Personal Data Processing in Student Projects

Guidance for the HT Faculties

Approved by the Working Committee of the Faculty Board on 15 October 2025
Reg. no STYR 2025/1648

This Guidance is primarily intended for teaching staff, supervisors and course directors responsible for managing first and second-cycle student projects potentially involving the processing of personal data. For example, personal data is collected in connection with interview studies or participant observation used as material in a student project. In these cases, the processing of personal data constitutes a learning activity linked to an programmes' learning outcomes. This Guidance is intended to provide support for teaching staff working on such learning activities in their teaching and supervision.

The Guidance is supplemented with advice on collection, equipment, software, storage facilities, and other practical aspects of personal data processing in student projects. This practical advice is available on the HT Faculties' internal website.

Contents

Personal data and data protection at Lund University

Lund University must process personal data in accordance with the EU's General Data Protection Regulation (GDPR) and the Swedish Data Protection Act. The GDPR has two fundamental purposes. The first is to protect individuals' fundamental rights and freedoms, especially their right to the protection of personal data. The second is to facilitate the free flow of personal data within the EU. The Regulation's principles on the protection of individuals' privacy must be applied in a way that is consistent with the core tasks of higher education institutions, namely education, research and external engagement.

Within Lund University's remit, students and employees may process personal data for the purposes of education, research and external engagement, provided that this processing complies with the GDPR. The University must process personal data in a secure and correct manner, which among other things means that information must be protected against loss, corruption, and unauthorised access during processing.

Personal data and sensitive personal data

Personal data is defined as: *any information relating to an identified or identifiable natural person (often called **the data subject**). Simply expressed, it concerns information through which a person can be directly or indirectly identified* (see Article 4 of the GDPR). Examples of **direct personal data, or direct identifiers,** include names, personal identity numbers or coordination numbers, photos of people and voice recordings. **Indirect personal data, or indirect identifiers,** may include a person's job title, place of work, place of residence, email address, and information about their interests, or other factors that are specific to, for example, their physical, mental, financial, cultural or social identity, where this information can be traced to a specific person, either on its own or when combined with additional information.

Common security measures

Pseudonymised personal data are encrypted or coded data that require additional information in order to be linked to a specific person.

Anonymised data are data that can never, or can no longer, be traced to a living person. In anonymisation, all sources of identification have been removed. Please note that if there is a theoretical possibility of identifying a person by, for example, combining several apparently anonymised pieces of information, the combined information is then considered personal data and can no longer be regarded as anonymised.

Sensitive personal data

The GDPR distinguishes between personal data and sensitive personal data, the latter requiring stronger protection during processing. According to the GDPR (Article 9.1) sensitive personal data refers to data that discloses:

- ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership

or that refers to:

- genetic data
- biometric data used to clearly identify a person
- data concerning health or a person's sex life or sexual orientation.

According to the GDPR, the general rule is that processing sensitive personal data is prohibited, but exceptions can be made in certain situations. The following exceptions can be applied to student projects under certain circumstances:

- The data subject has given explicit consent to the processing of their personal data for one or more specific purposes (Article 9.2 a)
- The processing relates to personal data that has been manifestly made public by the data subject (Article 9.2 e)[1].

Personal data worthy of special protection

Certain types of data are considered to be integrity-sensitive and worthy of special protection and must therefore be processed with extra care. These types of data include:

- personal identity numbers or coordination numbers
- salary information
- data on legal violations (which has a special status in Swedish regulation, including the Ethical Review Act)
- evaluative data, such as information from staff appraisals or the results of personality tests or personality profiles
- information relating to a person's private sphere
- information on social relationships

In addition, children's personal data is also worthy of special protection. This is because children are not considered to be able to exercise their rights in the same way as adults, and they may have greater difficulty foreseeing the consequences of the processing of their personal data. It is therefore particularly important that supervisors, when applicable, assess whether processing the children's personal data is necessary. This assessment should be based on both age and the child's personal maturity, taking into account the type of personal data processing involved. For children up to and including the age of 14, a legal guardian's consent is required for participation in a study. From the age of 15, children may give their own personal consent; however, supervisors

[1] For more information on sensitive personal data, see https://www.staff.lu.se/support-and-tools/personal-data-and-data-protection/general-information/faqs

should consider whether it is appropriate for the student to discuss participation with the legal guardian, even though this is not a legal requirement.

Responsibilities and lawful grounds

Lund University processes personal data within the remit of its role as an education provider and research organisation, as well as in its capacity as an external engagement partner. As a general rule, the University is the personal data controller, unless the responsibility has been assigned to another party through a formal agreement. This means that the University – in practice the head of department or equivalent – is responsible for ensuring compliance with the GDPR.

According to the GDPR, the processing of personal data may only be conducted if it is supported by a **lawful ground.** Employees at Lund University can rely on five different lawful grounds (Article 6.1), of which the most common in education, research, and external engagement are **tasks in the public interest** and the **exercise of official authority**.

"Processing" is a broad term under the GDPR and encompasses everything that can be done with personal data. For example, personal data may be collected, recorded, processed, disseminated, stored, or deleted[2].

Conditions for personal data processing in student projects

Lund University is responsible for any personal data processing conducted by students as part of their education. This processing must be supported by the GDPR. Regarding personal data in student projects, Lund University's assessment is that, in normal cases, processing is supported by the lawful ground **task in the public interest**. In practice, this means that students may only process personal data if their supervisor determines that it is necessary to ensure that the students achieve the programmes' learning outcomes. The outcomes state in general terms that, upon completing the programme, students should have knowledge of, and the ability to apply, appropriate methods within the main field of study as well as the skills required to work (and ultimately conduct research) in the field to which the education pertains. In relation to these targets, an assessment is made as to whether the students need to learn how to process personal data in order to meet the objectives concerning appropriate methods and skills in the subject.

The supervisor's assessment that the processing of personal data is necessary must be documented. At the HT Faculties, it is recommended that the student includes in their method section a statement indicating that the supervisor has deemed that the personal data processing in question is necessary to ensure that the student meets the programmes' learning outcomes.

The processing of personal data in student projects must comply with the general principles of the GDPR:

- **Lawfulness, fairness and transparency**

[2] For more information on lawful grounds, see https://www.staff.lu.se/support-and-tools/personal-data-and-data-protection/general-information/legal-basis

Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the individual whose data is being processed.
Based on this principle, data subject have the right to be informed about the processing of their personal data that and to request information on the type of personal data processed by the personal data controller, known as a register extract.

- **Purpose limitation**
  Personal data must be collected for specified, explicit, and legitimate purposes.
  This means that the purposes for the processing of personal data must be determined in advance and clearly communicated to study participants before any personal data is collected. Existing personal data may not be used for a new purpose without first establishing whether there is a lawful ground for the intended processing and whether any information requirements apply to the data subjects.

- **Data minimisation**
  Personal data must be adequate, relevant, and limited to what is necessary for the purposes of processing.
  This means that only the personal data needed for the task in question may be collected or used. For example, a video recording should not be made if a voice recording is sufficient.

- **Personal data must be kept up to date**
  Personal data must be accurate, which among other things may require the establishment of procedures to ensure that updates can be made when necessary.
  This means that the person who collecting and storing personal data must ensure that it is kept up to date, if necessary.

- **Storage limitation**
  Personal data must not to be stored in a form that allows identification of the data subject for longer than is necessary for the purposes for which it is processed.
  This means that personal data may not be processed beyond what is necessary. In the context of student projects, personal data must be deleted as soon as the course has ended, and the grade has been set.

- **Integrity and confidentiality**
  Personal data must be processed in a way that ensures that the data is appropriately secure, and this must be taken into account when choosing hardware and software.
  This means that the digital tools the students use throughout the process, from data collection to data deletion, must maintain an appropriate level of security.

- **Accountability**
  The personal data controller is responsible for, and must be able to demonstrate compliance with, the above-mentioned principles. This means that employees not only need to follow the GDPR but also need to demonstrate how they are doing so.

The data subject's rights

When Lund University processes personal data, the data subjects must be informed about the processing of their personal data, regardless of which lawful ground is applied. When a data subject gives their consent to participate in a study, they must also be provided with clear information about how the personal data will be processed. This information must be provided in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 12.1). Data subjects must be informed of the following: the purpose and lawful ground for the processing; that the University is the controller of the personal data; which categories of personal data will be processed; who will have access to the personal data; whether the data will be transferred to a third country (a country outside the EU); and the period for which the personal data will be processed. Additionally, the information must include contact details for the University's data protection officer. This in turn requires supervisors to give students clear instructions on how to inform data subjects about the processing of their personal data. Further information on the processing of personal data by students is available at education.lu.se.

When processing personal data that was not collected directly, but instead obtained via social media, blogs or other publicly accessible sources, the supervisor must plan how the data subjects will be informed. If the supervisor deems it unreasonably difficult to inform the data subjects, it is particularly important that this is documented, preferably alongside the assessment of why the processing of personal data is necessary to achieve the intended learning outcomes.

Criteria for secure processing

Caution must be exercised when processing personal data. For example, the higher education institution is responsible for ensuring that data storage is secure and that the data is handled in a secure and controlled manner and not improperly disseminated. Personal data processed for student projects may not be retained longer than necessary and must be deleted when it is no longer needed for the defined processing purpose.

Processing sensitive personal data in student projects

While processing sensitive personal data is generally prohibited under the GDPR, there are exceptions to this rule. If a supervisor deems it necessary for a student to process sensitive personal data, an explicit exception under the GDPR, most commonly consent, must be used as the lawful ground, and specific security measures must be taken. Before the processing begins, the supervisor and the student must assess whether processing is appropriate and necessary in order to achieve the learning outcomes, and whether it is possible to minimise the types and volume of personal data processed. In addition, specific protective measures must be taken. For example, caution must be exercised when selecting digital tools. Furthermore, sensitive personal data must be pseudonymised wherever possible, and the code key must be stored separately from the raw data. A basic measure is to ensure that only individuals who have a right to process the data have access to the it, namely the student and the supervisor. Personal data processed for student projects may not be stored for longer than necessary and must be deleted when it is no longer needed.

Can student projects be subject to ethical review?

This Guidance refers only to first and second-cycle student projects and placement assignments that do not fall under the Ethical Review Act (2003:460), and for which the collected data will not to be used for research purposes. It is important to emphasise that the publication of results from student projects in scholarly journals requires that the project has undergone ethical review and been approved *before* data collection begins. The Swedish Ethical Review Authority describes this situation as follows:

> According to the Ethical Review Act, research does not include such projects or studies carried out as part of first- or second-cycle higher education (Bachelor's or Master's level (60 credits)). For student projects to be exempt from the requirement for ethical review, the activity must constitute a learning exercise. The project is therefore not to "overlap" with a research project, nor must there be any intention for it to lead to a "regular" research project. If the intention to publish the results in a scholarly journal is evident at the planning stage, this is a clear indication that the project constitutes research that must undergo ethical review (EPN no date, translation by HT).

Ethical review is a time-consuming and resource-intensive process. As students cannot carry out a review themselves, it is up to the department and/or supervisor to determine whether there are occasions when student projects should undergo ethical review to enable the use of collected material for continued research purposes. Regardless of the department's decision, it is important that students are informed that according to the law, sensitive personal data cannot be used for further studies unless the study has undergone prior ethical review.

Ethical review is a protective measure that only applies to research. As this protective measure is not available for student projects, there is instead a requirement that the data subject give their informed consent both for participating in the study and for personal data processing. Consequently, the protective measures for processing sensitive personal data in student projects are organisational and technical in nature. Data subjects must receive a clear description of these measures. See the practical guidance for support[3].

[3] For further reading relating to ethical review, see *Guidance for Ethical Review of Research at the HT Faculties*, Görman, U.(2021):

See also the following extract from Bill 2007/08:44 regarding student projects and ethical review:
"The Government considers it unreasonable to expect students in the first and second cycle of education to have with certainty acquired the knowledge and insight to the extent necessary to ensure the protection of research participants. Students should therefore not be given the responsibility for activities involving people where there is a risk of physical, mental or privacy-related harm. […] However, the government assumes that work carried out by students within the framework of first and second-cycle higher education is conducted in an ethically sound and safe manner. This responsibility lies with the education provider." (translation by HT)
https://www.riksdagen.se/sv/dokument-and-lagar/dokument/proposition/vissa-etikprovningsfragor-m.m_gv0344/html/

Student projects or placement assignments written on the instructions of other public authorities

When degree projects or placement assignments are written on the instructions of another public authority, it is the responsibility of that authority to ensure that the level of security for the processing of personal data is appropriate, since Lund University is not the data controller in these cases. For example, the public authority in question can make data available from its own sources and ensure that data is not transferred to other organisations, such as Lund University. This can be achieved by providing the student with access to equipment and a workplace at the public authority. The same measures apply when students undertake placements outside the University and, where applicable, write academic papers as part of these placements.