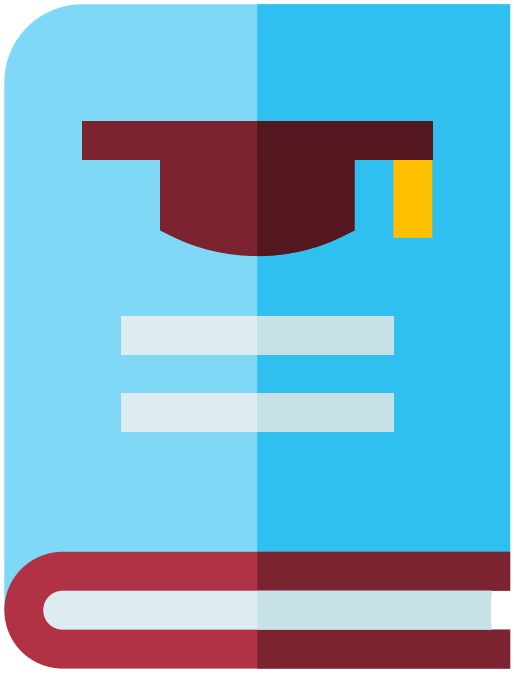

Essay writing and GDPR

Contents

1. Personal data processing in student projects, guidance in nine steps

The European General Data Protection Regulation (GDPR) and the supplementary Swedish legislation place many comprehensive requirements on all work involving personal data being performed in an open, correct and secure manner. If, in your role as a student, intend to process personal data in your independent project/degree project/essay project (below "essay project"), there is a great deal to consider before you can start.

Part 1 provides an overview of the nine steps that must be completed for the processing of personal data to be permitted. Part 2 provides a background to and explanation of the

legislation. Part 3 covers techniques for de-identification, such as anonymisation and pseudonymisation. Part 4 includes a checklist of information that must be given to someone whose personal data is processed by the university. Templates for an information letter and a consent form are appended to this document.

In brief, the requirements mean that you must:

1. Evaluate whether it is necessary to process personal data.
2. Define the purpose of processing the personal data and evaluate what data must be collected.
3. Ensure that sensitive personal data will not be processed.
4. Decide how the information will be stored and ensure that it is processed securely during your work.
5. Decide which parts of the information will be erased or retained when work is completed.
6. Write the information letter and consent form.
7. Complete the form for registering personal data in the essay project, so that the essay can be registered in the university records by the supervisor.
8. Inform and collect consent from every single person who will participate in the study, collect the necessary personal data, and process the personal data in accordance with what was decided in steps 1-7 above.
9. After the essay project has received a pass grade, erase or archive the personal data material in accordance with that decided in step 5 above.

Check with your supervisor regarding what is suitable for your essay project and remember that your supervisor must be involved and know about every step of the process. To fulfil the requirements of the GDPR, all the steps must be assessed and conducted in the correct manner.

Step 1: Must personal data be processed?

The first question you need to think about is whether it is really necessary to process personal data to complete your essay. If you do not process personal data, GDPR does not apply, which makes your work easier.

Personal data is all information that, based on the context, can be directly or indirectly linked to a living person. This not only includes information such as name, personal ID number and recorded interviews (even if no names are mentioned), but also information that indirectly identifies a person, such as physical, physiological, personality, financial, cultural or social traits. For example, if there is only one person with the postcode 123 45 who was born on 1 January 2000, these pieces of information together are indirect personal data about that individual. The description “the first man to set foot on the moon” would also be indirect personal data about Neil Armstrong if he was alive today.

Even when you conduct an “anonymous” survey, you often process personal data based on the GDPR’s definition of what constitutes personal data. Data is only anonymous to the extent that it is impossible for you or an external party to link a piece of information to an individual. If your survey tool logs the IP address or saves enough indirect information about the person who answered the survey (regardless of whether the person who created the survey can see that information), this is enough for regulations about personal data in apply. Additionally, the use of free text responses always entails a risk that the person answering the survey writes direct or indirect personal data about themself or others. You should assume that most surveys entail collecting some form of personal data, at least during the collection phase.

Tips! Södertörn University has a subscription to Survey & Report, which is a digital tool for creating surveys. You can use it to create an open survey with a public link, which you can share publicly or with the target groups for your survey. When you use that function, fewer personal data are collected.

Step 2: Define the purpose of the study (the purpose of processing the data)

If you have decided that you need to collect personal data to be able to complete your study, you must start to formulate the purpose of the personal data processing. This is a requirement of the GDPR.

The purpose of processing the data is that you will collect the information necessary for conducting your investigation. However, the description of your purpose should be adapted to what you are going to investigate and why.

It is important that you consider and formulate the purpose well, and that you are definite about what information is necessary to conduct your investigation.

Collecting more personal data than is necessary to fulfil the purpose you defined is not permitted. Once you have collected the personal data, they may not be used for any other purpose than the one for which you collected them.

Step 3: Ensure that no sensitive personal data will be processed

The foundation of the GDPR is that processing sensitive personal data is prohibited. There is limited potential for processing sensitive personal data in an essay project.

Södertörn University’s ambition is to allow students to use this limited legal space as a basis for processing sensitive personal data, when this is motivated. This requires a clear purpose and good reasons for allowing the processing of sensitive personal data. **Students are not currently permitted to process**

sensitive personal data because important legal and technical issues related to this are under investigation.

Step 4: Decide how the information will be stored and processed

The GDPR's provisions on security are obligatory and the person who has their personal data processed cannot agree to a lower level of security. It is therefore the responsibility of the student and the university to ensure that collected personal data is processed in a secure manner. The level of security is decided based on how worthy of protection the personal data is.

Södertörn University offers some tools that can used. Students can access Office 365, which includes e-mail and storage space on OneDrive. In addition, if the academic school applies for it, students can access the Sunet Survey survey tool. Please note that students may not process sensitive personal data in Office 365 or Sunet Survey.

Legally, the university must enter an agreement with every cloud service that will be used for the university's processing of personal data, and the agreement must include specific guarantees. The use of external cloud services (e.g. iCloud, Google docs, Dropbox, etc.) is therefore not permitted if they are not provided by Södertörn University. Nor may personal accounts for services the university subscribes to, such as OneDrive, be used; you must always use them via the university's agreement.

In addition, you must remember that is not appropriate to store personal data on unencrypted USB sticks or tablets and smartphones, because these may not be fully secure and are often synchronised with prohibited cloud services.

Step 5: Decide what information will be erased or saved

Personal data may not be saved longer than necessary and must be removed when no longer needed. However, there may be situations in which personal data needs to be saved for a certain length of time. For example, the data may be necessary to justify the conclusions in an essay or for future data processing (if the results are to be published in a scholarly article).

Before beginning work on gathering personal data, it is important to decide what will happen to the personal data. Must some data be submitted to the university to be saved for a particular period? Other personal data must be erased by the student as soon as the essay receives a grade. Before the grade is registered in Ladok, the student must submit a guarantee to the examiner stating that personal data has been erased.

Step 6: Write an information letter and a consent form

The GDPR states that anyone who has their personal data processed by the university must have received adequate information. Personal data may only be processed if there is a legal basis for it. In principle, for student projects, the only relevant legal basis is the individual consent of each person.

For consent to be valid I accordance with GDPR, the person participating in the study must have agreed to it after receiving adequate information. If the person is unable to make an informed choice on participation in the study, their consent is invalid. The requirement for voluntary consent is also met because there are no negative consequences if a person declines to participate in the study.

It is therefore important that your information letter and consent form contain enough information and accurately describe what you are going to do with the personal data. Once you have collected the personal data, you may not use it for any other purpose without obtaining new and updated consent. It must be as easy for a participant in the study to withdraw their consent as it is to provide it. Contact details for the student and the supervisor must always be included in the information letter.

A person participating in a study is entitled to information about the purpose of the study, the personal data you wish to collect, what the personal data will be used for and how long the personal data will be saved before they are erased, as well as other considerations. Södertörn University has produced a template for the information letter and consent form.

Step 7: Complete the form for reporting personal data processing to the university’s central records

Before any processing of personal data can start, you must complete a form and send it to the data protection officer. All data processing performed at Södertörn University must be included in central records. As a student, you must provide the information.

When you have completed the form and had it approved by your supervisor, it is the supervisor’s responsibility to ensure that the form is sent to the data protection officer. The supervisor is also responsible for reviewing the form for personal data processing, and that the information latter and consent form fulfil the requirements of the GDPR.

The records of personal data processing in essays is simply a central register that Södertörn University must have to check on what data processing is being performed. It must therefore describe what type of personal data is being processed and why. Do not send any actual personal data apart from the names of the people working on the essay and the supervisor.

Step 8: Collect informed consent, gather and process the personal data

If everything has been done correctly in the previous steps, then this step is formally important but not particularly demanding.

It is important that you keep all the collected consent forms organised throughout the entire process. The person collecting the personal data carries the burden of proving that there is documented and valid consent.

Step 9: Erase or archive personal data after you have received your grade

When the essay is complete, and you have received a grade for the course/module, there is one thing left to do. Personal data must be erased or preserved/archived according to what was decided in step 5.

Once you have erased the personal data material you must submit a guarantee that you have done this to the examiner, so the examiner can inform the data protection officer that the personal data processing has stopped. The grade is registered in Ladok after this.

2. Introduction to the General Data Protection Regulation

Everyone has the right to a private life, which is guaranteed through conventions on human rights and is enshrined in Swedish constitutional law. The EU General Data Protection Regulation, GDPR[1] is an EU law that includes the practical rules that guarantee individuals effective protection for their privacy and the right to their own identity in our modern, digitally connected society.

The GDPR places high demands on the transparent, secure and correct processing of individuals' personal data. Södertörn University may only collect and process someone's personal data when there is a legitimate reason or when a person decides to participate in a study of their own free will.

When, as a student, you write an essay as part of a course or programme, Södertörn University is legally liable for any personal data you process. The GDPR equates students writing an essay with the university's employees. Students and staff may, as representatives of Södertörn University, only process personal data in accordance with the law and instructions from the university.

The purpose of this document is to provide a succinct review of what you must do if your processing of personal data is to be legal. It is important that you communicate how you process personal data with your supervisor. If you have any questions, you are welcome to contact the university's data protection officer.

Preparing everything thoroughly is worthwhile. One rule of thumb is that collected personal data may only be used for the purpose for which it was collected. Also, a person whose personal data is processed by the university is often entitled to be informed about the processing and may require that the university takes particular measures. All collection of personal data must also be registered in central records that are managed by the university's data protection officer. The law also requires that the collected personal data are securely processed and stored.

2.1. Some important terminology

Personal data – personal data are all kinds of information that can be linked to a living person. This includes name, email, address and personal ID number, photos where the face is visible, audio recordings where no names are mentioned but the speaker is identifiable. The context determines whether it is possible to identify a person using direct or indirect data.

The data subject – a living person who has their personal data processed by Södertörn University. In this context, this is an individual who responds to a survey, is interviewed or

[1] GDPR is an abbreviation for the General Data Protection Regulation.

participates in your study in another way. The entire legislation is built upon the data subject having rights that Södertörn University must satisfy.

Personal data processing – in principle, everything that is done digitally with personal data, from typing them into a computer, scanning, photographing, editing, processing, analysing, printing, emailing, virus scanning, making a backup, to erasing, etc., counts as personal data processing. The purpose is that it should be a comprehensive definition of everything that someone could do with collected personal data. Personal data regulations must provide effective protection. Manual (handwritten) notes may also be included if they are adequately structured. Digital audio recordings are always included, but not if this one is made on an analogue tape recorder without being transferred to a digital medium.

Data controller – the person/organisation that, according to the GDPR, decides the purposes and means for the processing of personal data, e.g. Södertörn University.

2.2. Who is responsible for a student's processing of personal data?

Södertörn University is the data controller when a student processes personal as part of their course or programme. The university is formally responsible for the legality of the student's processing of personal data and that the individual's rights are respected. The student is a representative of the university. The student is responsible for only processing personal data in accordance with the university's instructions, cooperating with university staff and must submit collected material to university staff when this is requested.

If the student is on a placement, then the placement provider is normally the data controller for the data processing performed by the student on the placement.

2.3. Basic principles for processing personal data

All processing of personal data must fulfil the six basic principles stated in article five of the GDPR. When students at Södertörn University process personal data, the university must guarantee and be able to prove that this processing fulfils the below requirements.

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
- Personal data shall be accurate and, where necessary, kept up to date (accuracy).

- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation).
- Personal data shall be processed in a manner that ensures appropriate security of the personal data (integrity and confidentiality).

These are the basic principles for all processing of personal data and all activities must be considered based on the above items. More information is available on the website of the Swedish Data Protection Authority (https://www.datainspektionen.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/)

2.4. Personal data processing by students requires consent

All processing of personal data must have a legal basis; there are six of these bases. Södertörn University believes that normally only one of these can be used by students writing essays: individual consent from each person participating in the study. In special cases where it is not possible to collect consent, such as if a student wishes to analyse what a large number of people have written on Twitter, the supervisor must in good time contact the data protection officer for guidance.

The foundation of the GDPR can be said to be that every person owns their own personal data. The data subject who is to participate in a study must therefore have the opportunity to decide whether their personal data will be processed. For this to be possible, each potential participant must first get information about what personal data processing entails, and then be given the opportunity to decide whether they agree to the processing. It is therefore necessary for the participant to be able to make an informed choice to participate or not for consent to be considered valid. A participant also has the right to withdraw their consent at any time.

More information about consent is available on website of the Swedish Data Protection Authority. (https://www.datainspektionen.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/lawful-grounds-for-personal-data-processing/) There is also a checklist further down, with information that must be provided when personal data is collected.

2.5. Sensitive personal data

Some types of personal data are, by their nature, particularly sensitive. Processing such data is covered by restrictions and requirements for higher security. Sensitive personal data includes information about race or ethnic origin, political opinions, religious or philosophical conviction, membership of trades' unions, genetic information, biometric information to unambiguously identify a physical person, information about health or information about a physical person's sexual life or sexual orientation. Personal information such as mother tongue or home language may be sensitive personal data as, in some cases, they may indirectly indicate ethnic origin.

The main principle is that the processing of sensitive personal data is prohibited, but it may be permitted in some situation and is complicated. There are examples of higher education institutions that do not allow students to process sensitive personal data unless it takes place within a research project. However, Södertörn University believes that there may value in students at Bachelor's and Master's levels being permitted, in some cases, to conduct surveys or interviews with people who are disabled, LGBT+, have a particular political opinion or religious belief, etc. **Unfortunately, technical and legal issues that are currently being investigated must be solved before students can be permitted to process sensitive personal data. Therefore, students are currently not permitted to process such data.**

3. De-identification of personal data

3.1. Pseudonymisation

A typical example of pseudonymisation is when you remove all information that can be linked to an individual from collected data and give it a pseudonym that you store separately. For example, you can convert the person's name or email address to a unique code, such as respondent 11. The list of codes and individual identities must be stored separately to the collected data. When you do this, you must also store the list using adequate security, whether this is digital protection or a physical list that is stored in a safe.

Pseudonymisation still means, from a legal perspective, that you are processing personal data. This must be regarded as a protective measure that reduces the risk of linking a particular answer to the person who gave it. In a legal sense, pseudonymisation still means that you are processing personal data and that this processing must follow the GDPR.

3.2. On the anonymisation of personal data

Initially, it must be stated that anonymisation is a very complex and difficult to assess measure that is rarely suitable for a student project. As a student writing an essay, you are asked to collect the personal data necessary to do your work, process them in accordance with the university's rules and instructions and then destroy the personal data. In cases where personal data is not regarded as anonymised they are instead pseudonymised[2], which is a more realistic alternative in some cases. Pseudonymisation was described in the previous section. To provide an overall picture, a description is provided below of what anonymisation entails from the perspective of the GDPR.

[2] Frydlinger, David, *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, Edition 1, Stockholm, 2018 pages 281-282

Anonymisation is a process that irrevocably anonymises the collected personal data. Once the process is complete, it should not be possible for you, as the person who conducted the survey, or for any external party to reidentify individuals by merging your dataset with other data[3]. The assessment must be made based on all available aids that someone possibly and plausibly would use to reidentify individuals. This assessment must be made with consideration of what is technically possible[4]. This requires knowledge of data protection legislation and that being updated on the latest research into the strengths and weaknesses of various techniques for de-identification. If full anonymisation can be achieved, GDPR is no longer applicable to that information, which provides greater freedom for doing what you want with the information.

In practice, it is very difficult to ensure that the data are anonymises and that it cannot be merged with other data to obtain personal data. This can be illustrated using Netflix as an example. In 2006 they publicised ten million film ratings from 500,000 customers and anonymised their identities by replacing the customers' names with randomly generated numbers. Two researchers analysed some of this data and compared the customer ratings and time stamps with public information from a service called Internet Movie Database, IMDb. Through their analysis, the researchers succeeded in reidentifying individuals who had voted and could also establish their sexual orientation and political views.[5]

If you wish to look at the subject in more details, you can read an article form the EU on de-identification techniques. It can be downloaded from this address: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf . It was published by the Article 29 group in the EU. This was an advisory working group at EU level that comprised the data inspectorates of every EU member state. Since 25 May 2018, this group has received significantly increased powers and changed name to the European Data Protection Board. Their statement discusses the legal circumstances surrounding de-identification and anonymisation and the pros and cons of various techniques.

4. Checklist for information that must be provided

According to article 13 of the GDPR, the following information must be included when personal data is collected straight from an individual, for example when they answer a survey or are interviewed. Södertörn University has produced a template for the information letter and consent form (appended). This information must always be included in the

---

[3] Frydlinger, David, *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, Edition 1, Stockholm, 2018 page 282

[4] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_sv.pdf pages 6-7

[5] Frydlinger, David, *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, Edition 1, Stockholm, 2018 pages 281-282

information letter when personal data are processed as part of an independent project/essay that is conducted at Södertörn University.

The purpose of the information letter is to fulfil the university's obligation to provide information. A separate consent form must always be appended; the form is used to obtain the participants' consent to having their personal processed. Remember that you must store the consent forms so that they are not lost, because you must be able to prove that valid consent has been obtained.

The below checklist is so that you can ensure that the necessary information is included if you are not using the university's template. If the information is provided as part of an interview, print out the information and give the person this information both orally and in writing. You also need to document individual consent to participate. Consent may either be in writing or orally, as long as it is recorded.

Participants must receive the following information:

- ✓ That the university is the data controller, along with the necessary contact information:

  There is a legislative requirement for it to be stated that Södertörn University is the data controller and that the university's official contact information is provided: registrator@sh.se and the switchboard number +46 (0)8 608 4000, and the postal address

  Södertörns högskola

  Alfred Nobels Allé 7

  141 89 Huddinge

- ✓ Contact details for the student and supervisor: This information is not a legislative requirement, but Södertörn University's guidelines demand it. Participants in the study are primarily encouraged to contact the student and supervisor.

- ✓ Contact details for the university's data protection officer: Everyone who has their personal data processed by the university is entitled to know that they may always contact the data protection officer if they have questions or complaints. The data protection officer can be contacted by emailing dataskydd@sh.se

- ✓ Legal basis: Individuals must be informed that their personal data is being collected using the legal basis of consent. However, this can be expressed in simpler English, such as "personal data is collected and processed with your consent".

- ✓ Recipient(s) of personal data: If the personal data will be submitted to anyone outside the university, you must state which external parties may receive the personal data.

- ✓ Transfers of personal data to countries outside the EU/EEA: Individuals are entitled to know whether their personal data will be transferred outside the EU. You only need to provide information about this when it occurs. As long as personal data is saved in the cloud services OneDrive (via the university's agreement) and Sunet Survey, this will not

happen. However, please note that Microsoft transfers personal data to the USA when you use your personal OneDrive account, which is not permitted.

- ✓ Storage period: Individuals are entitled to know how long personal data will be stored. This must therefore be stated based on what was decided in step 5. If the storage period subsequently needs to be extended, the relevant parties must be informed of this.
- ✓ Rights: Individuals must be informed of their rights, which include that they have the right to request that erroneous information is corrected, the right to obtain copies of their personal data, the right to have their personal data deleted, etc.
- ✓ The right to withdraw consent: Individuals are entitled to have clear information about how it is always possible to withdraw their consent.
- ✓ The right to complain the Swedish Data Protection Authority: Individuals must be informed that they are always entitled to complain to the Data Protection Authority and supplied with a link to the website: https://www.datainspektionen.se and their email: datainspektionen@datainspektionen.se If personal data that have already been collected is to reused for a new purpose, individuals are entitled to information about this and new consent must be given. If you are unsure, we recommend that you contact the data protection officer so it is done correctly.

The templates for the information letter and consent form are adapted to situations in which information is collected directly from a person. When personal data is not collected from a person, two pieces of information must be added to the above requirements

- The source from which you have collected the personal data: For example, the website, blog, public register, etc.
- What type of personal data you have collected from the source: For example, name, personal ID number, email, assessments of the person, etc.