UiO : USIT

Key legal requirements for research

- in the GDPR and Health research act

Lars Soligard
Legal advisor, USIT
Data Processing Officer, UIO

Agenda

- GDPR and the Health Research Act
  - Why privacy and data protection?
  - What is personal data?
  - Data protection principles
  - DPIA
  - Transfer of data to third countries
- Health Research Act
  - Organizing health research
  - Approval from REC

GDPR and the Health Research Act

- GDPR is the general law
- The Health research act is *lex specialis*
- When does the Health Research act apply?
  - medical and health research: activities carried out with scientific methodology to acquire new knowledge about health and disease, HRA § 2(1) c.f. § 4(1)(a)

- HRA § 2(2): «For the processing of data concerning health, the GDPR and the Personal Data Act apply, to the extent that nothing else follows from this Act»

- HReA § 5: The GDPRs is the main law for the processing of health data in health registers in the health sector

Why data protection?

- Human right, NC § 102, ECHR art. 8
  - Right to privacy and data protection
  - HRA § 5(2): The research must be based on respect for the research participants' human rights
- Data protection entails the ability to have control of our own personal data and knowledge of how it is used and by whom
- Purpose of the GDPR: allocate more responsibility to persons processing personal data, and giving the data subject more control
- Purpose of the HRA: promote good and ethically sound medical and health research

What is personal data?

- ... means *any information relating to* an *identified or identifiable natural person* ('data subject'), GDPR art. 4(1)
- CJEU: Should be interpreted broadly
  - «Relating»: *"where information by the reason of its content, purpose or effect, is linked to a particular person», see: Case C-XXX*
- name, date of birth and personal identification number, email address, photographs, health information, voice, behaviour, ip-address, assessments, scores

- **Personal data is all the information and assessments that can be linked to you, either directly or indirectly.**

Special categories of personal data (Art. 9)

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- data concerning health or
- data concerning a natural person's sex life or sexual orientation

Data concerning health and Genetic Data

- GDPR art. 4(15), HRA § 4(1)(d): Data concerning health: «personal data *related* to the physical or mental health of a natural person»
- GDPR art. 4(13): Genetic data: «personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person»

Pseudonymisation

- GDPR art. 4(5): the processing of personal data in such a manner that the personal data *can no longer be attributed to a specific data subject* without the use of *additional information*, provided that such additional information is *kept separately* and is *subject to technical and organisational measures* to ensure that the personal data are not attributed to an identified or identifiable natural person

- Basically: de-identified and anonymous for the researcher without the identifier
- Pseudonymised data is personal data

Anonymous information

- Anonymous information is information that cannot in any way be used to identify individuals in a data material, either directly by name or personal identification number or indirectly by additional information
- X, who is the prime minister of Norway...

Data subjects, processing, controller, processor

- Data subject: the natural person information relates to, GDPR art. 4(1)
- Processing: «any operation or set of operations which is performed on personal data or on sets of personal data», GDPR art. 4(2)
  - Basically all handling of data such as:
  - Collecting
  - Storing
  - Analysing
  - Deleting
  - Anonymising
  - Etc...
- Controller: determines the purposes and means of the processing of personal data
- Data Processor: processes personal data on behalf of the controller

GDPR in a nutshell…

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Principles relating to processing of personal data

- 10 principles which represent essential axioms within data protection legislation, see: GDPR art. 5
- fundamental to understanding the GDPR
- Once we are aware of the principles, we will have knowledge of the GDPR provisions
- The processing of data concerning health in medical and health research shall be in accordance with the principles of the GDPR Article 5, HRA § 38(1)

1) Lawfullness

- Processing of personal data must be lawful
- This means that we must base processing of personal data on minimum one of the conditions stated in the GDPR Article 6; legal basis
- Special categories also require that an exception pursuant to Art. 9(2)
- most important bases for processing of personal data for research are
  - 1) consent – 6(1)(a), 9(2)(a) - main legal basis in the HRA § 13
  - 2) a task carried out in the public intrest 6(1)(e), 9(2)(j)
    - Supplamentary legal basis PDA §§ 8 and 9, cf. GDPR art. 6(2)

Conditions for consent

(GDPR art. 7, HRA § 13(2))

- Freely given
- Specific
- Informed
- Unambiguous indication of the data subject's wishes

- We must be able to demonstrate that the data subject has consented to processing
- The data subject shall have the right to withdraw his or her consent at any time

2) Fairness and 3) Transparancy

- Fairness: We must not take advantage of our position
  - as a research institution, we must not take advantage of our position in relation to the data subjects
- Transparancy: The data subjects shall be informed of what we do with their personal data, and and of how to exercise his/her rights, GDPR art. 5(1)(a) and HRA § 39
- Important to provide the required information in a clear and plain language, see GDPR art. 13 and 14 cf. art. 12.

4) Purpose limitation

- Personal data shall be collected for *specific*, *explicit* and *legitimate* purposes and not further processed for other purposes than those for which they were collected
- ... further processing for ... scientific or historical research purposes ... shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes
- Data concerning health cannot be processed for purposes that are incompatible with the initial purpose without the research participant's consent, HRA § 32(2)
- Specific: “The purpose of processing personal data is to investigate whether x is y in relation to z”. Broad consent, HRA § 14
- Explicit: the purpose must be communicated to the data subject in such a way that the data subject understands what the purpose involves
- Legitimate: Entails an assessment of whether the purpose is lawful and ethically justifiable. REC approval, HRA §§ 9 and 10.

5) Data minimisation

- The amount of personal data shall be limited to that necessary to achieve the purpose of data processing
- We must avoid collecting, storing or in any other way processing personal data that is not strictly necessary, even if it may be “good to have”
- Obligation pursuant to HRA § 32

6) Accuracy

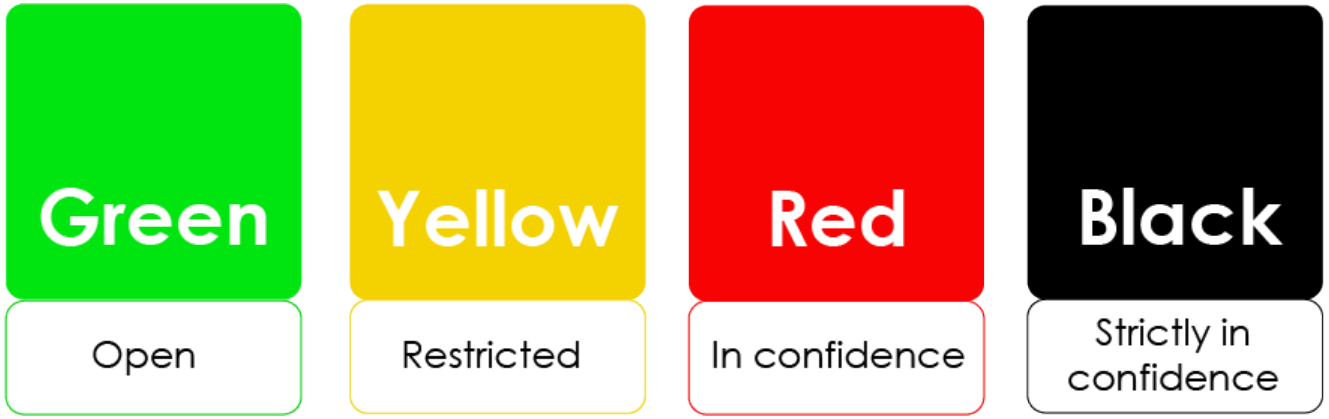
- Personal data shall be accurate
- important not only in consideration of the data subjects but also for the research
- Obligation to rectify or delete inaccurate personal data
- Rectifying and deleting personal data are key rights the data subjects can exercise, see: GDPR art. 16 and 17 and HRA § 36

7) Storage limitation

- Personal data shall not be stored for longer than necessary to fulfill the purpose, GDPR art. 5(1)(e) and HRA § 38
- Once the purpose has been achieved, the data shall in principle be deleted or made anonymous
- REC usually sets requirements for storage beyond the project period for reasons of verifiability, HRA § 38
  - Processing personal data for the pupose of verifiability is legitimate
  - personal data may be stored for longer periods insofar as the personal data will be processed solely for ... scientific or historical research purposes or statistical purposes in accordance with Article 89(1), see. GDPR art. 5(1)(e)

8) Integrity and 9) confidentiality

- Personal data must be processed in a manner that ensures appropriate security of the personal data
- protect personal data against unauthorised access, unlawful processing, accidental loss, distribution, amendment or damage



- Pseudonymization

10) Accountability

- The controller shall be responsible for, and be able to demonstrate compliance with the principles
- It is therefore important that all persons who process personal data at the UiO follow the prevailing rules and routines
  - The routines have been compiled to ensure that the UiO fulfils central requirements in legislation

Data protection impact assessment

- When is a DPIA necessary?
- GDPR art. 35: «Where a type of processing ... is likely to result in a high risk to the rights and freedoms of natural persons»
  - Based on new technologies, the nature, scope, context and purposes of the processing
  - the list of the supervisory authority, GDPR art. 35(4)
    - E.g.: «Processing of genetic data in conjunction with at least one other criterion.», and «Processing of personal data using innovative technology in conjunction with at least one other criterion»
- Why is it necessary?
  - Ensure that the privacy of the data subjects is safeguarded (e.g. demonstrating comliance with the principles in the GDPR art. 5)
  - Identify risks and take measures to reduce the risk
  - Assess necessity and proportonality of the processing activity

Transfer of data to third countries

- Common in research collaberation
- Third country = all countries outside the EU/EEA
- Transfer mechanism pursuant to GDPR ch. V
  - Adequacy decision
  - Privacy Shield: discontiniued
  - Most common: Standard Contractual Clauses adopted by the EU Commission, GDPR art 46(2)(c)
- Additional safeguards, cf. Schrems II
  - For research
    - Pseudonymization

The EU Commission has recognised:

Andorra, Argentina, Canada Far oe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay

Key additional HRA requirements

- the organization of a research project
  - This is part of the UiOs quality assurance system for medical and health reserch
- REC approval HRA §§ 33
- Final report when the research project is completed
  - REC approval for access to the use of health information collected in the health and care service for research, HRA § 35
    - exemption from healthcare professionals' duty of confidentiality and exemtion from consent
  - Processing of health information from health registers pursuant to the Health Register Act §§ 8 to 11 does not require prior approval, unless otherwise follows from the regulations of the registers

Thank you for your attention!

- Contact me and my colleagues?
  - behandlingsansvarlig@uio.no
- Contact the Data Protection Officer?
  - personvernombud@uio.no
- Contact me personally?
  - lars.soligard@usit.uio.no