Guidelines for processing of personal data in research and student projects at UiT The Arctic University of Norway (UiT)

Adopted by the University Director		Date: 19.11.2018	
Unit responsible	Research, Education and Communication Division (FUF)	Archive ref.	2018/5429-1
Updated with new department names on 18.2.2019		Archive ref.	2018/5429-4
Replaces	Routines for processing of personal data in research and student projects at the University of Tromsø	Archive ref.	2010/2582-17

This is a translation. The Norwegian original has official status.

1. Introduction

The guidelines are an internal control system that apply for research projects and student projects at UiT The Arctic University of Norway

- where personal data is processed wholly or partly by electronic means
- in the case of manual processing of personal data when the data is or should be in a personal data filing system

Personal data shall not be processed in student projects under the master's level unless necessary based on the learning outcome.

The system shall determine the division of responsibilities and security strategy, etc. and as such serve as an aid

- for researchers/students who are writing a thesis to ensure that the planning, implementation and completion phases of the project are in accordance with the provisions of the Personal Data Act
- for the management and research administration to keep track of personal data that has been processed for research purposes
- for the management and the research administration to supervise the research, prevent and rectify any discrepancies

2. Definitions and explanations (Refer also to Article 4 of the GDPR and the Norwegian Centre for Research Data (NSD) *Vocabulary* list.)

Anonymous data *(Anonyme opplysningar)*	Anonymous data is data that cannot be attributed to identifying a natural person, neither directly through name or social security number, indirectly through background variables, nor through a list of names or through an encryption formula and code/scrambling key. De-identified data are not anonymous.
Basis for the processing *(Behandlingsgrunnlag)*	The condition that makes it lawful to process personal data, e.g. compliance with a legal obligation or a contract with the data subject, etc. These are stipulated in articles 6 and 9 of the GDPR. The most practical for research projects is that you gain consent from the informant.

Contact person (the person with day-to-day responsibility) – *(Dagleg ansvarleg)*	The person who determines the purpose of the research project and has the day-to-day responsibility for ensuring the duties of the data controller are fulfilled. The project leader of a research project has the day-to-day responsibility for the project. This shall be a person who is employed at UiT.
Contact person (the person with day-to-day responsibility) for student projects – *(Dagleg ansvarleg for studentprosjekt)*	The (main) supervisor is the contact person (the person with day-to-day responsibility) for the student project, including PhD projects.
Data controller *(Behandlingsansvarleg)*	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, cf. Article 4 (7) of the GDPR. At UiT: The university represented by the University Director.
Data processor *(Databehandlar)*	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. A written agreement must be entered into. Click here to download the template for the data processor agreement at UiT.
Data protection officer *(Personvernombod)*	Public bodies which process personal data must have a data protection officer. The data protection officer shall inform and advise about data protection and monitor compliance with the regulation/act, etc. (Article 39 of the GDPR). UiT's data protection officer is employed internally. NSD collaborates with UiT's data protection officer on matters relating to processing of personal data in research and student projects.
Data subject *(Registrert)*	The person to whom the data (research data) may be attributed.
Discrepancy *(Avvik)*	Discrepancy from the routines. The integrity and/or accessibility is breeched. Example: Unauthorized persons gain access to data, data gets lost or data is stored in a different way than planned.
Filing system *(Register)*	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (Article 4 (6) of the GDPR)
General Data Protection Regulation (GDPR)	*General Data Protection Regulation* (EU 679/2016). Refer to the new Personal Data Act.
Informant (respondent)	The person who informs.
Informed consent *(Informert samtykke)*	*Freely given informed consent is regarded as one of the most central requirements for research on humans where the research entails recording of data and/or any kind of discomfort, inconvenience or risk to the subjects of the research. Research must not be carried out on individuals or groups without their express permission. The requirement that the consent be freely given and informed means that the subjects must not be under any kind of pressure when they give*

	their consent ("freely given" or "voluntary"), and that their consent must be based on knowledge of the research to be conducted ("informed").[1]
NSD	In these guidelines, the term 'NSD' means: *NSD as an adviser for UiT in matters relating to data protection in research and student projects*. NSD shall assist the data protection officer.
Obligation to give notification /notification (Internal obligation to give notification) – *(Meldeplikt/melding/ (intern meldeplikt))*	In these guidelines, the term 'obligation to give notification' means the *duty to get the project assessed by UiT*. The university is responsible for assessing whether the data processing is lawful. In practice, this means that the project leader of a project that will process personal data shall assess the consequences in consultation with UiT's data protection officer before processing of the data commences. This shall be done via notification to NSD, which will assist UiT's data protection officer in such cases.
Personal data *(Personopplysningar)*	Data or assessments relating to a natural person (the 'data subject') who can be identified or is identifiable • by reference to an identifier such as a name, an identification number, location data, an online identifier, or other personal characteristics • through one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (e.g. age, gender, occupation, nationality, institution, etc. through a photo, video or sound recording, etc.)
Processing of personal data *(Behandling av personopplysningar)*	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4 (2) of the GDPR) Be aware that all processing of personal data shall have a specific purpose.
Pseudonymisation *(Pseudonymisering)*	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. Such additional information must be kept separately (Article 4 (5) of the GDPR). This is a form of de-identifying and is not the same as anonymisation.
Special categories of personal data *(Særlege kategoriar personopplysningar)*	Equivalent to the term "sensitive personal data" in the former Personal Data Act. Article 9.1 of the GDPR defines special categories of personal data as: *Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely*

[1] From the article consent by Hallvard J. Fossheim, The Research Ethics Library

	identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. Goal and strategy

Data protection involves every individual being able to easily check when, what and how much personal data has been disclosed to others. This makes demands on researchers and students who use personal data in a project. The purpose of these guidelines is to create good routines so that personal data in research and student projects are processed in accordance with the applicable legislation, and that the university fulfils its responsibility.

4. Roles and responsibilities

As data controller, the University Director has the overarching responsibility. The responsibility is otherwise divided as follows:

- A researcher is responsible for the processing of personal data in the project(s) he/she establishes.
- A supervisor is responsible for the student's processing of personal data in the project(s) established.
- A student is responsible for following instructions he/she receives from his/her supervisor concerning the processing of personal data in his/her project.
- The faculties, The Arctic University Museum of Norway and Academy of Fine Arts (UMAK) and The University Library of Tromsø (UB) are responsible for
  - good internal routines so that that notification is given of projects that are subject to notification
  - personal data in research and student projects being processed in accordance with GDPR
  - performing a risk assessment of all research and student projects[2]
- The Financial and Organisation Division (ORGØK) is responsible for providing the necessary training to
  - Academic managers
  - researchers, supervisors and students
  - administrative staff involved in research administration
- The Director of Research is responsible for the maintenance, evaluation, control and revision of these guidelines and furthermore shall maintain an overview of all research and student projects which involve the processing of personal data.
- The Director of the Department of Information Technology is responsible for the management of information security.
- The Faculty of Health Sciences determines the guidelines for organisation of research that fall under the provisions of the Health Research Act. These guidelines apply for the entire UiT. NSD shall be notified of all projects involving personal data in accordance with UiT's general guidelines (these guidelines).
- Everyone shall familiarise themselves with and comply with UiT's Information Security Management System (see uit.no/sikkerhet)

5. Relevant documents

- Personal Data Act
- General Data Protection Regulation (GDPR)[3] (GDPR). The regulation forms part of the Personal Data Act.
- Information Security Management System, UiT
- Principles and guidelines for research data management at UiT

[2] The routines are being drawn up.
[3] Scroll down to Article 1 where the GDPR begins.

- The provisions relating to Duty of secrecy in Sections 13 – 13 f. of the Act relating to procedure in cases concerning the public administration (Public Administration Act)
- Act on medical and health research (Health Research Act)
- Act on Personal Health Data Filing Systems and the Processing of Personal Health Data (Personal Health Data Filing System Act)
- Other acts and regulations related to personal health data filing systems

6. Checklist for researchers

Are you going to have the day-to-day responsibility for a project which involves processing personal data? If so, you must find out whether the project is subject to notification to NSD.

I. Planning

- Allow plenty of time. If the project is subject to notification, such notification must be given at least 30 days before the processing begins.
- Assess whether it is necessary to collect personal data. In NSD's list of *Frequently asked questions*, you will find information about how a project may be carried out without being subject to notification.
- If it is necessary to collect personal data: Assess which data you must collect based on the purpose of the project.
- If you are unsure whether the project is subject to notification: Take the notification test. If you are still in doubt, ask NSD.
- Are you going to ask the informants for personal data? If so, preparing an information letter and consent form, cf. Section 9 of these guidelines. (NSD has information about this here).
- Have a conscious attitude towards and draw up a plan for secure storage and processing of data.[4] The data must be securely stored in accordance with UiT's Information security management system. Check uit.no/sikkerhet and the point below concerning risk assessments.
- If you plan to use a data processor, you must enter into a data processor agreement.
- The project must be risk assessed. Follow UiT's routine for risk assessment[5].
- If the project is subject to notification: Notify NSD. Attach documentation confirming a risk assessment has been performed.

Notify NSD if the project does not start or has undergone other changes of relevance for the assessment of the project.

II. Implementation

When NSD has recommended the plan and other necessary approvals[6] and the plan for secure storage of data is in place, you may commence the project.

- Ensure that the project participants receive the necessary training.
- Gain consent from any informants, cf. Section 9 below. NSD has information on this here. If a basis of processing other than consent shall be used, the assessment of this and any permit(s) must be filed.
- Ensure that data is stored and processed in accordance with UiT's Information security management system. Check uit.no/sikkerhet.

Notify NSD if the implementation of the project takes longer time than planned or of other factors of relevance for the assessment of the project.

III. Completion

End the project in accordance with the plan:

[4] Be aware of the obligation to draw up a data processing plan. Check 4.2 of the *Principles and guidelines for research data management at UiT*

[5] The routines are being drawn up.

[6] For example, REK approval for projects pursuant to the provisions of the Health Research Act

- Is the data material to be anonymised? Information about anonymising is in the vocabulary list under Anonymous data.
- Is the data material to be erased? If so, erase it
- Is it relevant to file the data? If so, you must document that you have permission to do so. The contact person must seek advice from the data protection officer, or NSD which advises the data protection officer, before a decision is made concerning filing of the data. The general rule is to erase or anonymise data. For filing of data related to health research, refer to the *Routines for health research*.

Notify NSD if the implementation of the project took longer than planned or of other factors of relevance for the assessment of the project.

When the project should have ended, NSD will send a link you may use to send your final report.

7. Checklist for supervisors

Are you going to be a supervisor for a student who will write a paper/thesis which involves processing personal data? As a supervisor, you are responsible for ensuring that any personal data in the student's project is processed in accordance with the requirements. You must find out whether the project is subject to notification to NSD.

I. Planning

- Allow plenty of time. If the project is subject to notification, such notification must be given at least 30 days before the processing begins.
- Assess together with the student whether it is necessary to collect personal data to implement the project. In NSD's list of *Frequently asked questions*, you will find information about how a project may be carried out without being subject to notification.
- If it is necessary to collect personal data: Ask the student to assess which data he/she must collect based on the purpose of the project. Quality assure the plan.
- If you are unsure whether the project is subject to notification: Ask the student to take the notification test. If you are still in doubt, ask NSD.
- Is the student going to ask the informants for personal data? If so, ask him/her to prepare an information letter and consent form, cf. Section 9 of these guidelines. (NSD has information about this here). Quality assure the letter.
- Draw up a plan for secure storage and processing of the data together with the student[7]. The data must be securely stored in accordance with UiT's Information security management system. Check uit.no/sikkerhet.
- If a data processor will be used, you must enter into a data processor agreement.
- The project must be risk assessed. Follow UiT's routine for risk assessment[8].
- If the project is subject to notification: Together with the student, notify NSD about the plan for collection of personal data.

Together with the student, notify NSD if the project does not start or has undergone other changes of relevance for the assessment of the project.

II. Implementation

When NSD has recommended the plan and other necessary approvals[9] and the plan for secure storage of data is in place, the student may commence the project.

Ensure that

[7] Be aware of the obligation to draw up a data processing plan. Check 4.2 of the *Principles and guidelines for research data management at UiT*

[8] The routines are being drawn up.

[9] For example, REK approval for projects pursuant to the provisions of the Health Research Act

- the student and any other project participants receive the necessary training.
- consent is gained from any informants, cf. Section 9 below. NSD has information on this here. If a basis of processing other than consent shall be used, the assessment of this and any permit(s) must be filed.
- data is stored and processed in accordance with the plan – the data must be securely stored and processed in accordance with UiT's Information security management system. Check uit.no/sikkerhet.

Together with the student, notify NSD if the implementation of the project took longer than planned or of other factors of relevance for the assessment of the project.

III. Completion

Ensure that the project is ended in accordance with the plan.

- Is the data material to be anonymised? If so, agree with the student who will do this. Information about anonymising is in the vocabulary list under Anonymous data.
- Is the data material to be erased? If so, ensure that the student erases it.
- Is it relevant to file the data? If so, you must document that you have permission to do so. Seek advice from the data protection officer, or NSD which advises the data protection officer, before a decision is made concerning filing of the data. The general rule is to erase or anonymise data. For filing of data related to health research, refer to the *Routines for health research*.

Together with the student, notify NSD if the implementation of the project took longer than planned or of other factors of relevance for the assessment of the project.

When the project should have ended, NSD will send a link you may use to send your final report. Send the final report together with the student or ensure that the student has sent the final report.

8. Checklist for students

Are you going to write a paper/thesis which involves the processing of personal data? If so, in consultation with your supervisor, you must find out whether the project is subject to notification to NSD.

I. Planning

- Allow plenty of time. If the project is subject to notification, such notification must be given at least 30 days before the processing, i.e. the work on your paper/thesis, begins.
- Is it completely necessary to collect personal data to implement the project? Assess this together with your supervisor. In NSD's list of *Frequently asked questions*, you will find information about how a project may be carried out without being subject to notification.
- If it is necessary to collect personal data: Assess which data you must collect.
- If you and your supervisor determine that the project is subject to notification: Together with your supervisor, notify NSD about the plan for collection of personal data.
- If you are unsure whether the project is subject to notification: Take NSD's notification test. If you are still in doubt, ask NSD.
- Prepare an information letter and consent form to any informants when your supervisor asks you to do this, cf. Section 9 of these guidelines. (NSD has information about this here).
- Draw up a plan for storage of the data together with the student. The data must be securely stored in accordance with UiT's Information security management system. Check uit.no/sikkerhet.

II. Implementation

When NSD has recommended the plan and other necessary approvals[10] and the plan for secure storage of data is in place, the student may commence the project.

[10] For example, REK approval for projects pursuant to the provisions of the Health Research Act

Ensure that

- consent is gained from any informants, cf. Section 9 below.
- data is stored and processed in accordance with the plan – the data must be securely stored and processed in accordance with UiT's Information security management system.

Together with your supervisor, notify NSD if the implementation of the project took longer than planned or of other factors of relevance for the assessment of the project.

III. Completion
End the project in accordance with the plan.

- Is the data material to be anonymised? Information about anonymising is in the vocabulary list under Anonymous data.
- Is the data material to be erased? If so, erase it.
- Is it relevant to file the data? If so, you must document that you have permission to do so. Your supervisor shall seek advice from the data protection officer, or NSD which advises the data protection officer, before a decision is made concerning filing of the data. The general rule is to erase or anonymise data. For filing of data related to health research, refer to the *Routines for health research*.

Together with your supervisor, notify NSD if the implementation of the project took longer than planned or of other factors of relevance for the assessment of the project.

When the project should have ended, NSD will send a link you may use to send your final report. Send the final report together with your supervisor or inform your supervisor that you have done this.

9. Information to the data subject / gaining of consent

When personal data has been collected from a data subject, the data controller must provide the data subject the following information of their own initiative

- that UiT The Arctic University of Norway[11] is the data controller
- the contact details to the data protection officer at UiT
- the purpose of processing the personal data
- whether the personal data will be disclosed to other parties and, if so, who is the recipient
- that it is voluntary to give the personal data
- about their right to lodge a complaint with the supervisory authority, e.g. the Norwegian Data Protection Authority (DPA)
- about to right to obtain access and rectification of any inaccurate personal data
- any other information that enables the data subject to utilise their rights pursuant to the act and regulation in the best manner possible

When processing of personnel data is based on informed consent from the data subject, cf. Art. 6 no. 1. (a) or Art. 9 no. 2. (a) of the GDPR, a voluntary, explicit statement must be gained from the data subject confirming that he/she accepts processing of his/her personal data, cf. Art. 7 of the GDPR, cf. Art. 4 (11) of the GDPR.

When data has been collected from sources other than the data subject, the data controller must inform the data subject about what data has been collected and provide information immediately and of their own initiative as stipulated in the points above.

10. Storage and erasure of personal data

Personal data shall be kept for no longer than is necessary for the purpose(s) for which it is being processed. The contact person must ensure that the personal data is erased.

[11] Provide details to the data subject about who they may contact

Personal data may be stored at the university for longer periods for scientific purposes in cases where the public interest in archiving the data clearly outweighs the disadvantages such storage may have for the individual informant. Decisions concerning storage and the place of storage are made by the University Director based on a proposal from the contact person for the processing. In cases where a decision has been made to store data, the University Director shall ensure that the data is not kept in such a manner that makes it possible to identify the informant for longer than necessary.

The contact person must inform UiT when the personal data have been erased. This must be done by informing NSD in the final report or specific notification.

11. Security requirements

The data in the project must be processed in accordance with UiT's Information security management system. All projects must be risk assessed before start-up. The contact person is responsible for ensuring this has been done. Follow UiT's routine for risk assessment[12].

The university's IT resources must be used for any electronic processing of personal data in research and student projects. Personal data in research data must only be stored in systems and services that are approved for this purpose and are in accordance with the requirements of the relevant regulations. Check uit.no/sikkerhet. The contact person shall ensure that the data material is stored in a place where regular backups are made under the auspices of UiT.

Code lists, scrambling keys and other material that may be used to identify the people must not be stored together with the data.

Privately owned equipment must not be used for the storage or other processing of personal data.

The user must exercise caution concerning the storage and transport of laptops and external storage devices to minimize the risk of theft and damage. External storage devices must be encrypted.

If the research project plans to use data processor, a written agreement must be entered into and the above-mentioned requirements must be fulfilled.

Private communication platforms (e-mail, Messenger, etc.) must not be used for correspondence about the project.

Following a risk assessment, the university will be able to impose further security requirements.

12. Checklist for faculties, UMAK, UB

Every unit is responsible for having good internal routines in place to ensure that personal data in research and student projects is processed in accordance with the provisions of the General Data Protection Regulation.

- Keep an overview of all research and student projects which involve the processing of personal data. UiT's overview is stored at NSD here.
- At least one employee with responsibility for internal control must have access to NSD's notification archive. Such access is given by Olaug Husabø at FUF.
- Ensure that internal control (evaluation) of the project is performed annually. The head of administration shall appoint a group to perform this evaluation. Such groups must contain at least one researcher and one person with information technology skills.
- 10% of research and student projects that are in progress must be evaluated with data protection in mind:

[12] These routines are being drawn up.

- This evaluation shall map whether the security requirements in the Information security management system have been fulfilled:
  - Is the project risk assessed?
  - Has a data processor been used? If so, is the necessary agreement in place?
  - Are all necessary approvals in place?
  - Does the project disclose data to other parties? If so, dies a basis for such disclosure exist?
- The result of the evaluation shall be documented in writing and a copy shall be sent to the data protection officer, university director and the contact person for the project.

13. Processing of questions concerning access, etc.

- Questions concerning access to personal data in research and student projects at UiT shall be sent to the University Director via eDialog UiT, cf. the link here.
- Questions shall be processed in accordance with the guidelines. UiT shall answer questions as quickly as possible and no later than 30 days after the question was received.

14. Disclosure of personal data

Personal data must not be disclosed to third parties. However, such disclosure may occur

- if the data subject was informed when the data was collected, and the informant has given his/her consent
- with the consent of the informant
- pursuant to a statute or a regulation issued pursuant to a statute

15. Rectification/erasure of personal data

- When a data subject requests that personal data concerning him/her be erased, this must be done as quickly as possible, and the person concerned shall receive a response no later than 30 days after the request was received.
- If a data subject provides notification that there is inaccurate or incomplete personal data concerning him/her in a project, or data the project is not permitted to process, you must rectify the error and notify the contact person about this.
- If you become aware that inaccurate or incomplete personal data are registered in a project, or data the project is not permitted to process, you must rectify the error and notify the contact person about this.
- If you discover an error that you are not permitted to rectify, you must notify the error to someone who is authorised to rectify it.

16. Discrepancy processing

Discrepancies concerning information security must be notified to the Department of Information Technology. Other discrepancies must be notified to the data protection officer by e-mail at personvernombud@uit.no.

17. Maintenance and revision of the routines

The Research, Education and Communication Division (FUF) is responsible for revision of UiT's internal control system for processing of personal data in research and student projects, including control of the choice of routines and how these routines are followed. NSD's archive of research and student projects and REK Nord's project register form the basis for this work.

An employee at FUF with specific authority shall be the contact with NSD. He/she is responsible for providing information to researchers and students about the data protection legislation, the obligation to give notification and the obligation to obtain a licence, arrangements for filing of personal data after

completion of the project and the university's routines for processing personal data in research and student projects.

Every second year, FUF must control a selection of research and student projects. The purpose of this control is to check whether the processing of personal data occurs in accordance with the university's guidelines, as informed about in the notification to NSD, in accordance with any licencing conditions and any recommended special security routines for the project.

After the project has ended, FUF shall control that the personal data are erased or transferred to a filing system.

18. Evaluation of the guidelines and routines

The University Director is responsible for evaluating the guidelines and routines. Such evaluation must be performed no later than one year after approval and then at least every third year.

22.2.2019 OH, AFU
English translation 15 April 2019.