rijksuniversiteit groningen / faculteit rechtsgeleerdheid

Guide to CETOR (Committee on the Ethical Review of Research in Law)

Guide to the application forms and further steps in the review of your research by the CETOR (Committee on the Ethical Review of Research in Law)

Research subject to the WMO

Does your research fall under the Medical Research Involving Human Subjects Act (WMO)?

In that case your research should be reviewed by the METC (Medical Ethical Review Committee) and not by the CETOR. You will find more information about this in the appendix on page 2.

DPIA scan

When there is a high risk of misuse of personal data, such as when collecting and processing large amounts of data and/or very sensitive data, you should first perform a "Data Protection Impact Assessment (DPIA)". Please check the Appendix on page 2 and 3 and have a look at the "DPIA scan" if this is possibly the case.

The application form

The application form contains (short) help texts. You can simply overwrite these with your own text.

In some cases the questions in the application form are accompanied by an explanation. You will find these explanations at the end of the form. Please read them before answering the question.

Annexes

You are required to submit a number of attachments to the application form. These are:

a) Information about the study for participants *or*
   Information about the study for 'data subjects';
b) A consent statement for the participants, if applicable in your research;
c) A 'debriefing' procedure, if applicable in your research;
d) A data management plan.

A template is available for appendices a, b, and c. You are not required to use the templates. You may also adapt these templates, for example, to the intended group of participants.

Appendix d, the data management plan, can be easily created with the RDMP web tool. You log in to this web tool using this link. Then choose to create a plan. If you have already made a plan via another route, for example with NWO or EU funded research, you may also use that plan.

Procedure at the CETOR

You can submit your application form and attachments to the secretary of the CETOR, Maarten Goldberg.

E-mail: m.goldberg@rug.nl, tel. 050 36 34904 / 06 10 500 501.

As a rule, you will receive a reply within 6 weeks.

According to the CETOR regulations (link) you can only start your research once the CETOR has given its approval. If you are pressed for time or if there are other reasons to start your research in the meantime, please contact the secretary of the CETOR.

More information about the CETOR and ethical review (link)

Appendix I: Medical or non-medical research

Research is covered by the Medical Research on Human Subjects Law (*Wet Medisch-wetenschappelijk Onderzoek met mensen, WMO*) if the following criteria are met:

1. It concerns medical/scientific research **and**
2. Participants are subject to procedures or are required to follow rules of behaviour.

In that case, the research proposal must be reviewed by an accredited Medical Research Ethics Committee (*Medisch Ethische Toetsingscommissie, METc*).

The WMO does not give a definition of the term *medical-scientific research*. As a result, it is not always clear if research must be submitted for review by a METc.

There are also cases where the participants are patients but the research is not medical in nature. In those cases, it is advisable that researchers contact the METc for advice. The METc can issue a *Statement of Exemption*, which certifies that the study does not have to be reviewed by the METc.

There are academic journals that demand a Statement of Exemption as a prerequisite for publication.

Researchers of the UG can find more information on the website of the UMCG: https://metcgroningen.nl/indienen/non-wmo-research/?lang=en

For more information, see also https://english.ccmo.nl/

Appendix II. Data Protection Impact Assessment (DPIA) en pre-scan DPIA

In some cases, the processing of personal data poses a risk to data subjects. In such a situation, the General Data Protection Regulation (GDPR) requires that a Data Protection Impact Assessment (DPIA) be carried out to ensure that major risks to the rights and freedoms of data subjects are prevented and that their rights and freedoms are safeguarded.

A DPIA is a systematic assessment of the impact of a particular system on the data protection of affected individuals. Such an assessment is required if the researcher intends to collect a large amount of data and/or highly sensitive data. Based on this assessment, recommendations can be made to minimize this impact as much as possible by applying technical and organizational measures. For example, by not asking for birth dates but birth years or by never storing data on a laptop or PC but always directly on a secure network storage.

The purpose of the DPIA is to identify the risks of data processing, before the start of a research project, and to name measures to limit those risks. What personal data will be

processed? What will the researcher do with it? What measures does the researcher take to protect the rights and freedoms of data subjects?

Please use the pre-DPIA scan below to check whether a DPIA is necessary. If so, or if you are hesitating, please contact the Privacy & Security coordinator of the Faculty of Law Maarten Goldberg.

Pre-Scan DPIA

If there are *two or more of the situations below*, it is advisable to perform a DPIA.

1. Processing sensitive personal data (e.g. criminal data, data on orientation, health data);
2. Processing personal data of vulnerable persons (e.g. children, mentally ill persons and patients);
3. Assessing people based on personal characteristics (i.e. profiling);
4. Making automated decisions based on personal data (making decisions without human intervention, for example providing a mortgage);
5. Systematic and large-scale monitoring (e.g. camera surveillance);
6. Large-scale data processing (e.g., because of numbers of people, duration, or amount of data);
7. Linking of collections of personal data (e.g., combining databases of multiple organizations);
8. Use of new technologies (e.g. mobile apps, new access control, smart camera systems);
9. Blocking a right, services or contract based on personal data (individuals lose control or a right).

More information: https://www.rug.nl/research/research-data-management/data_protection-gdpr/data-protection-impact-assessment/