Guide for Handling Data in University Research Projects

Ethics Committee of the University of Mannheim

Please note: This document aims to help applicants assess the relevance of data protection laws and the requirement of a vote of the ethics committee when handling data in research. It is not intended as legal advice and is not complete. In cases of doubt, the Ethics Committee advises to submit an application for advice. Please use the application form and follow the instructions on the Ethics Committee's website.

1. Is a vote of the ethics committee always required when handling data in research?

The statute of the ethics committee states that researchers must seek advice on the handling of *personal* data prior to a research project. For the concept of personal data, see number 3 below.

2. Do data protection laws (GDPR and domestic law, such as the State Data Protection Act of Baden-Württemberg) have to be considered when handling data in research?

Data protection law always applies when personal data is collected or processed. If the data to be used for research is collected anonymously or is already available in an anonymized form prior to the research project, data protection law does not apply (see the following questions).

3. What is personal data? Why is this relevant?

According to art. 4 no. 1 of the General Data Protection Regulation of the EU (GDPR), personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Whenever a personal reference in this sense exists or can be established, the provisions of data protection law must be complied with. A specific legal basis is then required for the collection and processing of personal data. This consists in the informed consent of the person concerned or in a legal permission.

4. What is pseudonymized data and what are the requirements for it?

The GDPR defines pseudonymization in art. 4 no. 5 as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject

to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Pseudonymized data is therefore information about a person which is laebelled with a code (pseudonym) instead of the name. This code consists of letters and/or numbers and may not contain the initials or complete date of birth. It must be stored and protected separately; otherwise, the data will be considered personal.

Pseudonymized data is basically treated as personal data if it is possible to assign the code (and thus the information, e.g. on questionnaires) to a person, i.e. if there is a list which can be used to decipher the data. Only if such a list does not exist, or if this list is not accessible to anyone, does data protection law not apply.

If an assignment to a person is not necessary or wanted, the data should be collected anonymously, for example in questionnaires that contain neither the name nor a pseudonym/code. For the question of consent for such a procedure, see question 8 below.

5. What is the difference between pseudonymized and anonymized data?

In contrast to pseudonymized data, anonymous data is any information that cannot be attributed to a person without using reasonable effort. Data labelled with a pseudonym becomes anonymized data if it can no longer be attributed to a person, for example because the identification list has been destroyed.

Even pseudonymized data that cannot be decrypted by the recipient of the data can be treated as anonymous data. Whether the attribution to a person is possible using reasonable effort, is a question of the individual case. In case of doubt, an application should therefore be made to the ethics committee.

6. Is consent of the subjects always required when data is collected and processed?

Generally, consent is required if personal data is to be collected or processed.

As an exception, data processing is possible without consent on the basis of a statutory provision in accordance with § 13 (1) of the State Data Protection Act for Baden-Württemberg (Landesdatenschutzgesetz – LDSG) "if the purposes cannot be achieved in any other way or only with disproportionate effort and if the interests of the public authority in carrying out the research or statistical project outweigh the interests of the data subject in excluding the processing".

For this and for the further requirements of § 13 LDSG, information must be provided to the ethics committee. Even if the consent of the data subject is not required by data protection laws, there is an obligation to consult the ethics committee whenever research is carried out using personal data. This obligation results from the statute of the ethics committee.

7. Which requirements must be observed when data protection law applies?

In addition to the subject's consent, the information requirements pursuant to art. 13 GDPR for potential participants must be provided in the information documents. Here, among other things, information must be provided on:

- The purpose of the data processing
- Duration of storage
- Type of processing: By whom? In which form? [please also add an explanation for the term "pseudonymization" and information about who can "decrypt" the pseudonym]
- The identity and the contact details of the controller and of the data protection officer,
- Information about the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.

Please note: If the study data themselves are collected anonymously, but personal data is collected as part of the informed consent procedure or e.g. for the payment of the participants' expense allowance, information pursuant to art. 13 GDPR must be provided with regard to these data.

8. Is consent required for anonymous data collection?

From the point of view of data protection law, no consent is required for the collection of data without personal reference. This would be the case, for example, if the participants in a study filled out questionnaires without stating a name or pseudonym.

Depending on the scientific discipline, it may, however, be considered necessary for ethical reasons that participants agree to participate in the study. Such consent can also be given implicitly by conclusive ("implied") behavior, e.g. by voluntarily completing a questionnaire after receiving information about the study.

Please note: If you document the declaration of consent in writing and record personal characteristics (name, address, etc.) for this purpose, data protection law applies regarding the collection of these data (see question 7).

9. What should be considered when using survey platforms and other online tools (e.g., SoSciSurvey, Prolific and similar systems)?

If you use online tools for your research purposes, you should especially explain whether it is possible for you as researcher of the University of Mannheim and/or the operator of the tool/platform to assign

the survey data to individual persons. This should also be explained to the test subjects in the information leaflet. If it is not possible for you to assign survey data to individual participants and the platform operator is not allowed/able to provide any information about this to you, you will be using anonymous data. For their data protection claims, the test subjects can then be referred to the information provided by the platform operator.

If address data (e-mail addresses, postal addresses) are collected for the purpose of processing an expense allowance: Can these data be assigned to the survey data (and thus to individual test persons) or are they stored separately?

10. Debriefing in case of deception or incomplete clarification of the research purpose

If you use a survey platform or other online tools for your studies, you must ensure that the study participants still receive a debriefing in the event of premature termination of the study. The Ethics Committee suggests the following options for this:

a) First, an e-mail address of the participants could be recorded as part of the informed consent form, which would only be used for one-time feedback and would not be associated with the study data. This registration could ensure that all participants receive a debriefing at follow-up, regardless of whether or not they dropped out of the study prematurely. The list of e-mail addresses would have to be deleted immediately after the study ended. The information leaflet for the participants must inform about this.

b) On the study pages, a “dropout button” is placed in a clearly visible position, which participants can click on in the event of premature termination of study participation. If the button is activated, a window opens with the debriefing. In the information for the participants, they should also be obligated to terminate the study – if desired – only by clicking on the “dropout button” and not to participate in the study again. This self-commitment should be confirmed by the participants by an explicit confirmation in the consent form (e.g., by placing a “check mark”).

Of course, you are free to propose other effective solutions to the commission for a debriefing in case of premature termination of the online study.