Privacy in research, not just a hiding game

Responsible conduct of research, data management and privacy

e.hoorn@rug.nl
In 2027 what will the most likely excuse be for not having verifiable results?

a. Somebody stole the laptop with all the data.
b. All European participants used their right to be forgotten.
Present danger for integrity when using personal data for research schizophrenia between perceived requirements on openness and responsibilities for personal data of participants.
Programme

• General Data Protection Regulation
• 3 steps in a learning model for transparency on legal and ethical issues
• Open data in Horizon2020 and the Data Protection Impact Assessment
GDPR

• **General** Data Protection Regulation: May 2018...big fines!
• Controller has to be able to demonstrate compliance
• Transparency for participants more important
• Derogations for research
• Challenges for research:
  • Harmonization in Europe and worldwide
  • Responsibilities of the board, support and researchers
  • In keeping with ethical standards
Instruments in the GDPR

• Needed at all times: technical and organisational protection measures to balance the rights and freedoms of the participants.

• How?

• Privacy by design

• Privacy Impact Assessment: an ‘early warning instrument’ to speak the same language in a multi-stakeholder assessment to design relevant measures.
Process: Asking the right questions...

Step 1: documentation of questions based on ethical peer assessment

Step 2: Data Management Plan with Privacy Impact Assessment

Step 3: insight in possibilities for FAIR data
Horizon 2020
FAIR Data Management Plan

• Findable
• Accessible
• Interoperable
• Reusable

And as open as possible...
Open access to research data

Open access as the default setting

But... projects can opt out at any stage if (among others) they are incompatible with:

- the need for confidentiality in connection with security issues
- rules on protecting personal data
Don’t opt-out, do a PIA!
A German method to do a PIA

• Preparation stage
  • Projecting the assessment: goals and scope
  • Standard data protection model
  • Target, actors, relevant legal requirements

• Evaluation stage
  • Identification of protection goals with stakeholders
  • Attacks and evaluation criteria

• Report and safeguards stage
  • Technical and organisation measures
Standard Data Protection Model

Typical measures to guarantee transparency:

• Documentation of:
  • procedures
  • **data flows** and the IT systems used
  • contracts

• Internal responsibility assignments
Thank you!
Read more:

- https://www.knaw.nl/nl/actueel/publicaties/ethische-en-juridische-aspecten-van-informaticaonderzoek