rijksuniversiteit groningen / faculteit rechtsgeleerdheid

Ethical rules for conducting research with human participants at the Faculty of Law

Introduction

The Faculty of Law of the University of Groningen is home to researchers carrying out various types of research. In some of these research projects, human participants are an important source of information.

To protect the rights of these participants, the Research Ethics Review Committee Law (in Dutch: *Commissie voor Ethische Toetsing Onderzoek Rechtsgeleerdheid* or CETOR) has been installed to provide guidelines and to evaluate research proposals.
The CETOR bases itself on the General Data Protection Regulation (GDPR), the GDPR Implementation Act and the Netherlands Code of Conduct for Research Integrity.
For more information on the CETOR please have a look at the UG website (link)

All research conducted under the responsibility of a staff member of the Faculty, which:

- relates to *human subjects* (test subjects, respondents) further referred to as "participants"; and/or
- relates to the processing of personal data;
- involves research (or research results) that poses risks for the researchers (or their assistants and others);
- may lead to malevolent use of research results;
- may damage the reputation of the RUG or the researcher

must be submitted in advance to the CETOR.

The CETOR will examine whether the proposed research project complies with the ethical rules for conducting research with human participants.

In case a research project involves *medical research*, the research proposal must be reviewed by an accredited Medical Research Ethics Committee (METc). See also: www.ccmo.nl.

On the following pages the main ethical rules for research with human participants are listed:

1. Providing full information;

2. Obtaining informed consent;

3. Debriefing participants;

4. Ensuring confidentiality and anonymity;

5. GDPR and data subjects' rights.

1. THE OBLIGATION TO FULLY INFORM PARTICIPANTS

Participants must be fully informed in advance regarding the nature and duration of their participation in the study, the processing of data regarding them in the context of the research and any risks or burdens associated with it, and must then give their consent to participate in writing (informed consent, see below). The researcher must also make it clear to the participant that he or she may withdraw from the study at any time without any cost by withdrawing his or her consent.

The information must be geared to the participant in question and must be provided in a concise, transparent, intelligible and easily accessible form by using clear and plain language, especially where minors or intellectually impaired people are concerned. This information is to be given in writing or by electronic means if this is appropriate. Usually, the information is provided in the form of a letter. All the basic information about a study can be concentrated in this letter, which the participant can read before signing a form consenting to participate.

The CETOR has a form that can serve as a model for writing an *information letter*. In cases where the research involves face-to-face contact between the researcher and participant, such as interviews or focus group discussions, the CETOR recommends that the researcher also briefly goes through the information about the study with participants to ensure they have understood their rights and the nature of the research.

The contact details on the form enable participants to contact the principal investigator at a later point if they have any queries or comments. Participants also have the contact details of the CETOR should they have any questions or concerns about the research ethics of the project as a whole that they wish to report.

2. THE OBLIGATION TO ASK FOR WRITTEN CONSENT

The researcher must obtain written consent from each participant for participation in a study after providing the participants with information. Consent is given by means of clear affirmative acts of participants. These acts must be able to establish a freely given, specific, informed and unambiguous indication of their agreement to their participation in the study.

In the case of **minors** aged under 12, the consent of the parents/guardians is required. In the case of minors aged 12 to 16, consent from both the parents and the child is required. If the child is older than 16 but is younger than 18, consent obtained only from the child would be sufficient.

In research among young people, *passive consent* (that is, no response from the parents means consent) may not be sufficient. The CETOR will base its decision largely on the extent to which the research places a burden on the child participant.

In addition, it is possible that certain individuals, such as **mentally disabled persons**, are not capable of giving consent. In this case, consent must be authorized by legal representatives of such individuals.

In studies involving **online surveys** participants should also explicitly give their consent. This can be done by adding the following sentence: *'By proceeding to the survey, you automatically consent to participate in the study'* **and** by letting them click 'yes' in a tick box. A signature is not required for an online survey.
The researcher should not appeal to people in **public spaces** to take part in a study without explicitly asking for consent (oral or written).
For low-burden studies taking 10-15 minutes or less, oral consent is usually sufficient, so long as full information is provided. The CETOR will decide on this. For studies of longer duration with a greater burden, participants must always sign a consent form.

A standard consent form of the CETOR can be downloaded from the website and adapted for the specific purposes of the research project. A copy of the consent form is given to the participant at the time of signing.

3. THE OBLIGATION TO DEBRIEF PARTICIPANTS

Sometimes, (temporarily) withholding information or deceiving the participants is unavoidable. In these cases, the information given about the nature of the study can be incomplete or even false. The CETOR will assess whether it is necessary and permissible to withhold information or to deceive participants regarding the nature of the study. In these cases, an adequate debriefing is essential. Participants must never be deceived regarding risk or burden of the study they take part in. If a study involves withholding information or deceiving participants on the nature of the study, the researcher is obliged to fully inform the participants *afterwards* regarding the nature of the missing information or deception (debriefing). The true nature of the study must then be explained. The CETOR also has a model form for this purpose on its website: 'Debriefing after withholding information or deception*'*.

In some studies involving withholding information or deception it may be undesirable to disclose the true nature of the study immediately afterwards, in order to prevent this information being 'leaked' to new participants. In such cases the researcher can opt to debrief the participants after completion of the study as a whole, for instance by sending an e-mail or letter. Alternatively, the participants can be asked to sign for a 'period of confidentiality' for the duration of the study.

It is essential that participants receive a debriefing in case of withholding information or deception**.** In other cases it is advisable to debrief. If that is not done, participants may get the feeling they are not taken seriously. In addition, they may become cynical ('They say you will get information afterwards, but you never do') and will therefore not be motivated to participate in other studies.

4. THE OBLIGATION TO TREAT THE PARTICIPANTS' OR DATA SUBJECTS PERSONAL DATA CONFIDENTIALLY

The researcher must treat all the participants' or data subjects' persona data *confidentially* (this has been laid down in the General Data Protection Regulation, GDPR). 'Confidentially' means ensuring that the data cannot fall into unauthorized hands, for instance those of people not involved in the research project. Researchers should take suitable technical and organizational measures ensuring appropriate security of personal data and provide details of how they will protect their data once it is collected.

In addition, research data must be processed *pseudonymously* or – if it is possible – *anonymously*. By using pseudonymization or anonymization techniques, researchers can ensure that the research data cannot be traced back to the person. This means that no personal details such as name or address may end up in the research data file (the data for analysis).

Pseudonymization refers to the processing of personal data in such a way that this data can no longer be attributed to research participants without the use of additional information. This additional information must be kept separately from other research data and it is required to take technical and organizational measures in order to prevent the possibility of attribution to data subjects. Usually a participant in a research is assigned a number that is used as a pseudonym and linked to the research data.

Anonymization means the processing of personal data in such a manner that the identification of data subjects is irreversibly prevented. It is the case when data subjects cannot or can no longer be considered identifiable. In practice, it is difficult – if not impossible – to deploy anonymization techniques that are entirely effective.

While pseudonymized data is regarded personal data under the GDPR and needs to be sufficiently protected, anonymized data does not fall under the scope of the Regulation. From the data protection perspective, it would therefore be less complicated and cumbersome for the researchers to make use of personal data that has been anonymized. From a methodological perspective, drawing appropriate conclusions from such a research would not always be possible, for instance, when empirical research in the form of interviews is conducted and insights gathered from these interviews must be linked to interviewees.

When pseudonymization requires a disproportionate amount of effort or is impossible, the processing of the research data must be done in a secure environment, for example exclusively within the RUG network.

While pseudonymized data is regarded personal data under the GDPR and needs to be sufficiently protected, anonymized data does not fall under the scope of the Regulation. From the data protection perspective, it would therefore be less complicated and cumbersome for the researchers to make use of personal data that has been anonymized. From a methodological perspective, drawing appropriate conclusions from such a research would not always be possible, for instance, when empirical research in the form of interviews is conducted and insights gathered from these interviews must be linked to interviewees.

With regard to the storage of pseudonymized and anonymized data, both the research data and the consent forms must be kept in a safe place after the research is completed. In principle, this is the network storage of the RUG (X or Y disk). Retention periods depend on the type of research.

In many cases it is *not* necessary to collect personal information from the participants. If there are good reasons to collect personal information, for example to send summaries to the participants, these data should *not* be linked to the research data. Research data and personal data must be stored in different places.

Because informed consent forms contain the names of the participants, they must also be collected and stored separately from the research data.

In the case of interview recordings, it is recommended that these recordings be destroyed after the study if the interview transcription contains the information needed for the study.

Because informed consent forms contain the names of the participants, they must also be collected and stored separately from the research data.

Personal data, apart from informed consent forms, may only be kept as long as is necessary for the purpose for which they have been collected. For example, once summaries of the study have been sent, they can be deleted. In the case of research projects in the context of degree programmes (such as Bachelor's or Master's theses) 6 months is a reasonable period. If personal data is kept for a longer period for a special purpose, explicit consent for this must be given by the participant (on the informed consent form).

The Principal Investigator (PI) is ultimately responsible for the confidentiality and anonymity of the data, but usually the data is managed by another person involved in the

research project (such as a research assistant or a student). In that case the daily responsibility lies with that other person.

PLEASE NOTE!
If it is necessary for personal data to be linked to research data, for instance in the case of a longitudinal study, the participant number should be recorded in both the file with research data and the file with personal data. Research data and personal data must be stored in different places.

The consent form should not be stapled to the questionnaire package. This results in a breach of anonymity, because the personal details are linked to the research data. The solution is to use separate forms for the consent form and the questionnaire.

The participant number should not be recorded on the consent form. This again breaches anonymity. The participant number may only be written on the questionnaire or other research material.

The file with the research data and the personal data should not be stored in the same folder on an external device (such as a memory stick or laptop).

In accordance with the data management policy of the RUG and the faculty, research data must be stored on the RUG network. Several folders can be used for this purpose. Depending on the sensitivity of the data, it is recommended to store the personal data and the pseudonymization key on the personal drive (X drive) and the research data on the Y drive.

When necessary, the personal data folder can also be protected by encryption.

For storing research data, a so-called Publication Package on the Y: drive is available. For PhD students this is created by default. Other researchers can request such a folder from the Privacy & Security coordinator of the Faculty (Maarten Goldberg).

5. Your research and the GDPR

For the processing of personal data in scientific research, the AVG has a number of details. If you submit an application to the CETOR, you will be asked in more detail about the processing of personal data in your research and you will be given further explanations about the AVG.

You can request the application form from the secretary of the CETOR or download it here

For more information on research and the GDPR see the UG website.