Guidelines for processing personal data in student and research projects at the University of South-Eastern Norway

Version No. 1 valid from: 01.01.2019

Approved by: Vice Rector Pål Augestad

The University of South-Eastern Norway (USN) has an agreement with the Norwegian Centre for Research Data (NSD) to preliminarily assess all student and research projects at USN that involve personal data. This means that all such projects should be submitted to NSD for privacy protection review. NSD will give a final recommendation before the project can start.

Projects that fall outside The Health Research Act (e.g. quality registries, quality studies, health care research) should only be pre-approved by the NSD. Projects that fall within The Health Research Act (Medical and health-related research) must also apply to Regional Committees for Medical and Health Research Ethics (REC). New from 20th July 2018, REC may no longer provide legal basis for the purposes of processing personal data. Henceforth, projects that also fall within The Health Research Act should also be reported to NSD for privacy protection review.

It is recommended that applications are submitted to REC and NSD at the same time so as to achieve the shortest possible processing time. The project manager must send decisions received from REC on to NSD. NSD then conducts a privacy protection review and provides final recommendations regarding whether the project can be started.

Introduction

There are a number of requirements regarding how student and research projects that include personal information should be recorded, evaluated and managed to ensure privacy protection from the project's beginning to end. Here, you can find more information about what is considered personal data, notification requirements, consent and secure data processing. [1]

The guidelines have been complied in accordance with the new personal privacy legislation of 20th July 2018[2]. The aim of the new regulations is to strengthen the rights of individuals in all matters, including research.

Regarding research, the principles of privacy protection ensure that all personal data processing is predictable for those being researched:

Personal data should; [3]

- Personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject,
- collected for specified, explicit and legitimate purposes,
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed,
- accurate and, where necessary, kept up to date,

[1] More comprehensive information can be found on the website of the Norwegian Centre for Research Data (NSD) and The Norwegian Data Protection Authority (DPA).
[2]The law on processing of personal data (the Personal Data Act) https://lovdata.no/dokument/NL/lov/2018-06-15-38 The law is rooted in the EU's General Data Protection Regulation (GDPR).
[3] Source: Excerpt from article 5 of the Personal Data Act: Principles relating to processing of personal data.

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed,
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

The new regulations do not cause any major changes regarding research on personal data, however, one should note:

- Notification and licencing obligations will be replaced by an obligation to register and document the processing of personal data. The University of South-Eastern Norway (USN) has an agreement with the Norwegian Centre for Research Data (NSD) to preliminarily assess all student and research projects at USN that involve personal data. This means that researchers and students must report the processing of personal data to NSD.
- Regional Committees for Medical and Health Research Ethics (REC) provide an ethical preliminary approval of medical and health-related research projects in accordance with The Health Research Act. The new personal data act requires that projects must also be assessed making sure that the processing of personal data happens in accordance with the institution's guidelines regarding basis of processing. NSD will continue to make this assessment for USN. In practice, this means that projects that pertain to The Health Research Act must be approved by REC and assessed at NSD.
- You must be able to document that your participants have agreed to participate by providing a signature/sound recording, for example.
- It should be just as easy for the participants to withdraw consent as to provide it.

About personal data and notification requirements

Are you planning to process data about people in your research or student project? Then you must check whether you need to report the project to the Norwegian Centre for Research Data (NSD) which is USN's privacy protection advisor for research. Use the notification test which is available on the NSD website and submit the form if the test shows that you are processing personal data. When your form has been evaluated by NSD, it serves as documentation that the project processes personal data in a lawful manner. NSD records all projects that they process for USN in a separate database. USN can document the handling of personal data in student and research projects regarding an inspection from The Norwegian Data Protection Authority.

Notification requirements also apply to student projects at both Bachelor and Master levels. However, both the student and the supervisor have a duty to consider whether it is actually necessary to gather personal data in order to carry out the student project. Sensitive personal data should not be collected in Bachelor's projects and should also be avoided as much as possible in Master's projects. See the advice provided on NSD's website regarding how you can make data anonymous.

In addition to NSD, all medical and health-related research projects must receive an ethical preliminary approval from the Regional Committees for Medical and Health Research Ethics (REC).

Additional documented approval is necessary if you are researching an institution such as a school, prison, hospital or workplace. This approval should be collected from the institutional management before conducting the research.

What is personal data?

Personal data is anything that can be traced back to one person, either directly or indirectly, identifying who the information originated from. Keep in mind that combinations of background data can be personally identifiable.

NB! Note that while all reporting/publishing from your project is anonymous, you may still have processed personal data that is subject to notification.

Notification requirements for processing personal data collected as sound, image, text or number

You must report the project to NSD data protection services if you process personal data. This concerns both research and student projects. The project must be reported to NSD even if the personal data is replaced by a number, code, fictitious name or similar, which refers to a separate list of personal data.

The use of pictures and sound recordings of people also entails the processing of personal data if:

- the recording is processed or saved using electronic aids (on computer such as an audio or picture file)
- transcripts contain personal data and are processed electronically (computer), transcripts contain sensitive personal data and are systemized in a manual register

USN has formulated its own guidelines for processing audio files in research.[4]

The project manager or supervisor of the student project is responsible for notifying NSD about the project. This notification must take place no later than 30 days before data collection begins. You are not allowed to start the project until you have received approval.

Risk assessment

You should complete a risk assessment prior to processing personal data; an assessment of privacy protection implications. The assessment will help prevent adverse incidents or deficiencies in the processing of personal data. Measures are taken to protect the processing of research data that are relative to actual risks based on the risk assessment. Key aspects of the risk assessment are the scope of the project, the sensitivity of data and the duration of the project. In addition, you must be aware of the risks associated with IT data processing:

- Confidentiality: Prevent unauthorized persons from accessing the data.
- Integrity: No unintended or unauthorized alteration of data.
- Availability: Data cannot be lost and is available when access is required (for authorized persons).

Upon filling out the form to the NSD Data Protection Official, you must answer and describe what you deem as a risk regarding your processing of personal data and what you intend to do to reduce this risk.

An extended privacy protection impact assessment will be required in particularly intrusive projects, such as projects where sensitive personal data is processed on a large scale. These assessments are

[4] Guidelines for processing audio files in research by USN
https://www.usn.no/forskning/publisere/retningslinjer-for-behandling-av-lydfiler-i-forskning-ved-usn-article218068-26849.html

more extensive than usual and must be planned in cooperation with the institution's management, USN's Data Protection Official[5] and NSD.

Consent

Participation in research projects where personal data is not treated anonymously should be based on documented consent from the participants.

Research participants may not be included in a research project until a declaration of consent is signed. The declaration of consent can be collected electronically. Informed consent is the communication and the information that allows each participant, regardless of age and mental capacity, to make an educated decision whether to participate in a research project or not. An informed consent should provide the necessary information about the study and shall serve as a formal agreement for each participant to participate.[6]

It is mandatory to describe how the participants' confidentiality will be protected during the project and in the results section. As a general rule, the informed consent should contain information about long-term storage and sharing of anonymous data. An example could be: "Your answers from the questionnaire will be delivered to and in long-term storage in the (for example...) USN Research Data Archive and made available for reuse for new research purposes and/or teaching.[7]

Key principles of consent:

- The capacity to consent of legally competent persons can cease to apply due to physical or psychological impediments that obviously impede their understanding of what the consent includes.
- Incapacitated people are to consent themselves as much as is possible. If this is not possible, their legal guardian shall consent on their behalf.
- Health research: Minors between 16 and 18 years may consent unless otherwise follows from specific statutory provisions or the nature of the action. Parent/guardian consent is required if the research involves bodily intervention or drug testing. The Health Research Act Section 17 has further provisions regarding the capacity to consent.
- Other research: Depending on the nature and scope of the project, common practice is that children need to have reached 15 years of age before they can consent to participate in research. The age limit is 16 -18 years if sensitive personal data is involved. If minors (under 18 years of age) are to provide valid consent to the processing of personal data, it is presupposed that they understand the consequences. The possibility of understanding involves factors such as age, nature and scope of personal data and the purpose of the data collection. Information must always be provided regarding which age limit applies when minors disclose personal data.
- When minors are included, age-appropriate inquiries must be prepared that take into account maturity and background of experience.
- If research occurs without consent, the project manager is obliged to inform the participants unless there are exceptions in the disclosure requirements.

[5] Here you will find information about USN's Data Protection Official:https://www.usn.no/om-usn/organisering/rad-og-utvalg/personvernombudet-article217184-6754.html

[6] Read more about consent on the websites of NSD, REC and The Norwegian Data Protection Authority (DPA).

[7] Read more at http://bibliotek.usn.no/kvar-du-kan-lagre-forskningsdata/category30791.html about where you can store your data.

Is assessment of the capacity to consent a difficult topic in your project? Read more on the home page of The Norwegian National Research Ethics Committees, for example. Please contact NSD data protection services, REC or USN's Data Protection Official.

The rights of the research participants

If a person can be identified in the data material, they have the right to:

- access the personal data that is recorded about them,
- correct the personal data that is about them,
- delete the personal data that is about them,
- receive a copy of their personal data (data portability), and
- send a complaint to the Data Protection Official or The Norwegian Data Protection Authority (DPA) regarding the processing of their personal data.

This is what you have to disclose in your information and consent forms.

Changes to a project in progress

If significant changes are made to the project, an application should be sent to REC/ notification to NSD. Your changes cannot be put into operation until REC/NSD has given feedback. Check the notification of change form at NSD and REC if you are unsure about whether the changes are such that they need to be announced.

Roles and tasks

If you are a project manager of a research project

- The project manager should send a notification to the Norwegian Centre for Research Data (NSD) and also seek approval from the Regional Committees for Medical and Health Research Ethics (REC), if necessary. In addition, where relevant, make sure that agreements required for the safeguarding of information security and personal privacy are entered into by those who have authority to do so.
- The project manager should prepare the necessary information and the consent form.
- The project manager has to inform the head of research at the associated faculty (Pro Dean research) before sending a notification to NSD/REC and submit the notification/s if the head of research asks for it.
- The project manager should undertake a risk assessment and, if necessary, consult with USN's Data Protection Official; NSD's data protection services regarding research and/or REC if an extended personal privacy impact assessment is required after the General Data Protection Regulation Article 35 (DPIA)
- The project manager should prepare a data management plan (DHP). A template for DHP is available on NSD's website.
- The project manager must ensure access control of active research data if confidentiality is required when processing personal data in the project. Please contact forskningsdata@usn.no if you need instructions.

If you are a student or a supervisor in a student project

- The supervisor functions as the project manager in student projects. Ph.D. studies are defined as regular research projects.

- The supervisor must assess whether the student project processes personal data, whether the data is sensitive and whether it falls into the category of medical and health-related research.
- The supervisor should assess whether the planned processing will be in accordance with the basic personal privacy principles of the EU's General Data Protection Regulation (GDPR), including the legal basis (statutory provision) for the processing or plans to obtain consent from the project participants.
- Sensitive personal data should not be collected in Bachelor's projects, as a general rule. This should also be avoided as much as possible in Master's projects and must be the subject of discussion between student and supervisor.
- The supervisor should assess whether the student project can be carried out without notification, i.e. that no personal data is processed online in the student project. (see more information in the next section)
- The student should prepare a data management plan in collaboration with the supervisor.
- The supervisor, or the student if the supervisor has given approval, must send notification to the Norwegian Centre for Research Data (NSD) no later than 30 days before the processing begins. the student, in close collaboration with the supervisor, fills in the notification form to NSD, as well as preparing the accompanying attachments. If the project concerns health research, the project manager should submit an application for preliminary approval to the Regional Committees for Medical and Health Research Ethics (REC).
- The student should have carried out necessary training regarding data security and personal privacy before processing personal data in student projects.

Anonymity, Anonymized and Pseudonymized

Anonymous data collection is possible if the project is a survey with a single round of questioning. This is unlike iterative questioning (time series) that requires a scrambling key. It is always preferable if anonymous data collection is possible.

Online forms can be completely anonymous, i.e. so that the respondent's e-mail and IP address can at no time be attached to the questionnaire. If an online questionnaire tool has a preference function where the respondent's IP address is not registered, this will provide sufficient anonymity and the notification requirements are waived if all other terms and conditions are safeguarded.

Please note that the rights of research participants (of course) do not come into effect during anonymous investigations. Without personally identifiable data, the questioning is anonymous and it is not possible to withdraw consent. For example, you can provide information about this in the following manner: "Participation in the survey is voluntary and anonymous. If you respond, you have consented to participate. Simply don't respond if you don't want to participate. If you change your mind during the questioning, do not submit the form and cancel what you have written. After the form is delivered, responses cannot be withdrawn because they are delivered anonymously and cannot be traced back to you."

Anonymization

Anonymization means making personal data anonymous. This means that no individual can be recognized in the data material that remains. You need to analyse your data material and decide what information you need to remove or rewrite.

Usually, anonymization involves:

- deleting data that directly identifies someone, including scrambling keys/name lists.
- deleting or reworking data that indirectly identifies someone (by broadly categorizing variables such as age, location and school, for example)
- deleting or editing/censoring audio recordings, pictures and video recordings

You are usually allowed to store anonymous data material after the project has ended. However, you must ensure that you have revised the data material in such a way as to ensure that no individual can be recognized. However, in some cases you still need to delete the entire data material. For example, this is the case if you have declared to the participants that you will delete the data material, or when the data owners, such as SSB, instruct you to delete the entire data material at the end of the project.

Think carefully when writing about anonymization in the declaration of consent that your informants will sign. You must make sure that your informants understand that personal data will be processed by a few selected researchers while the project is in progress. Anonymization will take place at the end of the project which enables publishing and long-term data storage.

Note that you don't need to delete personal data in the publication/task. Personal data can usually be published if you have a scientific reason for it and you have obtained consent from the participants involved.

Pseudonymization

Pseudonymization means that certain parameters that directly identify someone are replaced with pseudonyms which will still be unique indicators.

The data is pseudonymized if names, social security numbers or other unique characteristics are replaced by a number, code, fictitious name or similar, which refers to a separate list containing the real personal data (scrambling key). Note that data which indirectly identifies someone must also be categorized in broad categories or removed before it can be considered pseudonymized. For example, broad categories could mean a region instead of a specific municipality or city and age ranges (10-19 years, 20-29 years, etc.) instead of stating the precise age. The only way to identify individuals in pseudonymized data material is through the name list/scrambling key.

Pseudonymized data is considered personal data, regardless of who stores the name list, where and how it is stored.

De-identification means that all unique characteristics have been removed from the data so that they can no longer be associated with an individual. Pseudonymized and de-identified personal data are overlapping concepts in the General Data Protection Regulation.[8]

Internet research

If you are going to research information that has been made available online, you have to report your project if you plan to process personally identifiable information. Examples of such processing of personally identifiable information may include saving documents from open or closed discussion forums and “nicknames” of discussion participants. Furthermore, direct quotations can be searchable and traced back to individuals.

[8] Do you require more information? Read The Norwegian Data Protection Authority’s guide (2015) Anonymization of personal data.

As a general rule, you must provide participants with information and obtain consent regarding the processing of personal data in connection with internet-based research projects. However, some cases may be exempt from the obligation to inform. You can find more about internet research on NSD's websites and the Guide to Internet Research from The National Committee for Research Ethics in the Social Sciences and the Humanities (NESH), released in September 2018.

Collecting data abroad

If you are a student/researcher at an institution in Norway and wish to collect personal data abroad, the application should be sent to NSD/REC in the same manner that data collection takes place in Norway.

Research data management

USN has complied guidelines for managing research data.[9] All digital processing of personal data in research can be stored in USN's own research archive: Research Data Archive (for data that is not sensitive). If it is sensitive data, it can be stored on the P-server or at the University of Oslo via the Services for Sensitive Data (TSD). Unfortunately, the P-server is not available to students but employees can create a folder to store the students' sensitive data. Both employees and students can store sensitive data at TSD. However, one has to pay for this storage (about 20,000 Kroner a year, including VAT). A common project can be created for a group of students. Please contact forskningsdata@usn.no if you need instructions.

The project manager is responsible for the data that the project collects and uses and must have access to all research data that the project includes. The project manager assigns access rights and keeps track of who is allowed to access the data. The project manager is also responsible for managing active research data and for the deleting and/or storage of data in an adequate way when the project ends.

The supervisor is the formal project manager regarding student projects, while the student carries out the tasks agreed with the supervisor.

Active research data is owned by USN as the Data Controller. This does not apply to students. As a rule, employees who leave or stop working must assign their active data to the research group that they are part of. The notification of change to NSD or REC must also be considered.

Regardless of the kind of research data you have, whether it is personal data, confidential or not, you must make sure that access and storage are secure, both electronically and physically. The measures must be in relation to the degree of personal privacy, commercial interests and intellectual property rights. Security also involves that you must pay particular attention when data is deleted from the project folders or from external devices such as recording equipment and measuring instruments.

Therefore, be aware of all the measures required to reduce the risk of accidental or malicious destruction or modification of data. Keep in mind that security is just as much about you 'making a mistake' as it is about unauthorized persons obtaining your data.

[9] Guidelines for the management of research data at the University of South-Eastern Norway http://bibliotek.usn.no/retningslinjer-for-forskningsdata/category32812.html