THE UNIVERSITY OF STAVANGER	*Management of research data:* Guidelines for the processing and storing of research data containing personal data in student projects at the University of Stavanger	
Approved by: UiS Data protection officer (power of attorney)	Date: 27/05/2021	Revision no.: 1.2

Common guidelines for the processing of personal data in student projects at Bachelor's and Master's degree level at the University of Stavanger. (PhD candidates must follow the guidelines for researchers at the University of Stavanger).

1. Scope and definitions

These guidelines shall apply to all student projects at the University of Stavanger that involve the processing of personal data. The requirements concerning processing of personal data in student projects correspond to the requirements applicable to researchers at the University of Stavanger. The following also applies to student projects:

1. All students that will process personal data in connection with student assignments must read the relevant information at the Norwegian Centre for Research Data (NSD) web pages and to investigate whether the project must be reported to the NSD.
2. It is recommended that Bachelor's students do projects without processing personal data, with the exception of **joint assessment** or as part of a researcher-led project. The use of anonymous registry data, journal data or other anonymised data is recommended. If a student and supervisor wish to implement a student project that involves the processing of personal data, the NSD guidance *How to implement a project without processing personal data?* – must be reviewed before a final decision is made.
3. The student should only submit a notification form to the NSD in consultation with their supervisor and the form must be shared with their supervisor when reporting the project to the NSD.
4. The student will be responsible for following up on all feedback from the NSD and must not start a project that involves the processing of personal data before permission has been granted by the NSD. The student must confirm in writing to their supervisor via e-mail that permission has been granted.
5. The student will be responsible for submitting a notification/feedback to the NSD upon conclusion of the project to confirm that all data has been deleted/anonymised. The student must also confirm this in writing to their supervisor.
6. If private devices will be used in connection with the management of collected data (e.g. personal PC, tape recorders, etc.), please refer to the relevant item of the guidelines.

These guidelines are complementary to the *Policy for data security and protection of privacy at the University of Stavanger,* dated 24/09/2019 and *the Regulations for data security and protection of privacy, dated 02/06/2020.*

Definitions:

Personal data: Personal data is all information that can be linked to a physical person or persons. Information may be available as text, images, video, sound recordings or electronic traces, for example IP addresses or activity logs in IT systems. In order for information to be considered personal data, it must be possible to identify the person or persons to whom the information relates. (In accordance with Article 4-1 of the Norwegian Personal Data Act)

Processing of personal data: "Processing" refers to all operations or sequences of operations on personal data in administration, research, customer service, etc., whether automated or not. Examples include collection, registration, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, release through transfer, dissemination or other forms of disclosure, compilation or merging, restriction, deletion or destruction. (Article 4-2 of the Norwegian Personal Data Act)

Directly identifiable personal data: people can be directly identified by their name, date of birth and personal identity number or other unique personal characteristics.

Data Protection Officer: The Rector is the chief data protection officer. Each unit is responsible for implementing data security at the unit. The faculty management represented by the Dean is responsible for implementing these guidelines and providing information concerning these guidelines to the units. Unit managers are responsible for the implementation and follow-up within their units.

Daily responsibility: The student and the appointed supervisor have the daily responsibility for fulfilment of the data protection officer's obligations for the student project. The supervisor will be responsible for student projects that have been reported to the NSD. If the supervisor is not employed by the University of Stavanger when the project is discontinued, the supervisor must agree with the unit manager as to how the responsibility to NSD will be followed up before they leave as a supervisor.

2. Responsibility

Students and their supervisors shall ensure that the managing of research data is planned and documented at the beginning of a research project and that data containing personal information is processed in line with these collection and storage guidelines. This also applies to the storage of documentation associated with the project concerned, e.g. reports to the NSD (the Norwegian Centre for Research Data) and information and consent forms.

It is important to assess whether it is necessary to utilize a data management plan (DMP) for the project. If there is an external funder associated with the project, it is important to investigate whether the funder sets requirements concerning the use of a DMP. In such a case, the University of Stavanger recommends using the Data Management Plan template from the NSD. Such plans explain how data should be processed during the course of a project period and after the project has been completed. The University of Stavanger has published a separate overview of the classification and management of various types of personal data.

3. Notification obligations relating to projects that involve the processing of personal data

3.1 Notification to NSD Data Protection Services

The Norwegian Centre for Research Data (NSD) provides privacy services for the University of Stavanger. Student and research projects that involve the processing of personal data must be reported to the NSD.

This also applies to projects relating to medical and health research after 1 January 2020. The project must be reported to the NSD no later than 30 days before data collection is due to commence. In order to reduce the administrative processing time at the NSD, we recommend that you read the Checklist before submitting the notification form.

Plans relating to the processing of personal data must be approved **before** commencing a project.

In the event that changes are made to the project programme relating to the information that forms the basis for the NSD's assessments, the change must be reported by logging into My page and adding the changes to the notification form as specified on the NSD web pages.

3.2 Assessment of research projects by the Regional Committees for Medical and Health Research Ethics (REK)

Medical and health research projects must apply to the NSD, which can be done in parallel with an application for ethical approval submitted to the Regional Committees for Medical and Health Research Ethics (REK).

All projects that fall under the Norwegian Health Research Act must be approved by the REK before commencement. The REK has its own portal which contains information about deadlines and processing times. The relevant forms are also available there. Access to forms and digital applications is contingent on having a user's account.

The REK undertakes ethical research assessments on the basis of applications and research protocols with attachments. The REK may request supplementary information. The project must not commence before approval from the REK has been obtained and the supervisor acting as the research manager has conducted an internal assessment. The REK will notify the project manager and research manager about the outcome of its assessments. Whoever has daily responsibility for a project must report it as soon as possible. The notification form and guidance and information about deadlines and processing times can be found at the REK web pages.

The appointed academic supervisor shall be responsible on a daily basis for student projects containing personal data, cf. NSD Notification Form.

Links to information about projects subject to notification requirements, notification forms, guidance, information and consent forms, as well as key concepts can be found at the University of Stavanger web pages.

4. Information and obtaining consent when collecting personal data

It is important that the selection of participants/respondents are well informed about all aspects of a study so that they can fully assess whether or not they would like to participate. This applies to the

objectives, risks and any possible benefits. An information circular should therefore be drawn up containing questions and providing information about the study in question.

Consent shall be provided voluntarily, expressly and on the basis of adequate information. Read more about the terms and conditions on the NSD's web page. Here you can also find templates for information/consent.

5. Processing of enquiries, corrections and deletion

All enquiries about how the University processes personal data in respect of research and student projects shall be referred to the Data Protection Officer at the University of Stavanger: personvernombud@uis.no

6. Disclosure of personal data/access control

Personal data in research or student projects must not be disclosed to outsiders. Access control in respect of data shall be set up and documented. Normally only students and their supervisors shall have access, in line with the notification submitted to NSD Data Protection Services.

7. Storage and deletion of personal data

Personal data in research and student projects shall not be stored for any longer than is necessary for completing the purpose of any processing. The student must confirm via e-mail to the supervisor that data has been deleted/anonymised in accordance with the notification to NSD Personal Data Services.

Health research data and personally identifiable data must not be stored in an unsecured manner. Personal data must be deidentified/pseudonymised and audio/visual data must be encrypted (cf. Item 8). If a code list/code key, or any other materials which can be used for identifying someone, are used, such shall not be stored on the same machine or file server.

8. Security requirements and regulations concerning the use of personal equipment.

When personal data is processed electronically on a private computer in respect of projects for which the University of Stavanger acts as the Data Protection Officer, such data shall be stored in encrypted form so that no-one else is able to access the data.

All computers, including private computers, which are to be used for processing personal data shall be protected with relevant security mechanisms, including anti-virus software, activated firewalls and systems which regularly update operating systems and security mechanisms.

Students shall be personally responsible for ensuring that security copies and backups are made of data and that backups are stored securely/locked away.

Students must also be careful when it comes to third parties being able to view their screen when choosing a place of work for data processing.

When using laptops and external storage media, users must be careful when storing and transporting such equipment in order to minimise the risk of theft and damage.
External storage media means memory sticks, external hard disks, audio recorders and cameras, etc.

Students must use their University of Stavanger e-mail addresses for communication/correspondence in the research project (personal e-mail addresses must not be used).

Subject to assessment, university supervisors may call for further security requirements for individual projects.

8.1 Requirements relating to equipment/procedures when recording audio material/or videos/images

We refer to the UiS web pages for guidelines regarding the use of private units like mobile phones, iPad or tablets for recording sound or video (please see here for information on the requirements for using Zoom (in Norwegian), and here for information on requirements for the use of Nettskjema (in Norwegian). Both video and audio recordings are regarded as being personal data.

Students shall be personally responsible for obtaining any equipment needed, such as electronic audio recorders, or other compulsory equipment such as external hard disks, encrypted memory stick, etc.

Procedures for audio recording /video: UiS uses the Nettskjema app for audio recording. In addition, you must adhere to the Zoom guidelines when using video.

Please see further information about security mechanisms and encryption on the University of Stavanger web pages.

8.2 Important things to know about encryption

Encryption options: Please see information about encryption options on the University of Stavanger web pages.

It is **very important** that you understand that if you encrypt a unit, e.g. a whole hard disk, you will lose all the information stored on that unit if you lose the encryption key and your personal password. Information will then be lost and cannot be recovered.

9. Reporting deviations

Have any deviations/errors occurred during processing of research data/personal information?

Deviations must be reported:
The student and/or supervisor is responsible for immediately reporting any deviations.
Reports of breaches or possible breaches of privacy must be submitted to the Data Protection Officer via personvernombud@uis.no. The supervisor should also be informed if the student discovers discrepancies.

Reports of breaches or possible breaches of data security must be submitted to it-hjelp@uis.no