GDPR – legal implications for research on humans

DMP workshop for Life Science Projects, 21.04.21

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

Agenda

About data protecton

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?

DMP and GDPR

If the data includes **personal data** you will need:

- To demonstrate compliance with legal requirements, both in the GDPR and national regulations
- Ethics approval
- Permission from data owners (hospital, health registers
- Data protection impact assessment (DPIA)?
- Advice from the institution's data protection offficer

Relevant legislation

GDPR: the EU General Data protecton Regulation, 2018

- 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 relevant laws: Act on health and medical research (2009), the Health care personell act, the personal data filing Act, etc

Data protection and data protection law

- The purpose of GDPR: a framework to safeguard the rights of individuals
- Data protection law - a **balance** between
  - The privacy interests of individuals, and
  - The needs of organisations to make fair and reasonable use of information
- Breach of data protection law: significant fines, adverse publicity, and civil og criminal liablity

- Individuals have extensive rights under the GDPR, including the right to complain to data protection authority
- Data protection is also usually consistent with the ethical requirements of research projects.

Data processing principles vs ethics considerations?

- The principles for processing personal data are basically the same as the ethical standards for human participation for research
  - To safeguard the fundamental rights and freedoms of the research participants
  - But ethics guidelines relate to participation, while data protection regulations relate to processing
  - Processing for scientific research purposes is allowed, as long as safeguards are in place, such as the research being in line with ethical standards

Consent vs legal basis for processing personal data:

- **Research ethics:**
  - Participation in research should be based on consent, unless an exemption applies (Health research Act)

- **Legal basis for processing personal data for research:**
  - Six legal basis for processing personal data
    - Consent is not usually the most appropriate legal basis
  - The most appropriate legal basis for scientific research is usually the **public interest** basis - GDPR art. 6 (1) e)
  - This also applies for secondary use of informasion, when **researches** do not obtain consent to make use of information
- **Complying with ethics requirements** is a necessary safeguard for processing personal data for research purposes

Primary vs secondary use of data

- The GDPR allows for secondary use of data for scientific research through exemptions
  - Art. 89 (1) – special derogations for research
- E.g Purpose limitation does not apply when the data is to be further processed for scientific research purposes, as long as certain conditions are met:
  - Safeguards (research ethics)
  - Data minimization (pseudonymization)

Does your project involve personal data?

Personal data

- any information which **relates to** a living individual who can be identified from that information, whether directly or indirectly, and in particular by reference to an identifier. Examples:
- Name, id-number, location data, online identifiers such as IP-address
- Can also include information that identifies an individual's characteristics, whether physical, physiological, genetic, cultural or social.

The definition of personal data is intentionally broad – general advice: err on the side of caution!

Scope of the GDPR

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

Processing means almost anything you do with personal 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

Different types of data

- **Anonymous** data is not personal data. Falls outside the scope, but anonymising poses challenges and careful consideration if at all possible
- **Pseudonymous data** usually involves the removal of common identifiers and use of a pseudonym (often a randomly allocated number). Pseudonymous data is still personal data
- **Aggregated data** is the process of combining information about many individuals into broad classes, groups or categories, so that it is no longer possible to distinguish information relating to those individuals. Not personal data, but will depend on factors such as size of population

Types of data

- **Biometric data, DNA and human tissue samples** are all considered personal data under the GDPR
- **Photographs, videos and sound recordings** of participants may disclose personal data about the individual themselves or others. The existense of the material itself may allow for identification. Therefore, these are all media which are capable of being personal data.

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
- **Can only be processed in certain situations and for certain purposes**

Responsibilites under the GDPR

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

- Data controller 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 protecton 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:

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

Selecting a lawful basis for processing

In view of the challenges with consent: the reccomendation in other EU countries is that researchers should not rely on consent as their only legal basis for the processing of personal data.

For the same reason, it is recommended that researchers should not select explicit consent as their additional condition for legitimating the processing of special category data. Rather, it is recommended that researchers should rely on **public interest task as the legal basis for the processing of personal data; and research as the additional condition for the processing of special category data.**

There will continue to be a need to seek consent from participants in research in order to satisfy ethical considerations, but this will be separate from, and in addition to, the requirement under the GDPR to identify a lawful basis for the processing of personal data and to meet a condition for the processing of special category data. How the consent is sought in such cases will depend on the nature of the project. For larger projects and/or for those involving special category data, it would be appropriate to seek positive, opt-in consent, even where consent is not the legal basis for processing.

However, in either case, the wording of such consent should be careful not to conflate the issues of consent to participate in the project and 'consent' to the University's use of personal data under the GDPR.

Lawful processing - GDPR

The processing of personal data must have a **lawful basis** in the GDPR art 6:

- **The Public interest task**:
  - **the most relevant legal basis for processing personal data for the purpose of scientific research.** This legal basis covers both consent-based and non-consent -based research.
- **Legitimate interests**: – may be relevant when cooperating with industry

- **Re: consent**:
  - Difficult to rely on consent as legal basis for scientific research
  - Data subjects have the right to withdraw their consent at any time – challenging for research, so **consent as legal basis should not be 1st choice**
  - **Important**: consent is still the ethical 'main rule' for human participation in research, but it is **not the same as consent as a lawful basis for processing under the GDPR**

Supplemental legal basis – Norwegian law

- The Data Protection Act, section 8:
  - Personal data can processed according to GDPR art. 6 (1) e) (task in the public interest) when **necessary** for purposes relating to scientific research.
  - Processing must have necessary safeguards, ref. art. 89 (1)

Special category data

GDPR art. 9: Only allowed for certain conditions, the most relevant being:

- **Medical purposes –** e.g. audits, safety, quality assurance projects
- **scientific research purposes**
  - as long as technical and organisational measures are in place to provide appropriate safeguards for the rights of research participants
- **NOTE**: the consideration given to data protection as part of the **ethical review** by REK will help demonstrate compliance with GDPR, but the ethical approval itself does not constitute a legal basis for processing personal data

Supplemental conditions for processing sensitive data - Norwegian law

The Norwegian Data Protection Act, section 9

- Processing special category data allowed if:
  - balance of interests
  - Necessary safeguards
  - Obligatory to seek advice of Data protection officer (NSD can be consulted, according to agreement with UiB)
  - **Exemption from duty to seek advice:** Health and medical research with approval from REK

The role of REK after GDPR:

- **Only ethical approval of research projects**
  - **And authority to give exemptions from confidentiality clause, and**
  - **import/export permission for human biological samples**
- **Legal basis for processing of personal data must be demonstrated in the data protection regulations**
- Ethical approval from REK constitutes a special **safeguard**, therefore:
  - Allows for exemptions for scientific research, from the general provisions relating to processing of personal data

Scientific research where participation is not consent-based

DPIA necessary: when exemption from consent requirement has been granted by REK for the specific project:

- The Data protection authority has decided that such projects need to perform a **data protection impact assessment – DPIA**
- **The data protection officer (DPO) must be involved** (UiB or Helse Bergen, depending on who is responsible for the research project)
- **DPIA not necessary:** broad /general consent for participation, or for quality audits

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:
  - Ethics approval
  - data minimization
  - Technical and organizational measures
  - Privacy by design and by default
  - Pseudonymization/further processing

Data subjects' rights

Strengthened rights under the GDPR:

- Right to be informed
- Right to access (innsyn)
- Right to rectification
- Right 'to be forgotten' /erasure
- Right to restrict processing
- Right to protest/object

Practical considerations

- Self-collection, or
- Third-party processing
- Third-party contribution
- Information security – processing should take place on a secure server, such as UiBs **SAFE server**
- Data sharing – consider what agreements are necessary
- Record-keeping: GDPR imposes a duty to maintain a record of all processing
  - For UiB-controlled research projects: projects must be registered in **RETTE**
  - Health research projects approved by REK are automatically imported to **RETTE** – researchers must supply additional information
  - Projects automatically imported from NSD

Other requirements

- **Accountability -** data controllers must be able to demonstrate that they are complying with the data protection principles and other requirements of the GDPR – all UiB projects must be registered in **RETTE**
- **Appropriate safeguards** - technical and organisational measures, particularly with regard to data minimisation.
- **Data sharing agreements -** have in place a written agreement between organisations setting out their respective roles and responsibilites. GDPR: Compulsory for joint controllers to have such an agreement in place
- **Data protection Impact Assessments (DPIA)**

Data Protection Impact Assessments (DPIA)

Under the GDPR, it is compulsory to carry out a Data Protection Impact Assessment ('**DPIA**') for any project that is likely to pose a 'high risk' to the rights and freedoms of individuals. (Such an assessment is part of the general requirement for 'privacy by design/default', whereby data protection requirements are to be embedded into systems and processes from the beginning.)

The GDPR does not define 'high-risk' but gives as one example the **'large-scale' processing of special category data**. It is likely therefore that a DPIA will be required for some research projects, particularly those in the medical field. The Data Protection Authorty has published a list of types of processing operations requiring a DPIA and further guidance is given on the University website: www.uib.no/personvern

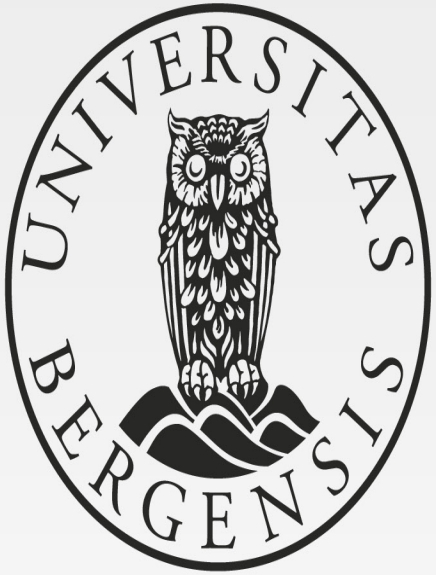
Even if a full DPIA is not necessary, researchers need to be in a position to demonstrate that they have proactively addressed the data protection implications of their projects, in order to comply with the requirements for accountability and privacy by design.

GDPR basics - to sum up:

- The GDPR prescribes adherence to **six** principles (Art. 5) when processing personal data
- processing of personal data must have a **legal basis** (art. 6)
- Additional conditions must be met for processing special categories of personal data (Art. 9)
- Data subjects have strengthened rights under the GDPR
- The GDPR contains **exemptions/derogations for research**, meaning that these rights may be different (less) when collecting and processing data for research purposes – 'the archiving/research' exemptions (Article 89)
- You may have to perform a DPIA

Any questions?

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



UNIVERSITY OF BERGEN

Eco-Lighthouse®