

Administrative procedure

2026-01-20

Registration number: MIUN 2025/2759

# Administrative procedure for handling personal data in student projects

**Published:** 2026-01-20

**Decision-makers:** Vice-Chancellor

**Responsible function:** Department of Infrastructure

**Administrator:** Eva Rodin Svantesson

**Date of decision:** 2026-01-20

**Period of validity:** For the time being

**Last review:** Newly created

**Summary:** The document describes what must be taken into account in order for the personal data processing that takes place when a student processes personal data within the framework of their studies, for example within a student project, to be legal. The purpose of the document is to support the department responsible for the course and the student in how personal data should be processed in order to comply with GDPR.

**Previous versions:** Newly created.

The document is translated by E-translation.

# Table of contents

<b>1 Procedure for handling personal data in student projects</b> .....	<b>4</b>
<b>2 Background</b> .....	<b>4</b>
<b>3 Some important concepts</b> .....	<b>5</b>
3.1 Student work.....	5
3.2 Personal data.....	5
3.3 The data subject.....	5
3.4 Processing of personal data.....	6
3.5 Ordinary personal data.....	6
3.6 Sensitive personal data.....	6
3.7 Privacy-sensitive personal data.....	6
3.8 Quotes, references and citations.....	7
3.9 Controller.....	7
<b>4 Who is responsible for the student's processing of personal data?</b> .....	<b>7</b>
<b>5 Basic principles of the processing of personal data</b> .....	<b>7</b>
<b>6 Students' personal data processing in student projects requires consent and information</b> .....	<b>8</b>
<b>7 Processing of sensitive personal data in student projects that form part of research projects or in student projects</b> .....	<b>10</b>
7.1 Student projects that form part of research projects.....	10
7.1.1 Sensitive personal data in the context of a research project.....	11
7.2 Student projects not included in research projects.....	11
7.2.1 Sensitive personal data at work.....	12
<b>8 Procedure for personal data processing in student projects</b> .....	<b>12</b>
8.1 Does personal data need to be processed?.....	13
8.1.1 For the department responsible for the course.....	14
8.2 Ensure that personal data is processed in a specified manner based on the data's protection value.....	15
8.2.1 For the department responsible for the course.....	15
8.3 Determine how the information will be stored and handled.....	16
8.3.1 For the department responsible for the course.....	17
8.4 Determine which parts of the information containing personal data are to be deleted or stored.....	17
8.4.1 For the department responsible for the course.....	18
8.5 Designing the consent and information form.....	18
8.5.1 For the department responsible for the course.....	19

Administrative procedure

2026-01-20

Registration number: MIUN 2025/2759

8.6 Obtain informed consent, collect and process the personal data .....	19
8.6.1 For the department responsible for the course .....	19
8.7 Thinning or archiving the personal data upon completion of the examination .....	20
8.7.1 For the department responsible for the course .....	20
8.8 Example – sensitive personal data .....	20

# 1 Procedure for handling personal data in student projects

The purpose of this document is to explain what must be taken into account in order for the personal data processing that takes place when a student processes personal data within the framework of their studies, for example within a student project, to be legal. The purpose of the document is to support the department responsible for the course and the students in how personal data should be processed in order to comply with GDPR.

## 2 Background

Mid Sweden University is the personal data controller for the personal data processing that students do within the framework of their studies. For example, when a student writes an essay as part of their education, Mid Sweden University is legally responsible for any personal data that may be processed. The student's processing of personal data must then comply with both GDPR (General Data Protection Regulation, 2016/679) and the University's regulations.

Every human being has the right to a protected zone, a private life, which is guaranteed by human rights conventions and enshrined in the Constitution. The GDPR sets out the practical rules to guarantee individuals effective protection of their privacy and the right to their own identity in today's digitally connected society.

GDPR places high demands on all processing of individuals' personal data to be transparent, secure, and accurate. The GDPR's provisions are mandatory and the person who has their personal data processed cannot, for example, agree to lower security than the GDPR prescribes. Mid Sweden University, as data controller for the processing that takes place within the framework of the University's activities, may only collect and process an individual's personal data when there is support for the processing in the GDPR. Within the framework of the University's educational and research activities, the University supports its processing of personal data on the public interest legal basis (Art. 6(1)(e) GDPR). As regards personal data in student projects, Mid Sweden University considers that it is normally only the legal basis of consent

on which the university can support the processing of personal data (Art. 6(1)(a) GDPR).

## **3 Some important concepts**

### **3.1 Student work**

This processing order focuses on the personal data processing that takes place when a student processes personal data within the framework of his or her studies. The term 'student work' in this guideline and the order of processing refers to such situations, for example in the case of degree projects, memos, essays, and assignments, where personal data processing takes place.

### **3.2 Personal data**

Personal data is any type of information that can be linked to a living person. These may include names, e-mails, addresses and social security numbers, photos where the face is visible, audio recordings where no names are mentioned but the speaker can be identified.

Personal data processing takes place as soon as it is possible to identify a person based on the context using direct or indirect data. 'Indirect personal data' means data that can be indirectly attributed to a living natural person by reference to an identification number or to one or more factors specific to that person's physical, physiological, mental, economic, cultural, or social identity.

As a general rule, data on deceased persons are not personal data, but they may in some cases constitute personal data of living persons, such as relatives. These can be rare diagnoses or crimes committed by the deceased. In such cases, is there reason to believe that the data may be linked to living persons? In this case, the GDPR applies and must be complied with.

It can be mentioned that data on deceased persons in healthcare is covered by the provisions of the Patient Data Act, and thus by the provisions of the GDPR.

### **3.3 The data subject**

The data subject is a living person who has his or her personal data processed by Mid Sweden University. In connection with student projects, it is the individual who responds to a questionnaire, is

interviewed or otherwise participates in a study. The entire legislation is based on the fact that the data subject has rights that Mid Sweden University must satisfy.

### **3.4 Processing of personal data**

Basically, everything that is done digitally with personal data, from entering them into the computer, preserving, scanning, photographing, editing, processing, analyzing, printing, emailing, virus scanning, to making backup and deleting, counts as processing personal data. Sometimes manual (handwritten) notes are also considered processing if they are sufficiently structured, i.e., if they are included or intended to be included in a manually searchable record so that certain information about an individual can easily be retrieved for later use. Digital audio recordings are always included.

The concept of processing of personal data shall be a comprehensive definition of everything that anyone might do with personal data collected.

### **3.5 Ordinary personal data**

Since any data that can be directly or indirectly linked to a living person is considered to be personal data, the term ordinary personal data is often used to describe such data that is neither sensitive nor privacy-sensitive personal data.

### **3.6 Sensitive personal data**

Such personal data reveal ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as personal data relating to health or sex life, genetic or biometric data. Data on health can include, for example, sick leave, pregnancy, and doctor's visits.

### **3.7 Privacy-sensitive personal data**

Personal data that deserves special protection - even if data is not classified as sensitive, it can still be privacy-sensitive personal data. This may include, for example, salary data, data on violations of the law, valuing data such as data from performance appraisals, data on results from personality tests or personality profiles, information relating to someone's private sphere or data

on social conditions. Personal identity numbers are considered privacy-sensitive personal data.

### **3.8 Quotes, references, and citations**

Normally, no personal data other than quotes, references and source references should be reported in the completed student work. By virtue of Article 85 GDPR and Chapter 1, Section 7 of the Data Protection Act, the personal data rules do not apply when the processing of personal data takes the form of quotations, references and source references in the actual completion and dissemination of the final product that constitutes the student work. When the student is to process personal data in addition to quotations, references, and citations within the framework of their student work, the rules and the processing order contained in this document must be followed.

### **3.9 Controller**

The controller is the person who, according to the GDPR, determines the purposes and means of the processing of personal data.

## **4 Who is responsible for the student's processing of personal data?**

Mid Sweden University is the controller of personal data when the student processes personal data within the framework of their education. The university is formally responsible for ensuring that the student's personal data processing is lawful and that the individual's rights are respected. The student appears in his treatment as a representative of the university. The student is responsible for only processing personal data according to the University's instructions and cooperating with the University's staff.

If the student does an internship or an internship, so-called VFU, the principal of the internship or VFU location is the controller of the personal data processing performed by the student in the context of the internship.

## **5 Basic principles of the processing of personal data**

Any processing of personal data carried out must comply with the six fundamental principles set out in Article 5 GDPR. When students at Mid

Sweden University process personal data, the university must therefore ensure and be able to demonstrate that the processing meets the following requirements.

- The data shall be processed in a lawful, fair, and transparent manner in relation to the person whose personal data we process, i.e., the data subject (lawfulness, fairness, and transparency).
- The data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (purpose limitation). This means that personal data collected for student work may not be used in other contexts without ensuring that such new processing meets these requirements.
- The data must be adequate, relevant, and not excessive in relation to the purposes for which they are processed (data minimisation). An example of such data minimisation is that personal data is processed in pseudonymised form as far as possible.
- The data shall be accurate and, if necessary, up to date (accuracy).
- The data shall be processed in a manner that ensures appropriate security of the personal data (privacy, confidentiality, and storage minimisation).

These are the basic principles for all processing of personal data, and all activities should be seen in the light of the above sections. More information can be found on the Privacy Protection Authority's website.

## **6 Students' personal data processing in student projects requires consent and information**

All data processing must be based on what is known as a legal basis. There are six legal bases: consent, contract, balancing of interests, legal obligation, exercise of public authority and task in the public interest and protection of fundamental interests. It is sufficient to be able to rely on one of these legal bases to process personal data.

A task of general interest is, for example, the assignment given to the university by the Riksdag or the Government. The Higher Education Act

states that the university's mission is to conduct education, research and to 'interact with the surrounding society and inform about our activities and promote the usefulness of research results obtained at the university.' In the performance of this task, the University may process the personal data necessary for the performance of the task on the basis of the legal basis of public interest. No consent shall be obtained for the University's processing within the scope of this assignment.

As regards personal data in student projects, Mid Sweden University considers that it is normally only the legal basis of consent on which the university can support the processing of personal data. Individual consent is therefore required from each person participating in the study whose personal data are processed in the study. Please note that the processing of personal data in the form of quotations, references and citations is exempt from this consent requirement, see above section 3.9.

Where it is not possible to obtain consent, the starting point should be that the personal data is not suitable to be the subject of student work. If this is nevertheless considered, the DPO shall be contacted in good time for guidance. Contact via e-mail [dataskyddombud@miun.se](mailto:dataskyddombud@miun.se)

Before consent can be given, the person whose data is to be processed must receive information about the intended processing of personal data. The starting point of the GDPR can be said to be that each person owns their own personal data. Data subjects who are to participate in a study must therefore themselves be given the opportunity to decide whether personal data relating to him or her may be processed. For this to be possible, each potential participant must first be informed of what the personal data processing entails, and then be given the opportunity to decide whether he or she consents to the processing. It is therefore a condition that the participant has been able to make an informed choice about whether to participate or not, for a consent to be considered valid. Furthermore, participants have the right to withdraw their consent at any time. It is also important that it is clear from the information that a withdrawn consent does not affect the legality of the processing that took place before the withdrawal, but the student may not continue to process the personal data covered by a withdrawn consent. Please note that storage also means that personal data is processed.

Students may use information from databases and sources that are publicly available, provided that the data is anonymized or cannot be linked to an identifiable person. When the material is already anonymized, it is not considered sensitive personal data, and therefore the use does not involve any handling of personal data according to the General Data Protection Regulation (GDPR).

However, it is important that the student and the supervisor always ensure that the information is genuinely anonymised, i.e., that no individual can be identified directly or indirectly through the data.

More information about consent can be found on the Privacy Protection Authority's website. Mid Sweden University has developed a template for obtaining consent and the information to be provided before consent is to be collected. The template for consent and information is available on the employee and student pages. Collected consents shall be archived.

## **7 Processing of sensitive personal data in student projects that form part of research projects or in student projects**

### **7.1 Student projects that form part of research projects**

When the student work is carried out within the framework of a research project conducted by Mid Sweden University and led by a responsible researcher, the student's processing of personal data takes place under the conditions given in the project in question and under the responsibility of the principal researcher. The legal basis for the student's processing of personal data is the same as for the research project, i.e., public interest.

The student's personal data processing must then follow the rules that apply to that research project, and all the student's data management must take place within the framework of the research project's secure storage areas and authorization structure.

### **7.1.1 Sensitive personal data in the context of a research project**

The main rule of the GDPR states that it is forbidden to process sensitive personal data, but this may be allowed in certain situations. If the processing of such personal data may take place, the processing is subject to restrictions and requirements for higher security.

An exception to the prohibition on processing sensitive personal data follows from the Act (2003:460) on ethical review of research concerning human beings, the Ethical Review Act, which contains, among other things, provisions on ethical review of research processing sensitive personal data and personal data on breaches of law.

In a research project that has received an ethical permit, this type of personal data may be processed. However, the Act does not cover work carried out within the framework of university education at undergraduate or graduate level, which is why students cannot obtain such an ethical permit.

However, student work can be part of an ethically approved research project led by a responsible researcher. In this case, the student's processing of personal data takes place under the conditions given in the project in question and under the responsibility of the principal investigator. In these cases, the student's processing of sensitive and privacy-sensitive personal data is based on the ethical approval given to the project in question. The student's personal data processing must then follow the rules that apply to the ethical permit obtained and all the student's data handling must take place within the framework of the research project's secure storage areas and authorization structure.

## **7.2 Student projects not included in research projects**

In cases where the student work is not part of a research project conducted by the university, the student's processing of personal data must be based on the legal basis consent. In that case, the procedure set out in Section 8 must be followed. Procedure for personal data processing in student projects are followed.

### **7.2.1 Sensitive personal data at work**

Although the processing of sensitive personal data is, as a general rule, prohibited under the GDPR and student work cannot be ethically reviewed in accordance with the Ethics Review Act, Mid Sweden University considers that there may be value in students at undergraduate and graduate levels being allowed to process sensitive or privacy-sensitive personal data in certain cases. The legal scope for processing sensitive personal data in student projects is very limited. The data subject must also have expressly consented to the processing and the purpose of the processing.

In order for it to be permitted to process sensitive or privacy-sensitive personal data, such as data on violations of the law, outside of an ethically approved research project, it is necessary for the examination of the student's work. If the student can be examined by carrying out a student work that does not involve the processing of sensitive personal data, the necessity requirement is usually not met. It is also required that the student work is carried out in ethically acceptable forms. The department responsible for the course is responsible for ensuring that such an assessment of suitability is carried out before the start of the study.

## **8 Procedure for personal data processing in student projects**

Mid Sweden University is the personal data controller for the personal data processing that students do within the framework of their studies. If the student processes personal data in a student's work, which is not part of a research project conducted at the university with the researcher responsible, this procedure must be followed.

If the personal data that the student will process within the framework of their student work consists only of the names included in quotations, references and source references, the provisions of the GDPR do not apply to this personal data processing and the rules in this processing order do not need to be followed.

The following seven steps, described in more detail in sections 8.1 to 8.7, must be fulfilled in order for the processing of personal data to be permitted.

Where sensitive personal data or privacy-sensitive personal data are to be processed, the specific rules applicable to those types of personal data shall be carefully taken into account.

In short, the requirements imposed mean that:

1. Assess whether it is necessary to process personal data.
2. Ensure that personal data is processed in an assigned manner based on the protection value of the data in question (as support, an information classification can be carried out).
3. Determine how the information is to be stored and ensure that it is handled securely during the work.
4. Determine which parts of the information are to be deleted or retained when the work is done.
5. Design the consent and information form.
6. Inform and obtain the consent of each individual who will participate in the study, collect the necessary personal data, and process the personal data in accordance with what has been decided in steps 1-5 above.
7. After grading the student work, delete or archive the personal data in accordance with what has been decided in step 4 above.

In order to comply with the requirements of the GDPR, all the different steps must be assessed and carried out correctly. It is the department responsible for the course that finally decides how these requirements should be met and will ensure that the student is well informed about the conditions that apply to the students' work. Both the students and the department responsible for the course must be involved and know each step of the process.

## 8.1 Does personal data need to be processed?

Given that Mid Sweden University's possibilities to create the necessary security and fulfil its personal data responsibility are subject to restrictions when it comes to students' personal data processing, the primary aim should be to ensure that no personal data is processed in student work. Secondly, as few personal data should be processed with as much security as possible.

If no personal data is processed, the GDPR does not apply, which simplifies the work. If the student work can be carried out with anonymous data, personal data will not be processed in the student work. Anonymized data is

data that cannot be linked to an individual, either with the data the university has access to or such data that can be obtained from other sources.

However, in cases where the student conducts an "anonymous" survey, personal data is usually processed on the basis of the GDPR's definition of what personal data is. Data is only anonymous to the extent that it is completely impossible for anyone to link the information with an individual. For example, it is enough that the survey tool somewhere logs the IP address or saves any indirect information about the person who answered the survey for the personal data rules to apply in the situation. Furthermore, the use of free text answers always means that there is a risk that the person who answers the survey enters direct or indirect personal data about themselves or others.

It should be assumed that most surveys involve the collection of personal data in some form, at least during the collection phase.

There is a difference between anonymised data and pseudonymised data. Pseudonymised data means that a code key or similar linking the task to an individual remains somewhere, regardless of whether the university has access to the code key or not. Pseudonymised data is considered personal data under the GDPR. However, Pseudonymisation means that both the processing of personal data is minimized and the degree of security of the processing is increased. Personal data that must be processed should therefore normally be processed in pseudonymised form.

As mentioned above, the processing of personal data in the form of quotations, references and citations is exempt from the rules on personal data processing.

### **8.1.1 For the department responsible for the course**

Emphasize before the implementation of the student work that only such personal data as are relevant and necessary may be collected in the documentation for the student work and processed during the preparation of the student work. Personal data other than quotations, references and citations should not be included in the finished work.

For statistical reporting, it is important to display aggregated statistics de-identified. It is not permitted or ethically justifiable to report so-called disclosing statistics, where it is possible in a statistical compilation to identify individuals, directly or indirectly.

## **8.2 Ensure that personal data is processed in a specified manner based on the data's protection value**

When personal data is processed at Mid Sweden University, it is important to assess the protection value of the data before each processing. It is particularly important to consider at an early stage what type of personal data will be processed in student work (sensitive, privacy-sensitive, or ordinary personal data). The type of personal data determines what protection value the data has and how they should be handled, which storage areas to choose, etc.

If sensitive personal data is to be processed within the framework of a student project, an aptitude test is also required, so that it can be ensured that the project is carried out in an ethically acceptable manner. A clear purpose and good reason are required to allow the processing of sensitive personal data, see section 7.2 above.

If there is consent and a necessity and suitability test has been carried out in a way that the faculty states, Mid Sweden University allows students to also process sensitive personal data.

### **8.2.1 For the department responsible for the course**

If the student is to process sensitive or privacy-sensitive personal data outside an ethically approved research project, it must be ensured that the project is carried out in ethically acceptable forms. The department responsible for the course is responsible for ensuring that an assessment of necessity and suitability is carried out before the study begins.

Questions about publishing can have ethical dimensions. A piece of information may be unsuitable for reproduction even if it is not by definition sensitive, such as an indication of poor finances or data worthy of protection of a more private or reprehensible nature. In case of doubt about a task being considered sensitive, the Data Protection Officer ([dataprotectionombud@miun.se](mailto:dataprotectionombud@miun.se)) can be contacted.

Data on breaches of the law, such as criminal convictions or suspicions, constitute privacy-sensitive personal data and, under this rule, must be protected in the same way as sensitive personal data. They can be treated if the student work moderately reproduces published convictions or suspicions of crime raised in the mass media or in legal databases.

If personal data relate to criminal offences (including criminal sanctions), they should be reported, at most, in a slightly pseudonymised form, in the same way as when publishing guidance judgments, i.e. only the initials of those concerned as designated, suspected or convicted. In addition, where possible, other identifying information should be avoided. The same applies in cases where the names of witnesses and victims appear in the published judgment.

It should also be noted that research involving the treatment of violations of the law, offences, criminal convictions, and coercive measures of criminal procedure or administrative detention is subject to obtaining an ethical licence. See above sections 7.1 and 7.2.

### **8.3 Determine how the information will be stored and handled**

The GDPR's provisions on security are mandatory and those who have their personal data processed cannot agree to lower security than the GDPR prescribes to be achieved. Thus, it is the responsibility of the department responsible for the course to ensure that the student handles collected personal data in a secure manner. The level of security is determined on the basis of how worthy of protection the personal data is, see 8.2.

The employee pages contain information about how and where information can be stored and managed. Only areas provided by the University for collection, treatment and storage shall be used. For sensitive or privacy-sensitive personal data, only those surfaces that are explicitly approved for the processing of such personal data shall be used.

External cloud services that are not provided by the University may not be used for the processing of personal data. Furthermore, it is inappropriate to store personal data on unencrypted hardware such as USB sticks, smartphones, or tablets.

Wherever possible, the University's tools should be used. This applies regardless of the type of material; written material, survey responses, recorded interviews or photographs and films, etc.

### **8.3.1 For the department responsible for the course**

The material, documentation, or data, etc., from which the student work is then designed, must be put on surfaces provided by the university and intended for storage and processing. Access shall, as far as possible, be limited to those who need the information in their role, such as the author, co-writer, or the department responsible for the course.

If the student work contains sensitive personal data, the department responsible for the course must ensure that the data is processed in a service approved by the university with sufficient security and that is explicitly approved for the processing of such personal data.

## **8.4 Determine which parts of the information containing personal data are to be deleted or stored**

Personal data shall not be retained longer than necessary and shall be deleted when they are no longer needed. Before the process of collecting the personal data begins, it is important to determine what will happen to the personal data. The student should be asked not to submit documents with personal data to the university. However, there may be certain situations where personal data may need to be submitted to the university and saved for a certain period of time. For example, if the data are needed to support the conclusions of the student work or if they are necessary for future data processing (for example, for the result to be published in a scientific article). In such cases, the material shall be archived.

The department responsible for the course must ensure that any personal data received is erased as soon as the student work has been graded, unless the prerequisites for archiving are met. At the same time, the student shall be asked to delete all personal data processed within the framework of the student work.

### **8.4.1 For the department responsible for the course**

The normal thing is that the university does not need to take documents with personal data. If this happens, the data should be screened after grading. The exception is if they are at the same time part of a research project or otherwise constitute such public documents that are to be archived by the department responsible for the course on the intended surface.

The archiving rules are set out in the steering document 'Mittuniversitetet's information management plan.'

For an ethics-tested research study, or if student work in exceptional cases would be considered research, the archiving must follow the ethical decision and the steering document 'Mid Sweden Information Management Plan.'

## **8.5 Designing the consent and information form**

GDPR requires that those who have their personal data processed by the university must have received sufficient information. Furthermore, personal data may only be processed if there is a so-called legal basis. In the case of student work, in principle, only the individual consent of each individual is the legal basis that can be considered.

In order for consent to be valid under the GDPR, the person who is to participate in the study must have received sufficient information before agreeing to participate. The requirement for consent to be freely given also presupposes that there are no negative consequences if a person declines to participate in the study. If the person is not able to make an informed choice to participate in the study, the consent becomes invalid.

It is therefore important that the consent form contains the information required by the GDPR and accurately reflects what the student should do with the personal data. Once collected, the personal data may not be used for anything other than what the participant has consented to without obtaining a new updated consent. It should be as easy for the participants in the study to withdraw their consent as to give it. The contact details of the students and the department responsible for the course must always be included in the information.

Mid Sweden University has developed a template for obtaining consent and the information to be provided before consent is to be collected. The template for consent and information can be found on the employee pages.

Children under the age of 16 may, as a rule of thumb, be considered to lack sufficient maturity to give valid consent. For children between the ages of 13 and 16, a case-by-case assessment must be made as to whether the child may be able to understand the consequences of consent. If it is found that the child cannot give valid consent or in cases where it is uncertain, the consent must instead be obtained from the person who is the guardian. When children are to consent themselves, the language of the consent and information form needs to be adapted. The text must be clear and simple and there is high demand for the information in order for correct consent to exist.

### **8.5.1 For the department responsible for the course**

When someone participates in a study within a student project, the developed template for the consent and information form must be used.

In some exceptional cases, written consent may be problematic. If oral consent is considered, the Data Protection Officer ([dataprotectionombud@miun.se](mailto:dataprotectionombud@miun.se)) should be contacted.

## **8.6 Obtain informed consent, collect, and process the personal data**

If everything has been done correctly in the previous steps, this step, which is formally important, is not very burdensome.

It is the person who collects the personal data who has the burden of proving that there is a documented and valid consent. Collected consents shall be stored on the surface where other collected material is stored throughout the process.

### **8.6.1 For the department responsible for the course**

The student shall store collected material and associated consents on the surface created for the student work. The department responsible for the course is responsible for ensuring that this happens.

## 8.7 Thinning or archiving the personal data upon completion of the examination

When the student's work is completed and the student has graduated on the course component, the last component remains. The personal data material shall be erased, erased, or stored and archived as determined in step 4.

### 8.7.1 For the department responsible for the course

The material is deleted, culled, preserved, or archived after examination as determined in step 4. The student shall at the same time be asked to delete all personal data (including digital and physical material) processed within the framework of the student work. The department responsible for the course is responsible for ensuring that this happens.

## 8.8 Example – sensitive personal data

When students carry out work where personal data may occur, it is important to always make an assessment of whether the data can be counted as sensitive. Even if the interviews are based on professional roles and do not directly concern individuals' private relationships, sensitive personal data may still arise if the conversation slips into, for example, health, political opinion, or religious beliefs.

Both students and supervisors therefore need to have basic knowledge of data protection and be aware of the risks. The supervisor has a special responsibility to guide the student in the assessment and ensure that the work is planned and carried out in a way that protects the persons involved. In this way, student projects can be carried out with respect for integrity and in accordance with applicable rules.

### Political science

A student interviews a politician who himself has openly explained his political views. Data about the political outlook is still considered sensitive personal data but can be processed because the politician himself made them publicly known. If a student interviews a private individual about their political sympathies, consent must be obtained.

---

## Nursing

A student writes about nurses' experiences of working night shifts. Questions about workplace organization usually do not contain sensitive personal data. However, if the interviews cover the nurse's own health or patient cases with medical information, it becomes sensitive personal data.

---

## Occupational health sciences

A student interviews rehabilitation coordinators about how they organize rehabilitation in the municipality. Issues related to work routines, resources and professional experience usually do not contain sensitive personal data. However, if specific patients or employees' health conditions are mentioned, it becomes sensitive personal data.

---

## Socionomist

A student interviews social workers about how they experience workload and legislative challenges. As long as the interview is about the role and general reflections, it usually does not contain sensitive personal data. However, if the interview includes details about individual clients or the social worker's own health, it becomes sensitive personal data.

Another example: A student on the social work programme interviews a young person who has contact with the social services about how they experience the support from the social workers and how they understand their own participation in the decision-making process. As long as the interview is about general reflections on the meetings – such as “I think it is good when the social worker explains the rules clearly” or “I wish I had more information in advance” – it usually does not contain sensitive personal data.

However, if the interview includes data on the health of the young person (e.g., mental illness, medical diagnoses), family situation (e.g., domestic violence, abuse by relatives, financial problems) or other details relating to identifiable persons, it becomes sensitive personal data.

---

## Preschool teacher

A student interviews preschool teachers about how they plan educational activities. Information regarding the professional role does not count as

sensitive personal data. However, if the interview contains information about the health, level of development or family circumstances of individual children, it may constitute sensitive personal data.

---

### **Teachers**

A student examines how upper secondary school teachers work with digital teaching materials in teaching. Questions about methods, resources and working conditions usually do not contain sensitive personal data. But if the interview goes into individual students' ethnicity or special needs, it becomes sensitive personal data.