



Data protection & research: responsibilities under the GDPR

Janecke Veim, Data protection officer, UiB
Janecke.veim@uib.no





Data protection and research

- Research projects carried out at the university will often involve information relating to individuals ('personal data')
- This information must be processed in accordance with the requirements of data protection law
- The presentation gives an overview of the legislation and provisions which apply, following the implementation of the EU General Data Protection Regulation and new national legislation in Norway, and the interplay between the GDPR and ethics requirements





Relevant legislation

General Data protection Regulation (GDPR)

- The GDPR is an EU Regulation that applies directly to Norway, as a member of the EEA

The Norwegian Data Protection Act 2018 (personopplysningsloven)

- The Norwegian Data Protection Act supplements the GDPR in areas where member states can vary or adapt GDPR provisions. A number of its clauses relate specifically to **scientific research**

Other laws relating to use of personal data, eg. Act on health and medical research





General Data Protection Regulation (GDPR) & The Norwegian Data Protection Act 2018

About data protection

What is it and why is it
important?

Scope of GDPR

Does it apply to your
research?

Responsibilities under the GDPR

Who is responsible and
what is required?

Transfer of data

Can personal data be
transferred outside the
EU/EEA?

GDPR exemptions

Are there exemptions
relevant to research?

Practical considerations

What do you need to
consider?





About data protection

What is data protection?

In policy terms – data protection law aims to strike a **balance** between

- The privacy interests of individuals, and
 - The needs of organisations to make fair and reasonable use of information
- This does not mean that researches cannot make use of such information, or that they always need to obtain consent, but it does mean that certain controls and restrictions must be complied with.
 - Technology has made it possible to collect and use increasing amounts of information.
 - The purpose of GDPR: a framework to safeguard the rights of individuals





About data protection

Why is data protection important?

- Compliance with the GDPR is a **legal requirement**. Breaches of data protection may result in investigations, significant fines, adverse publicity, reputational damage and civil or criminal liability. Enforcement action may be taken by the Data protection authorities (Datatilsynet)
- Individuals have **extensive rights** under the GDPR, which they may exercise by submitting requests. If dissatisfied, they may complain to the Data protection authority
- The University is committed to **responsible processing of information** relating to individuals and to respecting their rights and privacy. Data protection law is also usually **consistent with the ethical requirements** of many research projects.



Scope of GDPR

Does the GDPR apply to your project?

The GDPR applies to the '**processing**' of '**personal data**'.

Relevant questions:

1. Are you **processing**? Processing means almost anything a research team might do with the data, including:
 - Collecting it
 - Holding or storing it
 - Retrieving, consulting or using it
 - Organising or adapting it
 - Publishing, disclosing or sharing it
 - Destroying it /anonymising





Scope of GDPR

2. Does the project involve **personal data**?

Personal data is any information which relates to a living individual who can be identified from that information, whether indirectly or directly, and in particular by reference to an identifier, It includes

- A name, an identification number, location data, online identifiers. Can also include information that identifies an individual's characteristics, whether physical, physiological, genetic, cultural or social.
- Intentionally broad definition. General advice: err on the side of caution!





Scope of GDPR

Different types of data:

- Anonymous data
- Pseudonymous data
- Aggregated data
- Biometric data, DNA and human tissue samples
- Photographs, videos and sound recordings





Scope of GDPR

Special category personal data:

Personal data which the GDPR defines as more sensitive, and so needs more protection.

For example, information about an individual's:

- **Racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data (new), biometric data (where used for ID purposes – new), health, sex life or sexual orientation**
- This type of data poses greater risks to a person's fundamental rights and freedom, by e.g. putting them at risk of discrimination





Responsibilities under the GDPR

Who is responsible for complying with the GDPR? The GDPR imposes obligations on both '**data controllers**' and '**data processors**'

- Data controllers is the person/institution who (either alone or jointly with others) **determines the purposes** of processing and the manner/**means of processing**
- Data processor is the party who does the processing **on behalf of** the data controller, according to the controller's instructions

For research projects based at the University, the **University will most likely be the data controller**, also if the research project is taking place outside Norway or the EEA.



Duties and obligations under the GDPR

Data protection principles - researchers must process all personal data in accordance with the **GDPR 'data protection principles'**, unless there is a relevant exemption. The data protection principles represent the core requirements.

Personal data must:

- Be processed lawfully, fairly and in a transparent manner
- Be collected only for specified, explicit and legitimate purposes, and not be further processed in a manner incompatible with those
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Be accurate and, where necessary, kept up-to-date
- not be kept as identifiable data for longer than necessary for the purposes concerned; and
- Be processed securely





Fair, lawful and transparent processing

The **most important** data processing principle. It is the overriding objective of the GDPR and all the subsequent data protection principles are requirements for complying with this principle. Three aspects:

- **Fair processing** – requires researches to consider more generally how their use of personal data affects individuals
- **Lawful processing** – all processing must have a legal basis
- **Transparency** – also linked to the ability of the individual to exercise their rights and to object





The GDPR's research exemption

Background:

- The GDPR acknowledges the need to facilitate different types of research
- The GDPR has no formal definition of 'scientific research', but applies a wide definition to the **notion of research**, stating that:
 - «*the processing of personal data for scientific research **purposes** should be interpreted in a broad manner including for example technological development and demonstration, fundamental research and privately funded research*»
- 'Scientific work' and 'scientific researchers' is defined elsewhere – UNESCO
- GDPR, Recital 33: «it is not always possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection





GDPR article 89 – the research exemption

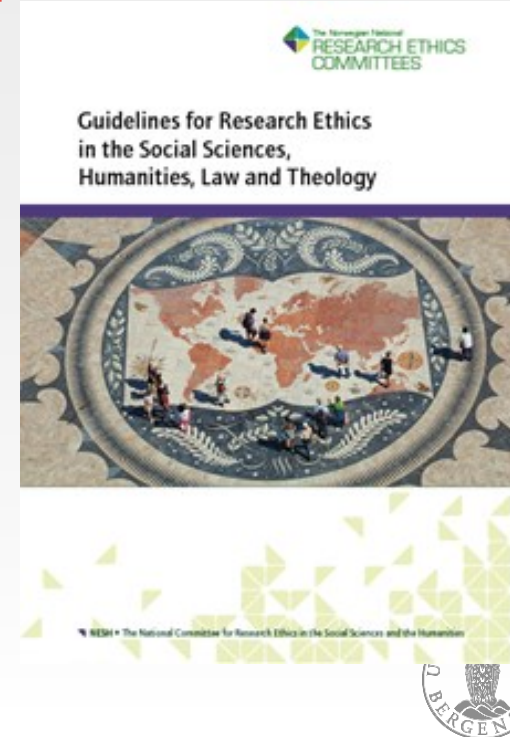
- Article 89 sets a baseline – requires that any derogation is subject to the existence of **appropriate safeguards** for the rights and freedoms of data subjects, including:
 - data minimization
 - Technical and organizational measures
 - Privacy by design and by default
 - Pseudonymization/further processing





Ethical standards and approvals

- **relevant and recognised ethical standards** and the requirements for obtaining **ethical approval** are part of these safeguards
- **This means:** research projects must fulfill recognized quality standards and processes required for conducting research – inextricably linked to the research exemption
- If these safeguards are in place, the following derogations may apply...





Derogations in GDPR:

- Further processing and storage limitation (Articles 5(1)(b) and (e) GDPR)
- processing of special categories of data (Article 9(2)(j) GDPR)
- Information provided by third parties (Article 14(5)(b) GDPR)
- Right to erasure (Article 17(3)(d) GDPR)
- Right to object (Article 21(6) GDPR).

In addition, the following derogations in the Norwegian Data protection act:

- The rights to access
- The right to rectification
- The right to restrict processing
- The right to object.

«Fundamentals of Clinical Data Science», ch. 5 The EU's General Data Protection Regulation in a Research Context

<https://www.ncbi.nlm.nih.gov/books/NBK543521/>





Practical considerations

- Self-collection
- Third-party processing
- Third-party contribution
- Information security
- Data sharing



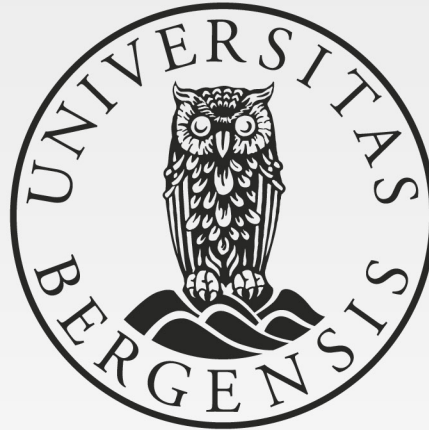


Any questions?

- Contact information:
 - Janecke.veim@uib.no
 - 55582029 / 93030721







UNIVERSITY OF BERGEN