Data protection in eHealth: what to keep in mind

Fundamental Rights Forum, 22 June 2016

WG 24: E-health: improving rights fulfilment through innovation

Claudia Prettner,

Unit for Health and Well-Being, DG CONNECT

Legal framework applicable

- Data Protection Directive 95/46/EC
- General Data Protection Regulation (EU)2016/679 "GDPR" (applicable as of 25 May 2018)
- Applying to the processing of personal data (including pseudonymised data)

Right to personal data protection

- Article 8, Fundamental Rights Charter
- Article 16, Treaty on the Functioning of the European Union
- GDPR: reinforces citizens' right to personal data protection while also ensuring a free flow of data between the Member States

Data protection principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Data protection by design and by default

"eHealth data" = sensitive data

- Health data: *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.*
  - data collected in a medical context;
  - data that allows to draw conclusions about a person's health status;
- Biometric data
- Genetic data

Health Data – provisions for processing

Processing of sensitive data in principle prohibited, unless derogation, for instance:

- explicit consent
- reasons of substantial public interest
- for medical/healthcare purposes
- necessary for research purposes with appropriate safeguards

Thank you!

claudia.prettner@ec.europa.eu