



## Data protection officer

### GDPR:

- Advising organisation on privacy issues
- Monitoring compliance to GDPR
- Contact for data protection authority
- Contact for participants
- Independent, protected position

## GDPR art 5.2

The controller shall be responsible for, and be able to demonstrate compliance with the GDPR principles relating to processing of personal data.

We have to prove compliance

3

## Data minimisation (art 5.1. c)

Documented arguments on the necessity of:

- Questionnaires used  
(Are all questions really needed for the purpose of the research project?)
- Variables (o.a. demographics) to be used  
You have to collect and process the variables in the least identifying form.  
Example: Do you really need full birth date? Can your question answered with a year range?

4

## Records of processing activities art 30

- Each research project is a processing activity
- Each research Project has a specific purpose
- Each research project needs to be recorded in the register of processing activities.
- VUmc solution: The researcher need a confirmation of registration before the METc accepts the research proposal
- Data protection officer uses register for compliance monitoring o.a. check around the end date of the project

5

## DPIA or PIA



Data Protection Impact Assessment or Privacy impact Assessment (art 35)

DPIA or PIA:

- Assessment of the risks when processing the data.
- Risks concerning a.o. subjects rights and security.
- Measures must be taken to mitigate the risks to acceptable levels.
- Obligatory when processing health data.
- Obligatory advice of Data Protection Officer.

6

## PIA

- Standard PIA like PIA Norea
- Time consuming, up to 2 hours
- Guidance DPO needed
- VUmc about 500 new research projects yearly

7

## 2 approaches

- Adapt short PIA
- PIA for standard research types

Adapt PIA Norea: stripped, only bare questions.

PIA for standard types

E.g. retrospective research with existing medical files

Situation known, one PIA Norea covers all similar research, coupled to measures for the risk mitigation

Questionnaire to determine similarity with standard research type

8

## Short PIA

- Takes less time compared with PIA Norea
- Can be done by researchers
- No guidance of DPO
- Not taken seriously enough: just part of the red tape
- Not coupled to measures for risk mitigation

9

## PIA for standard research types

- Full PIA, including advice DPO
- Just a short questionnaire to identify project type
- WP 29 Approved approach
- When not standard a full PIA must be done
- Time investment in standard PIA's

10

## PIA and METc

- Part of risk assessment done in wmo METC: information to participants, recruiting procedure, contracts
- PIA input for data management plan
- VUmc: also non-wmo proposals are tested.
- Future: integration registration, pia, METc questions, data management plan

11



12