PRIVACY IN RESEARCH - 10 KEY RULES

Scientific research often involves the processing of personal data. It is important for researchers to know what rules they have comply with when processing personal data. The following summary provides the 10 key rules.

Please note that this summary is intended to give you a first impression of the applicable data protection law (the General Data Protection Regulation (**GDPR**) and the Dutch Implementation Act for the General Data Protection Regulation (**GDPR Implementation Act**)) and is not a comprehensive overview.

1. **Personal data**
    - Any information concerning an identified or *identifiable* natural person is considered personal data. A natural personal can be identified directly based on identifiers such as the natural person's name, date of birth and/or address. Identification can also take place indirectly. This means that data which do not lead to direct identification of a person but by which, using reasonable means, a person can still be identified must also be considered personal data. Example: a research participant number or the combination of a postcode and house number.
    - A name is not always needed to identify a person. Certain identifiers, possibly in combination with other factors, can be enough for identification. Example: the 1.90-metre-tall woman with short grey hair driving a red convertible or the man sitting in the left-hand seat all the way in the back of the room to the right.
    - Personal data can be either objective or subjective. Example: Caspar thinks Lily is a socially-minded and committed person. This says something about Caspar (his opinion) and Lily (that she is socially-minded and committed, according to Caspar). The GDPR and GDPR Implementation Act apply when personal data are used (*processed*). This means that (among other rules) these 10 key rules apply.
2. **Pseudonymous ≠ anonymous**
   Pseudonymization is the hiding of identity. Pseudonymization makes it possible to process (additional) data about a person without this person being directly identifiable. Direct identifiers are then often stored in a separate encrypted file (communication file). It is important to realize that pseudonymized/encrypted data sets are <u>not</u> anonymous data sets. Although pseudonymization helps ensure appropriate security of personal data, it does not mean that the data in question have been anonymized. The processing of pseudonymized/encrypted personal data is still subject to data protection law.
3. **Publicly available ≠ can be used freely**
   Personal data from 'publicly accessible' sources, such as Instagram, Facebook and Twitter, cannot be used freely. Any processing of personal data will have to comply with the requirements of data protection law. 'Data scraping' of personal data is therefore not always allowed.
4. **A legal ground is always required**
   Processing personal data *always* requires a legal ground. Without a legal ground, processing personal data is *not* permitted, and any processing without a legal ground is unlawful. In the context of scientific research, the following two legal grounds often come into play:
        - <u>Data subject's consent</u> > For consent to be lawful, a data subject must have given a *free, specific*, *informed and unambiguous* indication of wishes. The data subject must be told in advance what he or she is consenting to and what will happen to his or her personal data. This means that the data subject must also be informed in advance of further processing of his or her personal data, such as when data obtained from the data subject are linked

to data obtained from other (publicly accessible) sources. One particular focus point is that the GDPR gives data subjects the right to withdraw consent at any time. Consent cannot be withdrawn with retroactive effect, but as soon as the data subject has withdrawn consent, his or her personal data may no longer be processed.

- Legitimate interest > In cases where requesting consent is problematic (for example due to the possibility of consent being withdrawn) or impossible (for example when processing an existing data set), 'legitimate interest' may provide a legal ground. To be able to invoke legitimate interest as a legal ground, three conditions must be met:
  1. it must concern a legitimate interest pursued by the controller or a third party;
  2. the processing must be necessary for the purposes of the legitimate interest pursued. This is subject to the principles of proportionality (the means are proportionate in relation to the objective pursued) and subsidiarity (there are no less drastic means available); and
  3. the legitimate interest overrides the data subjects' privacy interests.

5. Prohibition to use special categories of personal data

Besides 'regular' personal data, the GDPR also discerns special categories of personal data. The processing of special categories of personal data is prohibited, except in the derogations specified in the GDPR or GDPR Implementation Act. Special categories of personal data concern: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data concerning criminal convictions and offences. Processing of such special categories of personal data is not only subject to legal grounds for processing and the general data protection principles (see under 6 below), it also requires an assessment of whether the processing warrants derogation from the prohibition on processing special categories of personal data. In the context of scientific research, two possible derogations from this prohibition often come into play:

- Explicit consent

  The prohibition on the processing of special categories of personal data does not apply if the data subject has given *explicit* consent to the processing. The term *explicit* refers to the way consent is expressed, the abovementioned conditions for 'regular' consent are also applicable.

- Derogation for scientific research

  When it is impossible or would require disproportionate effort to ask data subjects for explicit consent, there may be grounds for derogation from the prohibition for the purposes of scientific research. To invoke this derogation, four conditions must be met:
  1. the scientific research serves a public interest;
  2. the processing is necessary for the research in question;
  3. asking for explicit consent has proven to be impossible or would involve a disproportionate effort; and
  4. safeguards have been put in place such that the data subject's privacy is not disproportionately compromised.

Please note: national identification numbers (BSN) may only be used when provided for by specific law. The Netherlands does not currently have such specific law with regard to research, meaning that BSN can never be used for research purposes, not even with consent.

6. General principles

Aside from the abovementioned rules, each processing of personal data must meet the general data protection principles:

a. Lawfulness, fairness, and transparency > Personal data can be processed only in a manner that is lawful, fair and transparent in relation to the data subject.
b. Purpose limitation > Personal data can be processed only for specified, explicit and legitimate purposes and cannot be processed further in a manner that is incompatible with those purposes. Further processing for scientific research purposes shall not be considered to be incompatible with the initial purposes.
c. Data minimization > Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
d. Accuracy > Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
e. Storage limitation > Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods if they are processed for scientific research purposes, provided that appropriate technical and organizational measures are taken to safeguard the rights and freedoms of the data subject.
f. Integrity and confidentiality > Personal data must be processed in a manner that ensures appropriate security of the personal data. Appropriate *technical and organizational* measures must be implemented to protect the personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage.

7. Information to be provided

Data subjects must *always* - also when personal data are processed on the basis of a legitimate interest and without consent - be clearly informed. Information to this effect can be provided in a so-called privacy statement. The VU Privacy Champions have a template privacy statement (ENG & NL) at their disposal. A privacy statement must at least specify the following:

- the identity and contact details of the controller;
- the purposes of and the legal ground for the processing;
- the recipients or categories of recipients of the personal data;
- the storage period;
- the rights of data subjects;
- whether the controller intends to transfer the personal data to countries outside the European Economic Area (= EU + Norway, Iceland, and Liechtenstein).

This information should be provided regardless of whether the personal data are collected directly from the data subject or through another source. Where the provision of information to the data subjects proves impossible or involves disproportionate effort, or is likely to render impossible the achievement of the objectives of the processing, the GDPR offers leeway to derogate from the information obligation. Such derogation is subject to the controller being able to substantiate that adequate safeguards have been put in place. See Articles 13 and 14 GDPR.

8. Joint research / exchange of research data

If the VU collaborates with other scientific research institutions by exchanging personal data with them, the allocation of responsibilities under data protection law must be assessed. If the VU conducts research in collaboration with one or more other institutions, it is possible that an agreement for joint controllers must be concluded. When research is not jointly carried out, but research data are provided to or received from another institution, it is possible that an agreement for independent controllers must be concluded. The VU Privacy Champions have templates for these agreements (ENG & NL) at their disposal.

9. Data Processing Agreement(s)

When using the services of third parties while conducting scientific research that involves the processing of personal data by third parties *on behalf of* the VU (such as third parties that provide survey tools, cloud storage or online research participant tools), a so-called data processing agreement must be entered into with such service providers (*processors*). This is a legal obligation that is intended to ensure that the personal data are processed according to the GDPR. One important provision to include in a data processing agreement is that the processor may only process the personal data as per the instructions of the VU (and possible partners) and not for their own purposes. Also, it is important to make security arrangements, especially when dealing with sensitive or special categories of personal data. The VU Privacy Champions have a template data processing agreement (ENG & NL) at their disposal.

10. International transfers

Personal data may not be transferred to countries outside the European Economic Area (EEA) or to international organizations, unless specific legal requirements are met. An international transfer takes place when personal data are stored on a server that is located in a country outside the EEA or when an organization outside the EEA receives or has access to the personal data. Transfers to countries outside the EEA are permitted only:

- to countries for which the European Commission (EC) has adopted an 'adequacy decision'. At present, this applies to 13 countries: Andorra, Argentina, Canada (please note: only for commercial activities), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay, the United States (please note: only for Privacy Shield-certified organisations) and Switzerland;

Transfers to countries for which the EC has *not* adopted an adequacy decision are permitted only if:

- appropriate safeguards are provided, such as Standard Contractual Clauses (SCC);
- on the basis of derogations for specific situations (see article 49 GDPR).

TO TAKE INTO CONSIDERATION

To make sure that data and privacy are appropriately protected when conducting scientific research, answer the following questions *before* starting on the study:

- What personal data will be processed at what stages of the study?
- From whom or what source will the personal data be collected?
- What are the purposes of the processing of personal data? Are these purposes specific, explicit and legitimate?
- How will the personal data be processed?
- What is (are) the legal ground(s) for the processing of personal data?
- Will special categories of personal data be processed? If so, are there grounds for derogation from the prohibition on processing such data?
- Which organization(s) and/or persons will be involved in processing the personal data? Are they (joint-)controllers or processors?
- Will personal data be transferred to countries outside the European Economic Area?
- How will data subjects be informed about the processing of personal data?
- What technical systems/means will be used to process the personal data and what arrangements have already been made with the suppliers of such systems/means?
- How is adequate security ensured?