MIUN 2018/801

2019-09-27

Version 2

Information about GDPR

For employees

Author of the original manuscript:
Åsa Dryselius, University of Borås
Benita Falenius, Stockholm University
Inger Helldal, University of Gävle
Sten Leander, Södertörn University
Erik Stavegren, Swedish University of Agricultural Sciences
Erika Tegström, Mid Sweden University
Jesper Wokander, Malmö University

Editing and structure:
Jesper Wokander, Malmö University

Local processing and editing:
Erika Tegström, Mid Sweden University

Appendix
Checklist for the content of the information that according to the General Data Protection Regulation is to be given when personal data is collected

Foreword:

Due to the common need for a basis for education of universities' staff, students and researchers in connection with the General Data Protection Regulation, the following basic material has been produced in a collaboration between several institutions of higher education. The material consists of modules that can be combined depending on the needs of the individual and is intended to describe the general basics of the legislation. It intends to provide the reader with a basic understanding of the regulation and, hopefully, clarify what applies in day-to-day work. The idea is also that you should know when it is time to seek further knowledge and where this can be found. For specific information about the conclusions from this information and education material, contact the legal function or the data protection officer.

The idea is that the reader begins by reading a common introduction to the new legislation that gives a general overview, and then follows the different modules depending on need. It is to everyone's advantage to be able to easily partake of each block and it is therefore packaged together and not in dedicated modules. The material is not intended to cover the needs of the groups that need a deeper knowledge of the subject, such as data protection officers, archivists, legal counsels and others. These groups are referred to the relevant legal texts.

Index

1.0 Introduction

Background

From 25 May 2018 the General Data Protection Regulation will replace the old Data Protection Directive, which has been in effect for some 20 years. Technological advances have been made very quickly over this period, particularly regarding collection and processing of personal data. Companies like Google and Facebook have grown into some of the world's largest and most profitable companies, selling personal information as their main source of revenue. The protection afforded the individual by the former data protection directive, in Sweden laid down in the Personal Data Act (former PUL), has proved to be inadequate. The EU has therefore adopted the new General Data Protection Regulation, the purpose of which is to strengthen the protection of personal privacy and to create a single set of rules for the entire EU. Anyone processing personal data of persons within the European Union must, regardless of whether the processing takes place inside or outside Europe, respect people's fundamental rights and freedoms, particularly their right to protection of personal data. This text intends to explain what this means in practice for our university and us as employees. The regulation applies to all processing of personal data and it is therefore important that we understand the governing rules. This applies regardless of whether we are responsible for processing or if processing data is merely as a part of one's daily work.

The term *data subject* is used throughout and refers to an identified or identifiable natural person whose information is used in our work in some way. The difference between these is that the first is visible in plain text, for example in Ladok or Primula, while the other kind of personal data requires for example an encryption key for the person to be able to be identified.

Collection and processing of personal data

Any information that directly or indirectly can be connected to a living person is personal data. This means that it is not only such things as names and personal identity numbers that can be personal data but also usernames, e-mail or IP addresses, biometric data, physiological data, and even a voice recording. Combinations of data are also included as long as it is possible to link them to a natural person through the data. All *processing* of personal data (collect, store, process, etc.) must comply with all the General Data Protection Regulation's principles governing processing. This means, among other things, that:

- the processing is to be done in a lawful, appropriate and transparent way in relation to the data subject,
- data is to be collected for specified, explicit and legitimate purposes,
- data must not be excessive in relation to the purpose for which it is collected, and

- data should be accurate and up to date,

- data must not be stored in the form of identifiable personal data longer than is necessary for the processing, and that
- data is to be processed in a secure manner.

The first three items, that processing is to be lawful and that the data is accurate and is processed securely can almost be said to be self-evident but the three that follow involve restrictions in relation to how we have often handled personal data in the past. Previously we sometimes have been happy to collect what we could given that we might need the data at some point in the future, even that questionable based on the Data Protection Directive. According to the regulation, we have to know what we are going to use the data for when collected. This is because we should not collect more data than necessary, only collect data for legitimate purposes, and because we also need to know how long we are going to use the data (even if we do not necessarily need to be able to specify an exact termination date).

Lawful grounds

In addition to the processing needing to comply with the principles, there must also be *lawful grounds* for the processing. There are six permitted grounds and it is sufficient that one of them is met for the processing to be allowed. Naturally, a combination of grounds is also possible.

- Consent – the data subject has given his/her informed consent to the processing. Consent must be documented and may be revoked at any time.
- The processing is necessary for the performance of a contract in which the data subject is involved.
- The processing is necessary for the performance of a legal obligation, for example laws and authorities' regulations but collective agreements are also included.
- The processing is necessary to protect interests of fundamental importance for the data subject, for example health and medical care.
- The processing is necessary for the performance of a task carried out in the public interest or as part of the data controller's exercise of official authority.
- The processing is necessary for a third party's justified interests (unless the data subject's interests, rights and freedoms have greater weight). Note that the possibility to use these last grounds is extremely restricted for authorities.

As far as Mid Sweden University is concerned, a large part of our operations constitutes exercise of official authority. This for example includes everything normally associated with education and examinations. Exercise of authority is used in the regulation in a wider interpretation than we normally use the term in in Sweden and comprises what we do within our commission as a public authority. Furthermore, our research is considered to be of public interest and the basis for this is found in the Higher Education Act. The work our students produce probably does not constitute public interest and preferably needs to be based on consent if personal data is used. For more about the students' processing of personal data see under **2.3 Education**. Other grounds may be relevant depending on the circumstances and if you are unsure you should contact the legal function or the data protection officer.

Processing of special categories of personal data (sensitive personal data)

According to the General Data Protection Regulation, special categories of personal data are data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sexual life or sexual orientation. The basic rule is that the processing of such data is prohibited.

There are a number of exceptions to this rule, where those that are most useful in an educational context are:

- the data subject has consents to the processing
- if it is necessary for reasons of substantial public interest,
- if the processing is necessary for the establishment, exercise or defence of legal claims,
- or in the cases stated in Chapter 3 Article 3 of the proposed Data Protection Act (SFS 2018:218). The proposal is that special categories of personal data (sensitive personal data) may under the provisions of Article 9.2 g of the General Data Protection Regulation be processed by an authority

    1. where the data has been provided to the authority and the processing is required by law,
    2. if the processing is necessary for the administration of a matter, or
    3. in individual cases, if the processing is necessary in view of a substantial public interest and does not constitute an improper intrusion into the privacy of the data subject.

Duty to provide information

When we collect personal data, we have a duty to provide information to the data subject that, among other things, must include:

- identity and contact details of the data controller (more about the data controller below),
- contact details of the data protection officer (more about the data protection officer below),
- the purpose of/reason for the processing and support for this,
- who is going to see the data, and
- any transfer to countries outside the EU and information about the level of protection on the part of the recipient.

There are checklists of what this information needs to contain (see MIUN 2018/682). These checklists are included as an annex to this document, but can also be found on the open part of the employee pages about personal data processing. There are also examples of how such information might look in practice.

The duty to provide information also applies if we do not collect the data directly from the data subject. There are some possibilities for exceptions; if the data subject

has already been informed, if it is not practicably possible or very difficult to provide information or if the processing is required by law. A practical example: When a student requests a computer account with us, we normally retrieve data from Ladok. We are then obliged to inform the student that this is being done and the data concerned at the same time as the account is requested. On the other hand, we do not need to specifically notify that a student's study results are entered in Ladok because the Ordinance (1993:1153) concerning the Reporting of Higher Education Studies states that this is to be done.

The processing needs to be done in an appropriate and transparent manner in relation to the data subject. If the data subject has questions or wishes to exercise his/her rights in relation to the processing we perform, it is our duty as part of Mid Sweden University to assist. This applies as long as there are no obstacles to this due to for example secrecy or archiving rules.

The data subject's rights and limitations of these

The General Data Protection Regulation gives the data subject certain rights, the purpose of which is to strengthen the protection of his/her personal integrity and his/her position in relation to the person processing the personal data, which it is important to remember. The basic idea is that the data subject must be able to predict what will happen to the data in question.

As mentioned earlier, this concerns the right to receive detailed information about what the data will be used for, and the right of access to data registered about him- or herself. The data subject has the right to have inaccurate information rectified without undue delay and the right to have personal data erased, rendered that it is legally and practically possible. The data subject also has the right to object to the processing, to withdraw any consents and the right to complain to the supervisory authority if the data subject considers that the processing is wrong.

The right to erase data or restrict processing is not an absolute right and there may be reason not to grant such a request. There may be other grounds that say that we are to retain the data, for example archiving regulations, various rules concerning finance or labour law requires us to preserve material. For example, an employee can certainly request to have their personal data erased from the salary specification we provide to the Swedish Tax Agency but we will not do so because we have a legal obligation to provide this information. In case of doubt as to what should be erased and what should be preserved, Mid Sweden University's archivist should be contacted in the first instance. Generally it can be said that the processing of personal data should be clear and transparent vis-à-vis the data subject and if possible we should comply with the data subject's wishes.

Roles and responsibilities

For all processing of personal data, from the individual student's essays to research projects and administrative systems, there is a *data controller.* The Data controller for the activities and operations carried out within the university is the Mid Sweden

University. It is the university that has the ultimate responsibility for all processing of personal data carried out within the context of our activities and operations. As an individual employee you are to handle personal data appropriately and have knowledge of the rules that apply specifically to your duties.

In the case of research or other collaborations the responsibility for personal data may be shared. If that happens it is important that this is clearly regulated between the parties and that there is a party who has primary responsibility for such aspects as storage for example. At certain times a third party, who then acts as a personal data processor, carries out the processing of personal data. The relationship between processor and controller is to be defined in a written agreement and the processor may not of their own accord process data that comes from the university.

The Swedish Data Protection Authority is the supervisory authority for the General Data Protection Regulation, and thus has responsibility for auditing our handling of personal data and dealing with complaints from data subjects. At the university there is also a Data Protection Officer (DPO) who reviews the processing internally but also provides help and support for the university's operations. The Data Protection Officer will also handle questions and complaints from data subjects and can be reached via the contact details on the website.

In case of errors and deficiencies in processing, both data controllers and the data processors may have to pay penalties (fines). It is the supervisory authority that applies for this and the penalties are imposed by a court of law. The fines are intended to be effective, proportionate, dissuasive and may be very high.

Registry

The university also has an obligation, by means of a registry, to keep track of what the separate personal data processing that are happening within the university. This registry needs to include the purpose of the processing of personal data, a description of data subjects and what is recorded and who will see the data that the processing concerns etc. More details about the registry can be found in the section on **Registration of personal data processing** under **3.0 Common**.

Security

The personal data collected is to be processed in a manner that ensures appropriate security for the data by means of appropriate technical or organisational measures. This includes protection against unauthorised or unlawful processing and protection against accidental loss, destruction or damage. This means that we must ensure that only authorised persons have access to the data and that any databases or systems are covered by various security measures. Deciding on, implementing and monitoring appropriate security measures, both technical and administrative, are required under the General Data Protection Regulation and are to be documented. More under the section **Security in our work** in **3.0 Common**.

Other legislation governing processing of personal data

It is not only the General Data Protection Regulation that governs the handling of personal data but it is complemented both by certain laws already in force and by new legislation that enters into force at the same time as the regulation.

We are already accustomed to the Freedom of the Press Act together with, for example, the Publicity and Secrecy Act governing public access to official documents. The regulatory framework for the archives, that among other things includes the Archives Act, in turn governs which of these documents should be kept and which can be discarded (screening). It is especially important to pay attention to the Archives Act and the Freedom of the Press Act regarding the right to have one's personal data corrected or erased. This is because there may be provisions in these that mean that data may neither be altered nor erased.

In our teaching and research activities the lawful grounds for our personal data processing in many cases are demands in the Higher Education Act, the Higher Education Ordinance or by other laws concerning activities at universities and other institutions of higher education. As an employer, for example, we have a far-reaching obligation via laws and collective agreements to process personal data relating to our employees. There are also rules about personal data in other parts of the legislation. The important thing, however, is to determine that our processing is lawful and why.

In addition to the laws and regulations that already exist, further laws will come into force simultaneously with the regulation. The Data Protection Act will complement the regulation with certain national rules at a more general level but also enables, for example, research by allowing processing in the public interest. The Ethical Review Act is also being revised as regards the processing of sensitive personal data for research purposes. The General Data Protection Regulation also requires a number of consequential amendments to be made to other legislation which means that an intensive legislative effort is going on during spring 2018.

Summary

It is important to be aware of the background to the work tasks you have, but for those who work with personal data in established processing activities, it is important to stay updated on the rules and instructions that apply and in the event of uncertainty contact the person responsible for the processing, the system owner, the research or education director, etc. The General Data Protection Regulation entails some changes and some new rules, but generally it can be said that the demands we already had to preserve the information, but also to screen data, continue to apply. Anyone intending to create a processing of personal data, for example within the framework of his or her research, must comply with the formal requirements for that processing to be OK. Mid Sweden University's legal function and/or the data protection officer can be contacted for advice and support.

2.1 Research

“Scientific research purposes”

According to the General Data Protection Regulation, the processing of personal data for scientific research purposes is to be afforded a broad interpretation and covers, for example, technological development and demonstration activities, basic research, applied research, and privately funded research. Studies that are conducted through general interest in the field of public health are also examples of areas covered by the regulation.

Starting point

The starting point of the General Data Protection Regulation is that the individual owns his or her own personal data and that others may only process the data if they have obtained permission from the individual (consent) or have other lawful grounds for processing, such as data of public interest, exercise of official authority or agreements. Before processing, it must therefore be ensured that a right to handle personal data exists. The processing must then be done in accordance with the applicable rules and instructions. These are completely inter-dependent. It is the person wishing to process the personal data who is to ensure that lawful grounds exist and that the processing is done in accordance with the applicable rules and instructions. It is important to focus on ensuring that the data subject is fully informed of what processing is being done and that the processing is secure.

If there is a possibility to achieve one’s research goals by reasonable means without using personal data, this is not to be used. This also means that the regulatory framework governing the processing of personal data is not applicable and the practical handling becomes easier (note that, depending on the nature of the research, there may be other laws that must be complied with).

Regulatory framework

The General Data Protection Regulation applies to all handling of personal data but certain parts need to be complemented through national laws. A researcher must therefore have knowledge of at least two additional laws; the Data Protection Act (SFS 2018:218) and the Ethical Review Act. The purpose of these two laws is to allow personal data processing for research purposes at the same time as the individual’s rights and freedoms are protected.

The Data Protection Act is being introduced together with the General Data Protection Regulation and complements the regulation in various respects, for example by permitting personal data to be processed in the public interest (amongst other things; research). Should the national law be considered to conflict with the General Data Protection Regulation, the regulation in principle always takes precedence.

It is important to remember that both the General Data Protection Regulation and the Data Protection Act govern the processing of personal data and that research undertaken without the use of personal data is not covered by them. The Ethical

Review Act primarily relates to personal data but also includes procedures carried out on deceased people, which the first two do not.

Permitted grounds for research

In addition to the basic principles needing to be met such as lawfulness, only collecting personal data for legitimate purposes and secure processing, it is also necessary that legal grounds exist for the processing in the case of research. There are in particular two grounds that may be applicable regarding research: processing with consent and the performance of a task carried out in the public interest.

Consent

For consent to be applicable, it must constitute a voluntary, specific and unambiguous manifestation of will. The data subject shall, by means of this, either by a statement or by an unequivocal confirmatory document, approve the processing of personal data concerning him- or herself. The document must be clearly focused on the processing of the personal data and not mixed up with other explanations and opinions on the part of the individual. For consent to be valid there must be a clear description of the data that is to be collected and the purpose for which it will be used. The individual then needs to take a position on this. It is the person who intends to process the personal data who is responsible for formulating the description of the purpose.

Consent is to be documented and stored in order to be produced as necessary. For information about which parts of and for how long the research material is to be saved, see Mid Sweden University records management plan. It is important to note that the data subject may revoke consent at any time without any requirement for justification. Revocation of consent means that it is no longer permitted to perform new processing of the data subject's data based on consent. Already completed processing, e.g. produced research results, may however continue to be used. Note that processing that was originally done with consent as the lawful grounds may have changed grounds over time, which means that certain processing can still continue, e.g. financial accounting of a project. In case of doubt, the legal function or the data protection officer should be consulted.

Because consent must be voluntary, it is problematic if there is any kind of dependency situation between the parties that renders the relationship unequal. An example of such a relationship is if the university wishes to do research with the help of personal data relating to students or employees of the university. If it can be suspected that consent is not strictly voluntary, a review must be made on a case-by-case basis. Where it is found that it may be questionable whether consent can be considered voluntary, it is not possible to use it as lawful grounds for processing.

The General Data Protection Regulation opens up for a broader view of consent in the context of research than previously applied. The underlying documentation states that it is often not possible to fully identify the purpose of the processing of personal data for scientific research purposes at the time the data is collected. A data subject should

therefore be able to give their consent to certain areas of scientific research when accepted ethical standards in scientific research are observed provided that this can be done without sacrificing the requirements to specify the purposes and that a renewal of the consent is necessary in the case of other purposes. In practice, research can most likely be conducted on previously collected material provided that the new research is in line with the purpose for which the material was previously collected. As stated, this is new and how far this extends will become clearer as time goes on.

The following applies to consent:

- there must be a clear manifestation of will on the part of the data subject,
- there may not be an unequal relationship between the person who gives their consent and the person who collects it for the processing of personal data,
- it can be withdrawn at any time and no new processing may then take place,
- express consent constitutes valid grounds for processing sensitive personal data, and
- it is not certain that further processing for research purposes is permitted without new lawful grounds.

The relationship between the data subject and the data controller must not be unequal. It is for example doubtful whether consent may be entirely voluntary if the data subject is dependent on the data controller for necessary care and may believe that consent to a research study is necessary to receive said care. It is thus extremely important how information about, for example, a study is given and that it is clear that there are no negative aspects of refraining from participating, neither specific nor implicit.

Public interest

On the basis of public interest personal data may be processed for research purposes if the processing is necessary and proportionate in order to conduct research in the public interest. If it is possible to fulfil the purpose of the research without personal data being used at the same time as this does not lead to the work thereby becoming unnecessarily complex or expensive, it shall not be used. However, if it proves difficult to achieve results without personal data, its use is normally permitted.

In the case of personal data for research purposes, a necessity assessment should be made; the processing must be judged to be necessary to be allowed to conduct the research. A reasonability assessment also needs to be made of what alternative ways of performing the research task are possible. The assessment also includes the possibility that use of personal data can provide higher quality and reliability of the research material. A better result can therefore be permissible grounds for using personal data even if it would have been possible to achieve a result without.

The data subject's rights and restriction of these rights within research

The General Data Protection Regulation among other things gives the data subject the right to be given information about the processing, the right to know what data is

processed and be provided with extracts of data concerning him-/herself, the right to have inaccurate data rectified, and the right to have personal data erased if no lawful grounds exist for retaining it.

In case of questions concerning the data subject's rights, the legal function or the data protection officer should be consulted.

Ethical review

The starting point for special categories of personal data (sensitive personal data) is that use of such data is prohibited. This applies to data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, and data concerning a person's health, sexual life or sexual orientation. Under certain conditions, it is nonetheless permitted to use this data, which as far as research is concerned primarily requires an approved ethical review application. If you process data within these categories but the collection of data was completely anonymously, an ethical review is not necessary.

In Sweden, we have had this kind of ethical review for a long time. The most important difference that the General Data Protection Regulation entails compared to previous laws is that there are more categories of personal data that require an ethical review. Student projects have hitherto been exempt from ethical review but a proposal has now been put forward to change this. This proposal, however, does not mean a change in the perception of what constitutes research but only the preconditions for ethical review.

In addition to when research is conducted on material containing special categories of personal data, an approved ethical review is required to be allowed to conduct research on material that contains personal data concerning offences. Other situations requiring an approved ethical review are research on for example material from a deceased person, if what you want to do entails a distinct risk that a person will be harmed physically and/or mentally, etc. See Section 4 of the Ethical Review Act for more details about these situations.

If the research is conducted based on consent, according to both the General Data Protection Regulation and the Ethical Review Act this must be explicitly stated. This means that the requirement is overall more stringent than for consent as regards processing of personal data.

In case of questions regarding ethical review, contact either Mid Sweden University's Research Ethics Committee or the regional ethical review board in Umeå, www.cepn.se.

2.2 Administration

Within the university's administrative systems, various kinds of processing of personal data takes place, all of which are governed by the provisions of the General Data Protection Regulation. All processing must have a clear purpose, the data subject has the right to information about what is done and what data is processed, and has a number of rights such as protection of personal rights and freedoms. Nor is it permitted to collect more data or retain data longer than is necessary to do our job. How long this can be varies greatly depending on the type of task concerned and the reason why it is used.

Permitted grounds

All processing must have a lawful basis. Regarding processing within the administration, the primary rule is that the processing is necessary to fulfil a legal obligation via legislation or that the processing is part of our exercise of official authority. These two grounds together cover the majority of the university's administrative functions and therefore the implementation of the data protection regulation do not involve any major, direct changes in the practical work within the administration.

- Financial events are governed by, for example, the Annual Accounts Act and the Accounting Act.
- Personnel administration at the university has, among other things, to comply with the Employment Protection Act, the Work Environment Act, the Non-discrimination Act, and collective union agreements.
- The university's processing of students' personal data is largely regulated by the Higher Education Act and the Higher Education Ordinance and the Ordinance concerning the Reporting of Higher Education Studies etc.
- In our exercise of official authority we are, among other things, governed by the Freedom of the Press Act, the Administrative Procedure Act, the Publicity and Secrecy Act and archiving legislation.

Types of personal data and their processing

The types of personal data collected in administrative contexts are mainly names, contact details, personal identity numbers, and taxation and bank information. The first three items exist to be able to make a correct identification of the employee and the latter two, naturally, to be able to pay salaries and make other payments with the correct amount of tax. It is important to remember that the Swedish personal identity number is an piece of data that should be handled with care, and only if it is necessary to uniquely identify a person, which is usually the case in our administrative systems. If it is doubtful whether the personal identity number is actually needed, contact the legal function to discuss the matter.

In some systems, such as the HR system, it is possible to add voluntary personal data of one's own. This might for example consist of information about close relatives, which of course makes it easier for the employer if something should happen but is

optional. The same applies to photos of employees on the employee portal; this is also optional.

Information about employees who are ill is also processed by the university based on, among other things, the Sickness Pay Act. This is both for the employee to be paid the right amount and for the employer to be able to fulfil its responsibilities regarding rehabilitation. This data is then removed in accordance with the National Archives' regulations: RA-FS 2012:9.

Other types of documents in which personal data is processed within the administration are application documents, contracts, information on ending of employment, different types of decisions, salary details, income statements, receipts and declarations in case of illnesses. For a complete list of different types of document, see Mid Sweden University records management plan.

Summary

In summary, for a person working at Mid Sweden University, it can be said that details of what lawful grounds an instance of processing stands on, the wording of the purpose or the registration of the processing etc. is often something that the individual employee does not need to take a position on. The purpose, the registration and the legal grounds apply to all the processing, and thus for each individual case within the application. Work with for example Ladok is therefore a kind of processing the aim of which is to record results of studies; it is in the registry, and has its basis in a legal obligation. This is true for everyone who enters results without the individual employee needing to report this on a continuous basis. As an individual employee you are to handle personal data appropriately and familiarise yourself with the rules that apply specifically to your duties. If you are unsure of what is required of you in this regard, talk to your immediate superior.

2.3 Education

Personal data in education

To be able to provide education, we also have to handle personal data. It is necessary for us to know what we teach and be able to record and report the progress our students make in their respective programmes. At the same time, this processing is also covered by the requirements of the General Data Protection Regulation and it is necessary for us to comply with its rules and principles as well as have permitted grounds for the processing.

Permitted grounds in education

Regarding to the lawful grounds in the field of education, the starting point is that in most cases processing is carried out with the grounds of "information of public interest", "part of exercise of official authority" or "legal obligation". For more details about grounds, see the section on **Lawful grounds** under **1.0 Introduction**.

"Consent" can not normally be used in cases where the data subject is in a position of dependence in relation to the data controller. As an education provider, we have a clear advantage over our students; therefore, the processing of students' personal data can be based on consent only in exceptional cases. The fact that the education is based on voluntary participation does not affect this. Consent can only be used as grounds if no negative consequences occur because of consent not being provided. These consequences need not be formal, but may be of an "it is voluntary ... but everyone does it..." nature and thus refer to social conditions. However, other grounds are permitted for work within the university's courses and programmes.

- *Public interests*
  Public interest serves as a legal basis for processing of personal data. The traditional view is that everything an academic institution does is generally considered to be in the public interest. According to the data protection legislation, however, this public interest should be explicitly expressed in Swedish law to be used as grounds for use of personal data. This can be done by either law, ordinance, government regulations or collective agreements. etc. It must also be necessary to process personal data to achieve this public interest in order for it to be used as grounds for the processing.

- *Part of exercise of official authority*
  It must be stated at the outset that the expression *exercise of official authority* is not the same as that used in the Administrative Procedure Act, but the concept in EU law that is used. This means a widening of the scope of the term compared to before. If a measure within the framework of exercise of official authority at an institution of higher education requires processing of personal data, this can be used as grounds for the processing. Examples of this are as good as all activities and operations that an institution of higher education is to perform under the Higher Education Ordinance. It is important to note, however, that the processing of personal data must have a

clear link with the task that is part of the exercise of official authority. If the task can be accomplished without personal data being used, we do it that way.

- *Legal obligation*
  In order for a legal obligation to constitute grounds for processing personal data, this must be established in Swedish law, including decisions by the government or public authorities or through collective agreements. The difference vis-à-vis the two grounds discussed above is that the legal obligation must be sufficiently clear so that the individual can understand what kind of processing will be carried out on the basis of the legal obligation. A typical example of this kind of obligation is the Ordinance (1993:1153) concerning the Reporting of Higher Education Studies etc., also known as "The Ladok Regulation".

Students' personal data processing

Mid Sweden University is not only responsible for the processing of personal data carried out in administration and research, but also for the students' own processing as long as it is part of their education. This means that if a student uses personal data for their studies, the same rules apply as for the university's other processing. There must therefore be grounds for the processing, the principles must be followed (it must be lawful, transparent, accurate, and efficient and concern a minimum of data), the data subject must be informed, and the processing must be registered via the supervisor/course teacher. More details about this can be found in the section on **Registration of personal data processing** under **3.0 Common**.

Students conduct personal data processing within the framework of their education when they, for example, write final theses. However, this is not limited to just final theses but all the essays, reports, etc. that are written within the framework of the education are encompassed if the student uses personal data. It is therefore important that course teachers and those who work as supervisors are well aware that the rules for the processing of personal data also apply to our students and can support them in this. To provide help and support, Mid Sweden University has produced an information document directly targeted to students who will process personal data and that covers the most frequently asked questions. This information document contains a step-by-step guide through what is required of the student and the university (see **4.3 Personal data processing in conjunction with student projects**). An annotated version of this guide exists for supervisors/course directors (see **4.2 Personal data processing in conjunction with student projects – with notes for supervisors**). The legal function, the information security officer, the archivist and the data protection officer can provide further support.

Grounds for processing in conjunction with student projects

If students' projects will contain personal data, it can be difficult to find grounds for the processing in addition to consent. This makes it particularly important that one

understands the importance of providing accurate information to the data subject and documenting and saving consents in some way. It may be appropriate to consider whether it is necessary that the project actually contain personal data or if it could be solved with anonymous data that is not subject to the legislation's requirements concerning for example lawful grounds, information and security. What is important here is to remember that this applies to not only the completed student project but also the path leading up to it. If the completed work does not contain personal data but such has been used for example during the course of the writing or development process, the normal principles, which were taken up under 1.0 Introduction, apply.

It is also important to remember that the pseudonymised data is considered to be personal data. It must thus not be possible to recreate a link between the data and the natural person in order for it to be considered anonymous and thus exempt from the data protection legislation.

What a student may collect with consent as the grounds for processing is not limited *per se* but the data may not be more extensive than necessary and must be collected for a specific and explicitly stated purpose. Collection, processing and storage must be done in a secure manner that corresponds to the sensitivity of the data and, in exactly the same way as for other processing, an impact assessment must be made if it is likely that the processing can lead to a high risk to the rights and freedoms of the data subjects. In case of questions concerning when such an assessment is needed and for help with the assessment, contact the data protection officer.

3.0 Common

Registration of personal data processing

Mid Sweden University is data controller for all processing within our university, ranging from the individual student's project reports to the major administrative systems and research projects that require an ethical review. To have control over what instances of processing are going on and be able to detail these for the supervisory authority, there is a registry where the processing of personal data is to be entered. Mid Sweden University uses the digital tool DraftIT to compile this registry.

The person responsible for the processing is the one who is required to enter information about the processing in DraftIT but this is also good to know for those working within an existing instance of processing. Details to be entered include the following:

- contact person for the processing,
- purpose/aim of the processing,
- a description of the types of data collected,
- who can access the data,
- for how long the data will be used (if this is possible to state)
- if possible, a description of the technical and organisational security measures.

All processing of personal data within the framework of the university's activities and operations is to be registered: from various super-systems down to individual student projects (if they contain personal data). If you need to register an instance of processing, contact the legal function for more information. Registration is not to contain any of the material to be processed but only information about the processing and who is carrying it out.

Anyone who is responsible for an instance of processing must have knowledge about the permitted grounds, the duty to provide information and the principles for registering processing. For example, this can be the system owner of one of the university's systems, the main user of digital services or someone who sets up an instance of processing within the framework of their research. For those who only work in a system that uses personal data, it is important to have knowledge of what applies but it need not be at the same level of detail as for the system administrator or the system owner.

Security in the work

When it has been judged that lawful grounds exist for processing of the specific personal data, all processing – in all parts of the flow – needs to take place in accordance within the rules and binding instructions. It is the person who initiates the processing who is to ensure this.

The General Data Protection Regulation imposes very high demands a person processing personal to document how this is to be done in a satisfactory manner. This means that before a project with personal data is processed, it must be ensured that

there are sufficient safeguards, that security is adequate, and that everyone processing the personal data does so in a proper and lawful manner. This must be able to be demonstrated upon request and it is therefore important to have clear documentation. Here a visit to the employee portal page for "Project support for internal projects" is recommended. There you will find templates and checklists that take up these parts at an early stage.

The security and protection measures to be taken depend on the kinds of personal data that are processed, how sensitive the data is, if there is a large amount, etc.

Here follows a number of examples of possible protection and security measures:

- *Pseudonymisation*. If the data processed is not directly linked to a person but there is a separate key that links person to information, this is pseudonymised data. The information is still formally speaking considered to be personal data but the handling is done with greater security.

- *Encryption and encoding.* Encrypting or encoding data is a way of minimising harm in case of data leakage and is good as technical protection.

- *Anonymisation.* Any information that neither directly nor indirectly can be linked to a living person is anonymised and in a formal sense is no longer personal data. This means that the General Data Protection Regulation need not be used. If the work can be carried out on the anonymised data, this should be done.

- *Access control.* Setting up and documenting the rules for who has access to the data collected is an administrative protection measure that should be used. This also includes devising a set of rules for who is allowed to do what with the information. (Who can read, search, and/or alter and in which parts of the material?)

- *Certification* of the staff who are to work with personal data may be a relevant measure. Information and knowledge on the part of the staff are important security precautions that unfortunately are often forgotten. It is important to ensure that those who work with personal data are also aware of and comply with the rules that exist for the work.

- *Physically separate servers, backups etc.* Although the General Data Protection Regulation does not require data to be technically protected from loss through different types of incident, it is necessary for properly functioning data security work, which we are obliged to have under other regulatory frameworks. An absolute minimum is to ensure that the data is stored in a way that is covered by backups.

- *Screening and deletion.* Personal data that is no longer needed for processing is to be deleted. Follow screening decisions and consult the archivist if

necessary. It is a good idea to visit the internal page for archives and see what quick guides are available for help and support.

Impact assessment

The General Data Protection Regulation requires that an impact assessment be made if the processing is deemed likely to lead to a high risk to people's rights and freedoms. The person responsible for the planned processing must then assess the consequences of the processing for the protection of personal data. This assessment must be documented in writing and done in collaboration with the data protection officer. If it is unclear whether the planned processing "is likely to result in a high risk", the data protection officer should be consulted.

Storage and screening

Preservation and screening of personal data is carried out according to the university's records management plan, which can be found on the employee portal page for archives and follows the National Archives' regulations. With regard to the storage of personal data, it is to be stored in a secure manner at Mid Sweden University in accordance with the storage rules that have been drawn up. If a new cloud service is to be used, only cloud services approved by the working group on data protection or the information security officer should be used. More about archives under **4.1 Archiving**.

Internet and social media

The Swedish exemption for personal data in unstructured material contained in the Personal Data Act is lost in the General Data Protection Regulation. This means that use of personal data on for example the Internet, in e-mails, on social media, etc. must comply with the regulation. We must therefore find legal support for each use of a name, image, or other personal data we have. This may be particularly problematic concerning use of personal data on the Internet and social media sites.

The Higher Education Act stipulates that institutions of higher education are to interact with surrounding society and inform about our activities. This thus constitutes legal grounds for use of personal data for example marketing of current research projects, what is happening quite generally at the university, collaboration with industry/municipalities/other universities, etc. If personal data is collected in various major contexts such as annual ceremonies, fairs, conferences, student induction days, etc. by for example photographing or filming, there are, therefore, according to the above reasoning, grounds for doing so. On such occasions, it is rarely or never possible to identify everyone in the pictures without risking making the event impossible. It is therefore not necessary to identify everyone and obtain their consent for the data collection. We must, however, as far as possible inform people about what we are doing and what we will use the personal data for. This can be done when people register for the event, when invitations are sent out, and restated via roll-ups on site etc.

It is also permissible to publish photographic overviews from our events where individuals cannot be identified, or where the person depicted has approved its publication. In these aspects, our website and social media do not differ from each other.

If we know who is in the pictures, information must be given to these people directly. For the content of this information, see the checklists in document reference no MIUN2018/682 (also provided as an annex to this document).

Uploading to our own web

Uploading personal data to one's own website based on one's own servers (or on servers within the EU/EEA under our control) does not mean that the data transfers to third countries, even though it might be accessed all over the world. The personal data we have collected to inform about our activities or interaction with surrounding society may therefore be uploaded/published on our own website as long as it is on our own server or at least not moved outside the EEA. No further support for this than what we have for collecting the data to begin with is therefore needed.

If publication on the web is part of, for example, a research project, procurement or an employment procedure, there is support for using the personal data in the basic processing. On the other hand, we have to state that the web will be used unless this is already clear from, for example, the placing of an advertisement.

Social media

We are responsible for ensuring that the use of personal data on the university's social media complies with the provisions of the General Data Protection Regulation. Examples of social media are LinkedIn, Twitter, Facebook, Youtube, Instagram, Snapchat, etc.

Most social media are based in the USA, for example Facebook, Instagram, Twitter and Youtube. Uploading data there often means a transfer of personal data to a third country, which is only permitted if there is legal support for the transfer. Today we as a university need express consent for the transfer of personal data to a third country to be able to upload pictures of identifiable people, name people, etc. on social media sites, regardless of whether it concerns a student, an employee or an external party regardless under the circumstances.

Consent to transfer of personal data must be in writing, recorded or clearly documented in some other way and must be retained so that it can be reviewed. It must also be able to be simply revoked so that future use of the personal data is stopped. Before consent can be given, the data subject must first receive the general information about what we will do with the personal data together with information that we cannot guarantee that the use of personal data will be limited to what we have collected the data for. See for example the agreement with the associated information letter that the Communications Department uses for, among other things, arranged photo sessions (MIUN 2018/53).

E-mail

Large amounts of personal data are being handled via e-mail, and this will continue. The main principles are the same as for any other personal data contained in the regulation, i.e. that personal data may only be used when necessary, must be processed in a lawful and correct manner, etc. and is to be saved only as long as is necessary. It is therefore extremely important to familiarise oneself with what an official document is, when official documents may be removed (deleted), etc. to be able to make an assessment of when you may throw an e-mail message away. Thus, there is no simple answer as to when an e-mail can be disposed of but this depends entirely on the content.

What will be a challenge is to go through the e-mail that already exists (because they are also covered by the new provisions) but it is also important to more generally adopt a new attitude towards e-mail and see it more as a tool than as an unstructured filing system. If you are unsure about what should be erased and what should be saved, Mid Sweden University's archivist should be contacted in the first instance.

Handling personal data in special cases

Not all cases of personal data processing can, however, be said to be legal requirements or exercise of official authority. An institution of higher education has a wide range of activities and it may be necessary to process personal data based on consent, for example at our various events with participants from outside. Note that a consent is to be documented and stored so that we can produce it as necessary. The data subject can only provide it him-/herself and it is therefore important that we ensure that the data subject has given consent, particularly in the case of sensitive personal data. Note, for example, that if we when arranging a dinner collect data on diet depending on any allergies, this constitutes sensitive personal data. In connection with questions about diet, it may be appropriate for us to word the question such that it refers to "needs" rather than health information.

4.1 Archiving

Mid Sweden University is an authority and therefore has responsibility for something called "archive formation". Archive formation consists of the information at the authority such as official documents, which naturally in many cases contain personal data.

The data must not be stored for longer than is necessary considering the purpose of the processing. This provision does not prevent an authority from archiving and preserving official documents or Mid Sweden University's archived material later being taken care of by an archive authority. The procedure is instead a lawful basis and counts as performing a task in the public interest.

According to archiving regulations, authorities' archives are to be preserved, kept in order and maintained such that the following are satisfied:

- *The public's right of access*
  The principle of public access to official records contained in the Freedom of the Press Act is central to the Swedish legal system. It means that the general public, often as individuals and representatives of the media, have a right to transparency in the work of the authority and access to its official documents. The official documents describing the authority's activities and operations over time must therefore be preserved.

- *The proper administration of justice and the administration*
  Documents showing what the authority or individual officer has done or not done, for example what the authority has agreed through an agreement with someone, are important to preserve.

- *The needs of research*
  Documents that are deemed to be valuable for future research are to be preserved. This assessment is often made in consultation with the university, primarily with the university's archivist.

In addition to the requirements concerning preservation, there is obviously an internal need to save information in order to be able to follow our own operations through concluded and archived matters and projects.

The term *document* and types of document

The term *document* is defined in Chapter 2 Article 3 of the Freedom of the Press Act:

"Document is understood to mean any written or pictorial matter or recording which may be read, listened to, or otherwise comprehended only using technical aids". A document is not limited to paper, digital files or similar.

There are different types of document:

Working document – this includes drafts or concepts for an official decision or written communication and memoranda. The document is not official if it has not been expedited or taken care of for archiving. A memorandum is for example a memo or similar or a recording that has only been created to be able to present the matter before a decision or one in the drafting process. A working document that adds one or several facts must always be preserved.

Official document – a document is official if stored, received or drawn up by an authority.

Public document – the general rule is that documents that are official are also public. This means that whoever requests the document may read it, look at it or partake of its contents in some other way. Exceptions can be made if there are regulations concerning confidentiality that must be observed.

Document subject to secrecy – Official documents or information in an official document can be protected by professional secrecy, in accordance with the Public Access to Information and Secrecy Act with respect to:

- national security or the country's relations with any other country or international organisation,
- the country's central fiscal policy, monetary policy, exchange rate policy,
- activities relating to inspection, control or other supervision,
- interest to prevent or prosecute criminal offences,
- the public's economic interest,
- the protection of the individual's personal or financial circumstances, or
- interest to conserve animal and plant species.

Preservation of documents

The main principle is that official documents must be kept!

Erasure means destruction of an official document or information in an official document and is therefore a restriction of the right of public access to official documents regulated in the Freedom of the Press Act. To erase an official document, whether it contains personal data or not, must be supported in the regulatory framework. Decisions on erasure that state what official documents may be erased, and after how long, can be found on the web page for archives on the employee portal and in the registry.

Official documents may be erased if the archival material that remains satisfies the public's right of access, the need for information in the administration of justice and the administration and/or the needs of research. Working documents may be cleared without any support in the regulatory framework, as these are not official documents.

Archiving – privacy by design

The expression *privacy by design* means allowing privacy issues to affect the system's entire life cycle – from preliminary study and requirement specification through

design and development to use and discontinuation. Some basic principles in the protection of privacy are, as we have said, to not collect more data than is needed, to not keep it longer than necessary, and to not use it for any purpose other than that for which it was collected. Stating how the data is to be processed, requesting consent and allowing insight in the further handling of the data are also a part of this.

Privacy by design goes hand in hand with the requirements that the archives set when a new IT service is to be developed. The requirements are set to allow the archiving of official documents deemed to need to be preserved, but also to allow documents that are not to be kept to be destroyed.

Archive requirements – some practical examples

- Possibility to make an archive retrieval with information for preservation or migration.
- Possibility to, among other things, be able to differentiate between information that must be preserved and information that is to be erased.
- Possibility to convert file formats to preservation/standard format.
- Possibility to give files unique designations.
- Possibility to maintain good quality of information, for example pre-selected terms or values.
- Possibility to use metadata to for example be able to separate out documents containing personal data.
- Possibility to be able to log events.
- Possibility to provide official documents.

Archiving – specific to research

Research activities are basic research, applied research and development work carried out at universities and other institutions of higher education under the Higher Education Act or by special research institutes as well as in operations-oriented research at other public authorities in accordance with instructions or special commission.

Documents to be preserved under the National Archives' regulations and general guidelines on deletion of documents in public authorities' research activities (RA-FS 1999:1) along with Mid Sweden University's local erasure decisions regarding research are documents that:

- contain basic data about the project's purpose, method and results
- reflect the project's context with respect to for example financial circumstances and external contacts, and show any changes in focus during the course of the work.
- are considered to have continued interdisciplinary value or value for other fields of research that is considered to be of great historical value as regards science, culture or person, or is deemed to be of great public interest.

Examples of such documents that are to be preserved are:

- Datasets, including code keys.
- Metadata (e.g. the kind of data contained in a data management plan.
- Project applications.
- Decision on funds.
- Ethical review documents.
- Survey and interview forms.
- Reports, publications and theses.

In addition to the above examples, documents which help provide a good understanding of what took place during the project and how the data is to be interpreted are also to be preserved. If you have questions about what is to be archived and how, contact Mid Sweden University's archivist.

4.2 Processing in conjunction with student projects – with notes for supervisors

Introduction

Mid Sweden University is data controller for all processing of personal data done within the university's activities and operations. This also applies in cases where our students work with personal data in their student projects, whether it be a simple survey with a picture of the person spoken to or an advanced degree thesis. It is therefore important that a supervisor can help guide our students in the applicable regulatory framework, make follow ups on how students work with personal data, and is able to provide correct information. In brief, the processing must be entered in our registry of personal data processing operations, the data subjects are to be informed, the data is to be collected correctly, processed and stored in a secure manner, and ultimately be deleted or archived as the case may be. How the student handles, and has handled, personal data during the course of the work must also be followed up.

This text intends to be a support for those who supervise students working with personal data in their studies and to provide the basic knowledge needed for the processing to be correct. For obvious reasons it is not possible to give a full and exhaustive explanation of the General Data Protection Regulation here, but the text intends to provide enough knowledge to handle a normal student project where personal data is processed.

There is a short guide in eight steps for students who intend to use personal information. The text of the student guide is shown in the *italicised sections* in this chapter. Explanations and notes follow these for supervisors. The student guide can be found in its entirety, but without notes, in chapter 4.3. In case of doubt, the legal function, the archivist or the data protection officer should be consulted.

———————————

The EU's General Data Protection Regulation together with a number of Swedish laws related to it set strict requirements that all work with personal data be carried out correctly. Mid Sweden University has formal responsibility for the processing of personal data carried out throughout the university which also applies to our students' own handling of personal data within the framework of their studies.

If you as a student intend to use personal data in an essay, degree project or something else that is related to your studies at Mid Sweden University, there is therefore a great deal to consider. This text provides a short walk-through of the steps necessary for the processing of personal data to be correct. In addition to the rules applicable to personal data, there may, depending on what you intend to do, be additional rules to take into account and you should therefore have a comprehensive discussion with your supervisor about what information you intend to process and how and plan accordingly.

Step 1 – Does personal data need to be processed?

The first question is if it is really necessary to process personal data? An investigation might be able to be carried out without personal data being processed and if so, this is preferable. If you do not use personal data, the General Data Protection Regulation does not apply, which makes your work easier. However, it is important to remember that all information that can directly or indirectly be linked to a living person is considered to be personal data, which means that it is not only such things as name, personal identity number, DNA or portrait photos that are personal data. It can also be a combination of more anonymous data that in total makes it possible to identify a specific person.

Example. The combination of a person's age and shoe size along with group membership is not personal data if we only know that it is a question of a Swedish citizen but can be if it is known that the selection is limited to a small group such as the Swedish Academy.

What is a piece of personal data?

The definition of a piece of personal data in the General Data Protection Regulation is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". To summarise this rather complicated definition in a more accessible way, what it says is briefly that:

> "personal data is any kind of information that can directly or indirectly be linked to a living person".

This means that it is not only such things that can be linked to a person (for example personal identity number, name, telephone number, DNA or portrait images) but also combinations of data that together make it possible to link the information to a specific person that constitute personal data.

What is processing?

The General Data Protection Regulation defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

As can be seen, the list of examples is a long one and can basically be summarised as saying that processing is everything you can do with personal data, including merely storing it. Anyone who handles personal data in some form also performs some form of processing in a legal sense.

Is personal data to be processed?

The first question one should therefore ask oneself together with the student is if he or she needs to process personal data. Where it is possible to obtain the necessary information without working with personal data, for example by using anonymous data, this is preferable. If personal data is not processed, the General Data Protection Regulation does not apply. Note that other legislation may nevertheless be relevant depending on the circumstances. Information in the form of personal data should not be used if this can be avoided.

Important to remember is also that the General Data Protection Regulation does not to any great extent care about in what form the data is handled; if it is in digital form or partly digital form or if it is intended to be part of a registry the data is covered by the General Data Protection Regulation. If the personal data on the other hand exists only on paper that will never be organised or transferred to a digital medium, this is exempt from the regulation.

Step 2 – Define the purpose of the processing and what data must be collected

Before the practical work begins, it is important to make it clear what information is to be collected and why. If you intend to conduct a student project, this should not be a difficult task; the purpose of the processing is quite simply to be able to carry out the investigation that is necessary to underpin your work. However, it is important to think through and formulate the purpose and that you understand what information is needed in order to achieve it. You may not collect information simply because it might be "of use".

Planning

In order to satisfy the requirements of the General Data Protection Regulation, it is necessary to be clear about the purpose of the work and know what data is necessary to achieve it. The regulation requires transparency in relation to the data subject and that he or she is informed already at the time the data is collected about the purpose of the processing and what data will be collected. It is therefore necessary to have formulated a purpose and identified what data needs to be used at an early stage. This

work should be documented in writing and saved should discussions arise during the course of the work or afterwards.

Step 3 – Register the processing

Every instance of processing is to be registered in Mid Sweden University's personal data processing registry. You must fill in the form that your supervisor gives you and return it for registration. You briefly state the purpose of the processing, what kinds of data you plan to collect and process, your contact information, for how long the data will be saved (if this can be stated), if any other party will participate in the work with the personal data, and how the information will be protected. The registry is not to contain any of the collected personal data but is only a list of what information is collected and used so that Mid Sweden University has control over what processing is going on.

Registration of the processing

As mentioned earlier, Mid Sweden University is also the data controller for students' degree projects and maintains a registry of the instance of personal data processing carried on within the framework of the university's activities and operations. Every instance of processing is to be registered which also includes students' use of personal data within the framework of their studies. For this to be practicable, the supervisor or course director must provide a form for each such project, which is to be completed by the student. These forms are then to be compiled at the department. The form among other things contains details of:

- the purpose of the processing,
- contact person for the processing (the student) and supervisor/course director,
- a description of the types of data collected,
- for how long the data will be processed (if this is possible to state)
- and if possible, a description of the technical and organisational protection measures.

A person working within an existing instance of processing does not have to register anything, only the person who begins the processing (for example a student who decides to work with personal data for his or her degree project). Registration is a requirement of the General Data Protection Regulation and is important for Mid Sweden University as a data controller to be able to have an overview of the work that is taking place and if necessary reach the right people.

Step 4 – How can the information be stored and handled securely during the work

Collected data must be processed in a secure manner. Storing collected personal data on the server space you have access to via your student account is recommended. External storage services may not be used for storage of personal data. This applies for example to Dropbox, Google Docs, iCloud, and OneDrive, among others. Many of the digital survey tools that exist cannot be used if no data processor agreement exists between Mid Sweden University and the survey provider.

Security measures

The most basic security measure is to never collect more information than is actually needed for the processing. Information that does not exist can never be mislaid or misused. If it is possible to carry out the work using completely anonymous data, this is, as stated earlier, to be preferred. If it is necessary to be able to link information to person, it might be appropriate to do so by means of a key that links person to information. This key should then be kept separate from the collected personal data. Data protected in this way is called pseudonymised data. It is still personal data in the legal sense but security is significantly better since only the person who needs to make the actual connection has access to the key.

Storage of personal data is to be done in a manner that ensures appropriate protection for the data. The data's sensitivity and the harm the data can cause the data subject are to be weighed against the costs and technical possibilities for protection. In brief, it can be said that the server space that all students have access to has sufficient security to also store sensitive personal data and is therefore an appropriate storage location. The same cannot be said of most of the storage solutions available on the Internet (OneDrive, Google Docs, Dropbox, etc.), which means that they cannot be used to handle personal data. For it to be permitted to use a third party in the processing of personal data, a data processor agreement, for example, must be signed with the provider and such does not currently exist in many cases. This also means that many digital survey tools cannot be used if no data processor agreement exists.

If special categories of personal data are to be processed

Racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sexual life or sexual orientation are the special categories of personal data that exist (sensitive data) and may not be processed at all unless a special exemption exists that permits processing. In the case of degree projects, explicit consent is such an exemption and the data may therefore be processed if the data subject has consented to the processing.

It is important to emphasise that there must be a clear and unequivocal consent to the processing after the data subject has received detailed information about the work. The consent is to be documented and stored so that it can be produced as necessary. Consent can be revoked at any time and further processing based on consent is not permitted. Sensitive data sets high requirements concerning the administrative and technical security measures and all such material should be stored in the student's home directory. If this is not possible, the storage is to have at least the equivalent technical and administrative protection; so do not hesitate to discuss this with the information security manager, the data protection officer or the legal function.

Step 5 – Decide what parts of the information are to be deleted or preserved when the work is over

Personal data may not be stored for longer than is necessary and is to be deleted when it is no longer needed. At the same time, there may be parts of the information that must be retained in order to be able to underpin the conclusions in the degree project or because they are required for future instances of processing. Before the practical work begins, it is therefore important to decide what is to be done with the collected personal data afterwards. What information is to be saved and what is to be disposed of? During the course of the work, there may be reason to reconsider the original plan but it is important that there is a basic plan that is agreed with your supervisor or course director (depending on the structure of the assignment). This is not least in order to be able to answer questions from the people whose information you want to use (the data subjects).

Discard or save?

Typically, personal data is only used as basic information for a student project and more rarely in the finished paper, the finished product or service. It is therefore important to be able to decide what parts of the work are to be preserved and what is to be erased. The basic principle regarding collected personal data is that it may not be handled for longer than is necessary. At the same time, it is important to be able to justify the conclusions drawn in the finished work, and it may therefore be necessary to retain information in the form of personal data even after the student project is finished and has been graded.

The student and supervisor, course or programme director, etc. must discuss and decide what needs to be kept and what should be discarded. How the data should be stored must also be included in the discussion and is governed by information given to the data subject. Important to remember is that the students' basic materials are seldom or never official documents and are therefore not covered by Mid Sweden University's records management plan. One exception to this is for example if the students are members of an internal research project.

Step 6 – Obtain consent, inform the data subjects and collect the necessary personal data

Personal data may only be processed if lawful grounds exist for the processing. The General Data Protection Regulation specifies a number of grounds which are regarded as permissible but in the case of a student project it is in practice only consent that can be considered. If it is not possible to use consent, you should raise this with your supervisor and the data protection officer to see if another solution can be found.

Obtaining consent means in practice that you clearly and distinctly state what data you wish to collect, what it will be used for and by whom, and for how long the data will be used. You must also say that it is possible to request to see the information collected and that it is possible to apply to the data protection officer or the Swedish Data Protection Authority with complaints. Once the data subject has been given the information he/she can consent to the processing and it is then permitted to process the data. It is important to know with regard to

consents that they must be documented and saved so that they can be produced if necessary. The data subject has the right to revoke his/her consent at any time. With regard to processing of special categories of personal data (sensitive personal data) based on consent, this must be specifically emphasised when the information is given and it must be made certain that the consent actually covers it. Consult your supervisor or course director if you are uncertain about consents. Note also that requirements are particularly strict regarding security in the handling of special categories of personal data (sensitive personal data).

Grounds for processing

The General Data Protection Regulation permits processing of personal data only if lawful grounds exist for the processing. For students' own handling of personal information consent is normally the appropriate lawful grounds. Consent means that the data subject him-/herself agrees that the data be handled (this assumes that the data subject is at least 18 years old, otherwise the consent of a parent or guardian is required.) For this to be done correctly, he/she must be given clear and precise information about what data is to be used and for what. A consent is also to be voluntary, documented and able to be produced as necessary. An example of how such consent might look can be found on the page for personal data processing on the employee portal. It is also important to note that consent may be revoked by the data subject at any time. Consents are to be saved so that they can be produced as necessary. If consent is revoked, this means that no new data can be collected; however, it is OK to use already collected material provided that the material itself cannot identify the data subject as the source. In case of uncertainty, the legal function or the data protection officer should be consulted.

Information given to the data subject

When the data is collected, the data subject has the right to receive information about, among other things, what the personal data will be used for and for how long it will be used. See the page for personal data handling on the employee portal for useful checklists concerning what this information is to contain. No long explanations are needed: it is sufficient to give the requested information clearly and concisely. This is relatively simple in cases where the information is collected directly from the data subject but the requirement also normally applies in cases where the information is obtained from another source unless one of the exceptions applies.

The data subject also has the right to know, among other things, what the personal data will be used for and the person collecting and processing the personal data has an obligation to describe this clearly and unambiguously. This information can be given in writing, but there is also a right to be given it verbally if the data subject so requests.

Exemptions from the duty to provide information

If the personal data to be processed has already been collected, it may be possible in two cases to avoid having to inform the data subject.

The first is if the data subject has already been informed, i.e. if the data was previously collected for scientific use in line with the processing that is to be carried out through the student project. Personal data that has been collected for scientific processing at the university can thus be reused without the data subject being informed each time as long as information about this has been given when the data was originally collected.

The second is if it is impossible or if it would involve disproportionate effort to provide the information. There may be personal information that can be used in the work but there is no contact information. It may then be possible to process the data without informing the data subject but here it is a difficult balancing act between how difficult it is to inform the data subject and how much risk it exposes the data subject to. When the supervisory authority's audits begin, a praxis will develop around what constitutes disproportionate effort, which will make things easier as time goes on. In case of uncertainty, the legal function or the data protection officer can be consulted.

Even if any of the exemptions are used and the data subject does not have to be informed about the use of personal data, the other rules laid down in the General Data Protection Regulation still apply.

The data subject's rights

The data subject has a number of rights that it is important to keep in mind. As mentioned earlier, this concerns the right to receive information about what the data will be used for, what data will be collected, for how long the data will be saved (or what decides for how long it is to be saved) and the right to be given access to the data registered about him- or herself. The data subject also has the right to object to the processing, to have inaccurate information rectified, to revoke any consent (without needing to give a reason) and to have the right to complain to the Data Inspection Authority if the data subject considers that the processing is wrong.

The right to erase data or restrict processing is not an absolute right and there may be good reason not to agree to such a request. In the case of a degree project, this may for example be the case when a project has been published and the data archived for future research purposes that could be harmed if the information were to be erased. In case of doubt as to what should be erased and what should be preserved, Mid Sweden University's archivist is to be consulted. Generally it can be said that the processing of personal data should be clear and transparent vis-à-vis the data subject and if possible we should comply with the data subject's wishes.

Step 7 – Process the collected material

Provided that the previous steps have been carried out, this is a formal step that does not require any further action. At the same time, this is in practice the main work.

The practical work

This step constitutes the practical work and requires no further explanation in relation to the General Data Protection Regulation. If the student and supervisor have followed steps 1-6, the student can now engage in the actual work.

Step 8 – After the processing, erase or archive the personal data material as needed.

This should also be an easy step since the practical work has now been completed. The material that has been processed must now either be saved or erased according to what you decide in step 5. Report to the supervisor that the processing is finished so that he or she can forward the information to the legal function, which is responsible for the registry.

Personal data after completion of the student project

This step is also part of the practical work and it involves following the plan for erasure and archiving drawn up in step 5. It is also important that the legal function be given the information so that this can be noted in the registry (DraftIT).

4.3 For students – Processing in conjunction with student projects

The EU's General Data Protection Regulation together with a number of Swedish laws related to it set strict requirements that all work with personal data be carried out correctly. Mid Sweden University has formal responsibility for the processing of personal data carried out throughout the university which also applies to our students' own handling of personal data within the framework of their studies.

If you as a student intend to use personal data in an essay, degree project or something else that is related to your studies at Mid Sweden University, there is therefore a great deal to consider. This text provides a short walk-through of the steps necessary for the processing of personal data to be correct. In addition to the rules applicable to personal data, there may, depending on what you intend to do, be additional rules to take into account and you should therefore have a comprehensive discussion with your supervisor about what information you intend to process and how and plan accordingly.

Step 1 – Does personal data need to be processed?

The first question is if it is really necessary to process personal data? An investigation might be able to be carried out without personal data being processed and if so, this is preferable. If you do not use personal data, the General Data Protection Regulation does not apply, which makes your work easier. However, it is important to remember that all information that can directly or indirectly be linked to a living person is considered to be personal data, which means that it is not only such things as name, personal identity number, DNA or portrait photos that are personal data. It can also be a combination of more anonymous data that in total makes it possible to identify a specific person.

Example. The combination of a person's age and shoe size along with group membership is not personal data if we only know that it is a question of a Swedish citizen but can be if it is known that the selection is limited to a small group such as the Swedish Academy.

Step 2 – Define the purpose of the processing and what data must be collected

Before the practical work begins, it is important to make it clear what information is to be collected and why. If you intend to conduct a student project, this should not be a difficult task; the purpose of the processing is quite simply to be able to carry out the investigation that is necessary to underpin your work. However, it is important to think through and formulate the purpose and that you understand what information is needed in order to achieve it. You may not collect information simply because it might be "of use".

Step 3 – Register the processing

Every instance of processing is to be registered in Mid Sweden University's personal data processing registry. You must fill in the form that your supervisor gives you and return it for registration. You briefly state the purpose of the processing, what kinds of

data you plan to collect and process, your contact information, for how long the data will be saved (if this can be stated), if any other party will participate in the work with the personal data, and how the information will be protected. The registry is not to contain any of the collected personal data but is only a list of what information is collected and used so that Mid Sweden University has control over what processing is going on.

Step 4 – How can the information be stored and handled securely during the work

Collected data must be processed in a secure manner. Storing collected personal data on the server space you have access to via your student account is recommended. External storage services may not be used for storage of personal data. This applies for example to Dropbox, Google Docs, iCloud, and OneDrive, among others. Many of the digital survey tools that exist cannot be used if no data processor agreement exists between Mid Sweden University and the survey provider.

Step 5 – Decide what parts of the information are to be deleted or preserved when the work is over

Personal data may not be stored for longer than is necessary and is to be deleted when it is no longer needed. At the same time, there may be parts of the information that must be retained in order to be able to underpin the conclusions in the degree project or because they are required for future instances of processing. Before the practical work begins, it is therefore important to decide what is to be done with the collected personal data afterwards. What information is to be saved and what is to be disposed of? During the course of the work, there may be reason to reconsider the original plan but it is important that there is a basic plan that is agreed with your supervisor or course director (depending on the structure of the assignment). This is not least in order to be able to answer questions from the people whose information you want to use (the data subjects).

Step 6 – Obtain consent, inform the data subjects and collect the necessary personal data

Personal data may only be processed if lawful grounds exist for the processing. The General Data Protection Regulation specifies a number of grounds which are regarded as permissible but in the case of a student project it is in practice only consent that can be considered. If it is not possible to use consent, you should raise this with your supervisor and the data protection officer to see if another solution can be found.

Obtaining consent means in practice that you clearly and distinctly state what data you wish to collect, what it will be used for and by whom, and for how long the data will be used. You must also say that it is possible to request to see the information collected and that it is possible to apply to the data protection officer or the Swedish Data Protection Authority with complaints. Once the data subject has been given the information he/she can consent to the processing and it is then permitted to process the data. It is important to know with regard to consents that they must be

documented and saved so that they can be produced if necessary. The data subject has the right to revoke his/her consent at any time. With regard to processing of special categories of personal data (sensitive personal data) based on consent, this must be specifically emphasised when the information is given and it must be made certain that the consent actually covers it. Consult your supervisor or course director if you are uncertain about consents. Note also that requirements are particularly strict regarding security in the handling of special categories of personal data (sensitive personal data).

Step 7 – Process the collected material

Provided that the previous steps have been carried out, this is a formal step that does not require any further action. At the same time, this is in practice the main work.

Step 8 – After the processing, erase or archive the personal data material as needed.

This should also be an easy step since the practical work has now been completed. The material that has been processed must now either be saved or erased according to what you decide in step 5. Report to the supervisor that the processing is finished so that he or she can forward the information to the legal function, which is responsible for the registry.

2019-09-27
Erika Tegström
DNR: 2018/682
version 3 - English

Mittuniversitetet
MID SWEDEN UNIVERSITY

Checklists for the content of the information that according to the General Data Protection Regulation is to be given when personal data is collected

Checklist for the content of the information

For whom

This checklist is designed for anyone who will use personal data in their work or project, regardless of whether he or she is working in the academy or in the university's administration. The checklist intends to make things easier when you are to compile the information that, according to the General Data Protection Regulation, you are obliged to provide a person whose personal data you will be processing. In the text and in the checklist this person is referred to as "the data subject".

It is never sufficient to simply state that "Mid Sweden University complies with the applicable legislation concerning personal information" or similar - complete information must be provided when the data is collected. Keep in mind that you need to express it in a clear and concise manner and that the information must be adapted to the data subject. The data subject also has the right to get the information verbally if he or she prefers.

The checklist's structure

Depending on whether we obtain the information directly from a data subject (such as during an interview or survey, when registering an account, when photographs are taken, etc.) or if the information is obtained in some other way (i.e. retrieving grades via databases, checking addresses against the national population register, using extracts from medical records) the requirements concerning information differs.

This document is dived as follows:

1. **General information**

   + additional information under 2 or 3

2. **Special rules regarding information that is to be given if personal data is collected directly from the data subject**

3. **Special rules regarding information that is to be given if personal data is collected, but not directly from the data subject**

How to read the checklist

The sections in italics are explanations or exemplifications of the item in question. If you wish to make changes, make it more condense etc. you may do so but make sure not to forget any item, if it is to be included.

The following appears under some of the headings:

"Text that ALWAYS should be included here is as follows:"

This is so that you do not forget to mention that the personal data in question also will be handled according to, among other things, the regulatory framework governing official documents and authorities' records, something that might be easy to miss. If you wish to express this in another way, you are free to do so but make sure that the information is included!

Contact in case of questions and reservations

If you have questions or concerns regarding the checklists and what they address (and what might have been omitted), consult the Mid Sweden University's legal function, archivist or data protection officer.

---

1. General information

Basic information

1. Who the data controller is and provided with contact details and, where possible, the natural person who can represent the data controller.

Mid Sweden University is normally the data controller but be sure to check this. Sometimes it may be a collaboration where there are several controllers, sometimes it may be someone else who's responsible and we only perform the collection as part of an assignment, etc.

A natural person should be someone who is responsible for, for example, a system or a research project.

2. Name and contact details of the data protection officer, e-mail address and phone number.

Look at Mid Sweden University's web to find out who the data protection officer is.

3. The reason for the use of personal data and the lawful grounds for this.

At our university, it might for example be a matter of public interest such as research or exercise of official authority etc. Describe the use briefly so that the data subject can understand how his/her information will be handled. In case of uncertainty as to what regulatory framework applies, contact the legal function or the data protection officer.

Text that should ALWAYS be included here is as follows:

Mid Sweden University is an authority and has an obligation to, among other things, comply with the rules concerning official documents, authorities' records and public statistics. The university will also therefore continue to process the personal data in the ways necessary to comply with applicable legislation.

4. Who will see the personal data or which functions will use it.

For example, only researchers within the project, everyone in the H&R and economics department, any collaborations with other authorities or companies in the private sector.

Text that should ALWAYS be included here is as follows:

If someone requests an official document that contains personal data, Mid Sweden University may release the data. if the document is not to be/may be subject to confidentiality.

5. If it is necessary to transfer the personal data to a third country, i.e. a country outside the EU/EEA or to an international organisation, this is to be stated together with the legal support for this transfer.

Note: Publishing anything on the web does not automatically mean that it transfers to a third country. If uploaded on a social media site, however, it is often such a transfer of which the data subject needs to be notified. There are various possibilities where this can be permitted, together with other information. Contact the legal function or the data protection officer for advice on what applies in the case of transfers to a third country.

Information to ensure fair and transparent processing

a) How long the personal data will remain with the data controller, or, if it is not possible to specify, what determines the length of the storage.

> *For example the research project's duration, legislation or collective agreements on employers' responsibility for employees, archive legislation. Check what applies according to the document management plan. If you are unsure, contact Mid Sweden University's archivist for advice in the first instance.*

Text that should ALWAYS be included here is as follows:

Your personal information is also stored for as long as is required by the legislation on official documents and authorities' records.

b) The right to be given access and, where possible, obtain rectification or erasure of personal data or restriction of the processing relating to the data subject or to object to the processing. The right to data portability (that the information collected should be easily to transfer) is also to be notified where relevant.

> *Once again, a great deal is governed by other legislation, which it is important to be aware of. For example; the scope to request correction in a research project is very limited, in instances of processing that have been archived it is neither legal nor practically possible to correct errors.*
>
> *Data portability in particular is rarely applicable in our activities and operations but exists to make it easier for individuals to change their bank, insurance company, etc.*

c) IF use of personal data is based on consent, the data subject must be informed that he/she has the right to revoke their consent and how to do so. Information shall also be given that revocation does not affect the legality of the use of personal data that took place before the consent was revoked.

> *Information collected based on a consent before it was revoked may therefore continue to be used. However, no new information may be collected.*

d) The individual is to be informed that he/she has the right to submit complaints about the use of his/her personal data. Complaints can be made either to Mid Sweden University's data protection officer or directly to the Swedish Data Protection Authority, which is the supervisory authority.

e) IF personal data must be provided due to a legal or contractual requirement or necessary to be able to enter into an agreement, this is to be stated separately. It is also necessary to notify the data subject if it's a legal requirement that the individual

provides the information, and if there are possible consequences of not providing the information.

Found within the university's administrative processes and within the administration.

f) IF there is automated decision-making based on the provided personal data, this is to be stated together with at least some information about the logic behind, what this way of making decisions means, and what predictable consequences there are of such processing.

Found within the university's administrative processes and within the administration.

Other purpose

IF Mid Sweden University intends to use the personal data for a purpose other than for which originally collected, the data subject must be informed thereof before such additional use is made. Needing also other relevant information in accordance with the section on information to ensure fair and transparent processing.

2. Special rules regarding information that is to be given if personal data is collected directly from the data subject

WHEN personal data is collected, not afterwards, the data subject must be informed of s/he's rights as stated under section 1. It is not permitted to firstly collect information and afterwards inform the data subject; the information must already have been given beforehand.

3. Special rules regarding information that is to be given if personal data is collected, but not directly from the data subject

Exemptions from the duty to provide information

IF any of the exemptions are used, be sure to document this along with at least a short justification as to why the information does not need to be provided.

- If it is impossible to give the information contained in this checklist, or if it would involve disproportionate effort, primarily to be used in archiving, research and statistics contexts.

What constitutes disproportionate effort is determined in the first instance by the data processor but praxis in this area will develop when the supervisory authority's audits begin.

- If providing the basic information in the checklist would likely significantly impede or render impossible the fulfilment of the objectives of the use of the personal data.

For example, a research project would not be able to be conducted.

In the above-mentioned cases, Mid Sweden University can instead take "appropriate measures" to protect the data subject's rights and freedoms and legitimate interests, including making the information available to the public. Feel free to discuss this with the legal function or the data protection officer.

- If expressly stated in the legislation that we are to register or provide information and this type of processing has appropriate measures to protect the data subject's legitimate interests.

For example, Ladok; it is a registration that we perform due to legal requirements.

- If the personal data must remain confidential as a consequence of mandatory secrecy, for example privacy legislation or other laws.

Can involve issues of national security.

If no exemption applies, Mid Sweden University is obliged to give the data subject the information under section 1 and, in addition, also to be given information regarding what personal data will be collected and used.

When to give information

This is to be done at different times depending on the situation:

- Within a reasonable time period after we have received the personal data, but no later than within one month. In assessing what is reasonable, any special circumstances regarding the manner in which the personal data is used must be considered.
- If personal data is to be used to contact the data subject, the information is to be given no later than at the first contact.
- If disclosure to another recipient can be assumed, the information is to be provided at the latest when the personal data is disclosed for the first time.