Brief instructions on Ethics and GDPR

For the latest version, always check https://fetc-gw.wp.hum.uu.nl/en/procedure-2/.

Introduction

The Faculty Ethics Assessment Committee of the Faculty of Humanities (FEtC-H) is responsible for monitoring the criteria for ethical conduct for all research carried out at the Faculty that involves human participation.

If your research involves working with *participants*, e.g. if you intend to conduct interviews, administer questionnaires or conduct observations and/or if your research involves working with *personal data*, i.e., information from which a (living) person can be identified, then you must obtain approval from the Faculty Ethics Assessment Committee before you start with your research.

If you are working with *personal data*, the General Data Protection Regulation (GDPR) will also apply and you will have to meet certain requirements in order to work in accordance with the GDPR. Researchers affiliated with the Faculty of Humanities are also required to draw up a data management plan. This is part of ethics as well, because ethics, privacy and data management are closely intertwined.

Ethics

The following elements are important when working with participants:

- **Participants**: are they capable of giving informed consent, or do they belong to a vulnerable group (i.e. under the age of 16, legally incapable of giving consent, or socially vulnerable)?
- **Selection method**: it is conceivable that participants may feel pressured (socially, financially)? How will you find and approach the participants?
- **Data collection**: How are you obtaining your data? If this is not directly from participants but indirectly, e.g. by web scraping, then you should contact the Data Manager at datamanagement.gw@uu.nl.
- **Voluntary participation**: are participants able to choose to participate freely and are they able to stop participating at any time without any adverse consequences?
- **Burden**: there are various types of burden, such as time investment (at the expense of something else), loss of privacy, effort (e.g. having to expend a lot of energy thinking). What type(s) of burden are participants exposed to?
- **Risk of harmful effects**: for example, can participating have an adverse effect on a participant's job situation if a superior would find out about it?
- **Unexpected results**: for example, a test may show that a participant suffers from dyslexia or may reveal that a participant has done something illegal. What will you do in the event of such unexpected results?
- **Research causing discomfort**: does the research involve being asked about emotional memories, for example, or participating in an EEG examination that requires sitting still for a prolonged period of time and having gel applied to your hair?
- **Anonymity and privacy**: will participants remain anonymous or will they be assigned pseudonyms, or have participants agreed to having their identity disclosed?
- **Adequate data management**: is the participants' data processed and managed in an adequate manner?

- **Deception**: sometimes participants cannot be informed in advance what the nature of the research is, as this might affect the results. In such cases, participants must be informed afterwards.
- **Information letter, informed consent and consent form**: information and consent are essential to any research that involves participants! Were the participants accurately and fully informed of all aspects of the research prior to giving their consent? And has consent been obtained separately for each of the various aspects or components of the research in the appropriate manner?

GDPR

All informed consent documentation must obviously comply with the GDPR. If you have any questions about the GDPR, then please contact the Privacy Officer of the Faculty of Humanities (privacy.gw@uu.nl) before submitting your application to the FEtC-H.

What is the GDPR?

The General Data Protection Regulation (in Dutch: Algemene verordening gegevensbescherming, AVG) is legislation that standardises the rules governing the processing of personal data by individuals, companies and public authorities for the entire EU plus Norway, Liechtenstein and Iceland (which together comprise the European Economic Area or EEA). Since the GDPR came into force in May 2018, the same privacy legislation applies throughout the EEA.

What is personal data?

Personal data means any information relating to a natural person who can be identified directly or indirectly from that information or from that information in combination with other information. The definition of a 'natural person' excludes legal entities and deceased persons. Personal data includes things like images, audio recordings and text. Examples:

- Audio/video recordings
- Name
- Address
- Telephone number
- Email address
- Age / date of birth
- Sex / gender identification
- Degree programme
- Profession
- IP address
- Native language(s)
- Answers to questions (including yes/no)
- Login details
- Facial images
- Test results

Certain types of personal data are classified as *special categories of personal data*. This relates to highly sensitive data that must be handled with the utmost care as they may lead to exclusion, discrimination or stigmatisation. Special categories of personal data include information about someone's:

- Religion / beliefs
- Race / racial identification / ethnic background
- Political preference
- Trade union membership
- Health (e.g. dyslexia, trauma)
- Gender and sex life
- Biometric data (*for the purpose of the unique identification of persons*)
- Genetic data
- Criminal history

If you intend to process any special categories of personal data, always contact the Privacy Officer of the Faculty of Humanities (privacy.gw@uu.nl) well in advance, as a privacy assessment will have to be carried out in such situations.

As a final point, the Citizen Service Number (BSN) may only be used in certain situations specified by law. These situations do not include research. Therefore, you may never ask your participants to provide their BSN for your research.

A clear overview of the various types of personal data is available on the intranet: Categories of personal data

What exactly does 'processing of personal data' mean?

The 'processing' of personal data refers to literally everything that you do with that data as a researcher, or instruct others to do on your behalf: collecting, storing, retaining, analysing, anonymising, showing to others, publishing, etc.

Am I allowed to work with personal data and, if so, how?

Before you start working with any personal data, you must assess two key questions:

Stap 1. Am I allowed to process the personal data? (Determine the research purposes and the legal basis under the GDPR/AVG)

Stap 2. And if so, how can I process the personal data with due care? (Determine what data you wish to collect and how to store it securely)

Step 1. Research purpose and legal basis

This step requires:

A. a **specific purpose** for the processing (e.g. requesting an email address in order to send a participant specific information, or processing data for the purpose of a specific research project) **and**

B. a (legal) **basis** for the processing. The legal basis for any research will almost always be consent. Only if it is impossible, impracticable or disruptive to request participants to give their consent (for example, if this would affect the results of your research), can you rely on the basis of a public interest to justify processing personal data (given that as a university, we are charged with a task that is in the public interest: conducting scientific research).[1]

When you request your participants' consent (step 1.B), you are obliged to inform them first, so that they understand what they are consenting to. You can do so, for example, by means of an **information letter**. The active consent of participants (so NOT a pre-ticked box for consent) is required for:

- their participation (including in anonymous research),

  unless the data would have been collected anyway outside of the research, such as in the case of research into children's school test results. This is an example of the basis of a 'public interest'. In such cases, participants must be *informed* afterwards and will likewise be able to *object* afterwards.[2]

- audio and video recordings (please note that by definition these are not anonymous data)

[1]The third possible basis to justify processing personal data is that of a legitimate interest. This, however, is subject to an additional requirement, namely drawing up a written assessment that weighs up the importance of your research and the privacy risks to the participants.

[2]In this situation, we speak of the ethical concept of "passive consent".

- sharing personal data with third parties.

How to obtain legally valid, 'informed' consent is explained in the document "Guidelines on 'informed consent' when conducting scientific research,", see section 'Privacy and GDPR' at https://fetc-gw.wp.hum.uu.nl/en/informed_consent/.

Personal data may only be processed if there is a specific purpose and a legal basis for this processing.

Step 2. Which data and data storage

After you have completed Step 1, Step 2 deals with **the way in which you process the personal data**. This requires keeping in mind the following:

- Do not request more information than is necessary for the research purpose. This is referred to as data minimisation: need to know, NOT nice to know.
- Store the data securely.
  - Provide a safe storage location, preferably UU storage and storage in the cloud (so Yoda or Surfdrive, but not Dropbox or Google Drive). Remove the data from any mobile devices as soon as possible;
  - Use encryption (e.g. Bitlocker) as well as password protection, especially on mobile devices;
  - Separate any contact details from the research data as soon as possible;
  - Try to anonymise your data as soon as possible (the link between the participant's research data and their personal data must be irreversibly severed – so that even the researcher no longer knows who is who among the participants!) or, if this is not possible, use pseudonymisation (this enables the controlled re-identification of participants; by means of a key, for example).
- Ensure that access to the data is properly controlled (authorisations).
- Set specific retention periods: as is the case at other Dutch universities, the standard retention period for research data at Utrecht University is at least 10 years after publication.

What's next?

In short: if your research involves participants, then you need prior approval from the Faculty Ethics Assessment Committee of the Faculty of Humanities (FEtC-H) before you start with your research. Applications must be submitted through the FEtC-H portal. Use your SolisID to log in. On the portal you can create a new application and then answer the questions and submit the information letter(s) and declaration(s) of consent. Templates are available on the intranet (the texts, without any reference to FEtC-H, are also available on FEtC-H website).

Students and PhD candidates cannot submit an application themselves but can start an application. In the application, they must state who their supervisor / PhD supervisor is. Applications can only be processed after the supervisor / PhD supervisor has approved the application.

If your research involves working with personal data, the GDPR applies. In that case, you must follow the instructions set out above. Furthermore, the GDPR requires the registration of your project – this will be made possible in the near future.

For further information, please see:

- FEtC-H portal
- FEtC-H website
- FEtC-H intranet
- Informed consent document templates
- Faculty of Humanities data management policy
- Guide for data management at Faculty of Humanities
- Privacy at the UU - intranet
- Handling personal data