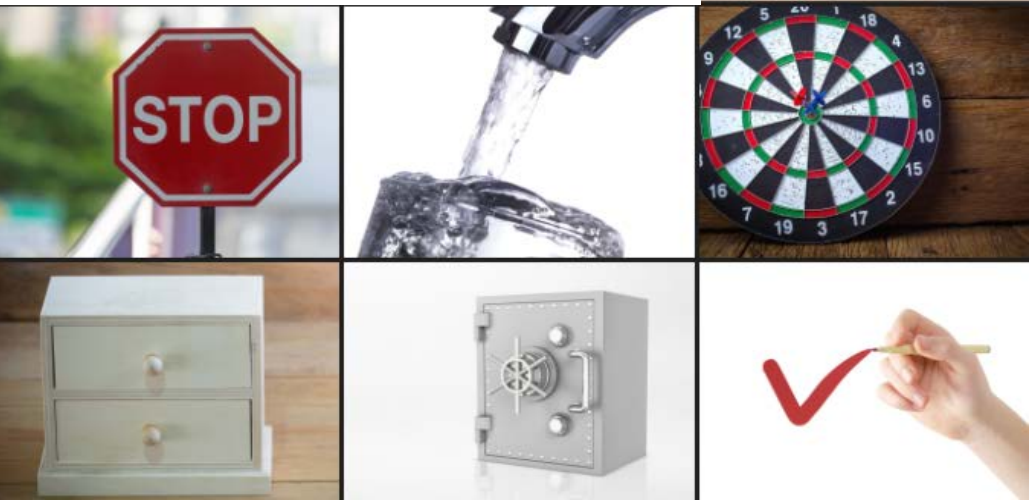
Organisational personal data

Are you the Controller or Processor?

Controller: Natural or legal person, Alone or jointly with others, Determine the purposes and means of the processing

Processor: Natural or legal person, Processes personal data on behalf of the controller

Seven principle of lawful data processing



- Lawful, fair and transparent
- For specified and explicit purposes
- Adequate, relevant and limited to the stated purpose
- Accurate & kept up to date
- Stored only for as long as necessary
- Processed securely
- Accountable controller and processor

LEGITIMATE BASES FOR PROCESSING

- Processing is only lawful if:
  - Data subject has given **consent**
  - Necessary for the performance of a **contract** or to take steps prior to entering into a contract
  - Necessary for compliance with **legal obligation** to which the controller is subject
  - In order to protect **vital interests** of a person
  - Necessary for **public interest** or **official authority**
  - For the **legitimate interests of controller**/3rd party

PROCESSING OF SPECIAL CATEGORIES

Prohibited unless:

- Data subject has given **explicit consent**
- Necessary for obligations/exercising rights in **employment/social security/social protection**
- In order to protect **vital interests** of a person
- For **political, philosophical, religious, trade-union** foundation/association/not-for-profit body
- Data **manifestly made public** by data subject

- **Necessary for establishment/exercise/ defence of legal claims**
- **Necessary for substantial public interest (under EU or MS law)**
- **Necessary for preventive or occupational medicine, assessment of working capacity, medical diagnosis, or healthcare**
- **Necessary for reasons of public interest in public health**
- **Necessary for archiving, scientific/ historical research or statistical purposes**

Further conditions by Member States for genetic data/biometric data/health data

Rights of the Data Subject

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to data portability
- The right to restrict processing
- The right to object
- Rights in relation to automated decision making and profiling.

Right to Information, Access, Rectification and Erasure (Right to be Forgotten)

What can the data subject demand?

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice
- Correction of any information that is incorrect
- Erasure of specified data

What duties does the controller /processor have?

- Provide access free of charge – unless excessive
- within one month of request - extension to two months is possible
- Rectification or erasure must be informed to third parties

When can the controller refuse erasure

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; the exercise or defence of legal claims.

Right to Portability

What can the data subject demand?

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.
- Available to data subjects when data was collected on the basis of consent or contract and is carried out by automatic means.

Right to Object or Restrict

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

Individuals have a right to 'block' or suppress processing of personal data.

- When processing is restricted, you are permitted to store the personal data, but not further process it.

Accountability

Compliance

Enforcement

ACCOUNTABILITY

- Implementation of **data protection policies**
- Data protection **by design** and data protection **by default**
- **Implement data security measures**
- **Record keeping** obligations (by controllers and processors)
- Undertake data protection **impact assessments**
- **Co-operation** with supervisory authorities (by controllers and processors)
- **Appoint Data Protection Officers** (for controllers and processors)

Compliance: Data Protection by design & by default

- Implement appropriate measures (e.g. pseudonymisation) designed to support data protection principles (e.g. data minimisation)
- Implement appropriate measures to ensure that only necessary personal data is processed

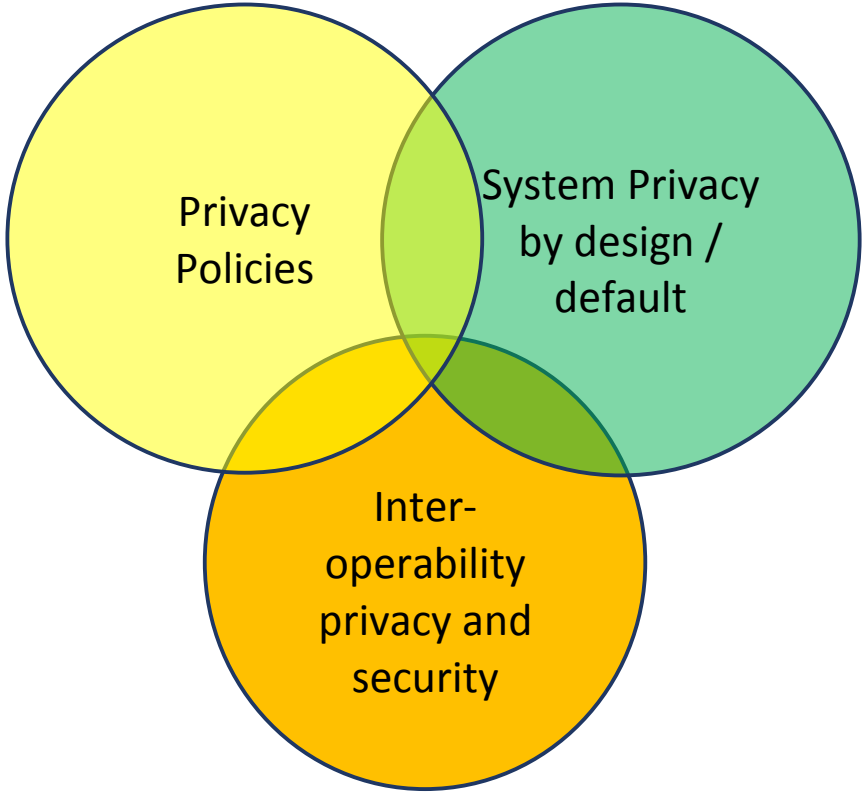
- Devise mechanism to ensure that:
  - ✓ Data protection by design, and
  - ✓ Data protection by default are taken into account at the development stage (i.e. data protection impact assessment)
- Devise compliance programme to implement identified measures during data protection impact assessment

Compliance:
Implement appropriate security measures

- Appropriate technical and organisational measures including:
  - Pseudonymisation and encryption
  - Ongoing confidentiality, integrity, availability and resilience
  - Ability to restore
  - Process for testing

- Notification of personal data breach to supervisory authority not later than 72 hours after having become aware, unless unlikely to result in a risk
- Communication of personal data breach to the data subject if high risk

How does GDPR influence the use of IHE profiles?



Can IHE help in facilitating the adoption of GDPR?

What already exists?

- BPPC and APPC - on patient consent
- ATNA - on access logging
- XUA and X.509 certificates - authentication

http://www.ihe-europe.net/sites/default/files/2018-05/IHE-Europe-GDPR White Paper-2018.pdf

But there is still work to be done

Thank you

petra@hcp.partners

Health Connect Partners
supporting trust in data