GDPR in a Nutshell

IMOTIONS

What is this about?

- May 25th 2018: EU General Data Protection Regulation (GDPR)
- Other regulations:
  - Act on Processing of Personal Data (persondataloven)
  - Public administrations:
    - Executive Order on Security
    - ISO27001 (since 2014)
  - Research: Act on Research Ethics (specific guidance on health projects)

DATATILSYNET

NVK
NATIONAL
VIDENSKABSETISK
KOMITÉ

GDPR

- Increased data subject rights
- Data subjects inside the EU (regardless of where processing occurs)

- Data controllers (principal responsible party)
- Data processors (on behalf of controller)
  - ‘data processing agreements’
- Penalties (up to 4% of annual turnover)

(Source: https://www.gdpreu.org/)

What is Personal Data?

- any information
- relating to
- an identified or identifiable
- natural person

(more specific national laws might apply)

Personal Identifiable Information (PII)

(Source: Article 29, Data Protection Working Party: Opinion 4/2007 on the concept of personal data)

IMOTIONS cachet Copenhagen Center for Health Technology

What is Personal Data?

Any information:

- subjective or objective
- need not be true
- not only ‘sensitive’ data
- in whatever form (digital, paper, …)

(Source: Article 29, Data Protection Working Party: Opinion 4/2007 on the concept of personal data)

What is Personal Data?

Relating to:

- an individual or objects they own
- for it to 'relate' to an individual
  - content element ('about')
  - or, purpose to evaluate or influence an individual
  - or, results in an impact on rights or interests of an individual

(Source: Article 29, Data Protection Working Party: Opinion 4/2007 on the concept of personal data)

What is Personal Data?

Identified or identifiable:

- able to distinguish from other members of the group
  - directly
  - indirectly (by combining information)
- depends on context
  - more than mere hypothetical possibility
  - likely to be used (cost, purpose, risk)

(Source: Article 29, Data Protection Working Party: Opinion 4/2007 on the concept of personal data)

What is Personal Data?

Natural person (also depends on national legislation):

- living individuals
- no legal persons (businesses)

(Source: Article 29, Data Protection Working Party: Opinion 4/2007 on the concept of personal data)

Consent

- Processing is only allowed when:
  - Consent
    - ≠ informed consent for health projects
    - Freely given, legible, purpose specific
    - by ‘clear affirmative action’
  - Required
    - contract
    - legal obligation
    - protect vital interests
    - task in public interest

(Source: “The ABC of GDPR: How General Data Protection Regulation will affect your organization” by Tieto)

Principles (context is key!)

- Purpose binding (only for one purpose)
- Data minimization (drop data when no longer needed for specified purpose)
- Transparency and openness (e.g., breach notifications)
- Information security (confidentiality, integrity, availability, portability)
- Accountability (internal and external auditing)

(Source: "The ABC of GDPR: How General Data Protection Regulation will affect your organization" by Tieto)

Rights of the Individual

- Access (a copy, *data portability*)
- Rectify (inaccurate or incomplete)
- Block (restrict processing) and erase

  (purpose fulfilled, consent withdrawn, …)
- Withdraw consent (for new data)

(Source: “The ABC of GDPR: How General Data Protection Regulation will affect your organization” by Tieto)
(Source: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)

Public Administrations and Research

Processing outside of EU is allowed:

- E.g., Amazon Web Services is working to be GDPR compliant

Specific to Denmark:

- Approval needed for public administrations
  - subject to change (e.g. from national to local regions, data protection officer)
- Measures should be taken so that data can be disposed or destroyed in the event of war or similar conditions

cachet | Copenhagen Center for Health Technology

IMOTIONS

Technical University of Denmark DTU

REGION H The Capital Region of Denmark

CITY OF COPENHAGEN

UNIVERSITY OF COPENHAGEN

Privacy by Design

- Risk analysis needed to choose relevant strategies
  - Identify assets
  - Identify associated risks (likelihood / impact)
  - Implement measures for highest risks

(Source: “Privacy and Data Protection by Design — from policy to engineering” by ENISA)

Privacy by Design

- Data-oriented strategies
  - Minimize (only collect what is needed, e.g., anonymisation and pseudonyms)
  - Hide (e.g., encryption at rest/in transit, mix networks)
  - Separate (process in distributed fashion, store data separately)
  - Aggregate (information applies to multiple individuals)

(Source: “Privacy and Data Protection by Design — from policy to engineering” by ENISA)

Privacy by Design

- Process-oriented strategies
  - Inform (transparency)
  - Control (agency over data)
  - Enforce (privacy policy enforced by technical mechanisms)
  - Demonstrate (be able to prove compliance)

(Source: “Privacy and Data Protection by Design — from policy to engineering” by ENISA)