Processing personal data at Linköping University

– Guidelines

Contents

1 Introduction

The Data Protection Regulation[1] (GDPR) came into force in Sweden and all other member states of the EU on 25 May 2018. The Regulation replaces the Personal Data Act[2], and applies to such processing of personal data that is wholly or partly carried out by automated means and to the processing other than by automated means of personal data that form part of a filing system or are intended to form part of a filing system. The purpose of the Regulation is to strengthen the protection of the privacy of individuals by regulating how the processing of personal data may take place. The Regulation applies to all management of personal data that relate to living natural persons. Personal data may consist of text, images, sound, etc. In other words, they may consist of any information that directly or indirectly makes it possible to identify an individual. The term "processing" is used to denote any measures that are taken with respect to information of this type, such as to examine, consult, print, collect, adapt, etc.

The Data Protection Regulation applies to all operations at Linköping University (LiU). The purpose of these guidelines is to describe the rules that all co-workers at LiU must follow when personal data are processed. The Regulation is new, which means that precedent in its use and interpretation has not been established. This means, therefore, that it is highly probable that the guidelines will need to be updated regularly. Furthermore, the guidelines will be supplemented with other advisory material. The data protection officer can be consulted if clarification is needed, and in certain questions the data protection officer must be included as a party. The website of the regulatory authority contains a great deal of information in the field.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (EUT L 119, 4.5.2016, p. 1)
[2] The Personal Data Act (1998:204)

2 Definitions

The Data Protection Regulation uses concepts that are defined in Article 4. The concepts that are most relevant for LiU are defined below.

Processing (of personal data)	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.
Restriction (of processing)	The marking of stored personal data with the aim of limiting their processing in the future.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Genetic data	All personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Personal data	Any information relating to a living identified or identifiable natural person. 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.
Controller of personal data	A natural or legal person, public government agency, institution or other body that alone or together with others determines the purpose and means of personal data processing.
Processor of personal data	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Filing system	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
The data subject	The one that the personal data concern.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Supervisory authority	The independent public authority established by the government to carry out supervision, at present the Swedish Data Protection Authority.
Third country	A state that is not a member of the European Union (EU) or connected to the European Economic Area (EEA).
Third party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, is authorised to process personal data.
Data concerning health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

3 Processing personal data at Linköping University

3.1 Responsibility for personal data

Linköpings universitet (LiU) is controller of personal data for all processing of personal data that takes place within the university. This is the case not only for the processing of personal data that takes place in the university's administrative systems but also information in the examinatory components of individual students and in research projects, etc. Thus, it is LiU that has the final responsibility for all processing of personal data that takes place within the framework of its operations. It is, however, expected that each individual co-worker will process personal data in a correct manner, and will be familiar with the regulations that apply to the tasks he or she carries out.

Even if LiU has the final responsibility for the processing of personal data, this responsibility passes downwards through the organisation through such instruments as policy documents and delegation to persons who are responsible for the processing of personal data for individuals. Certain people with various functions within LiU may have such a responsibility. The responsibility for larger administrative systems, for example, lies with the person who has the role of owner. Another example concerns individual researchers, who may be responsible for the processing of personal data within the research carried out, depending on the information that is used in it. It is generally the case that the person who creates or adapts a filing system or collection of personal data is also responsible for ensuring that all processing takes place in accordance with the Data Protection Regulation and these guidelines, independently of whether the person has been formally designated as responsible or not.

In certain cases, the processing of personal data takes place on behalf of LiU by a third party, which acts as personal data processor for LiU. The relationship between the processor and the controller is to be regulated by a written contract, and the processor may not process the information that is supplied by the university without the consent of the university *(see Section 4.15)*.

In the event of errors or deficiencies in the processing, LiU and the personal data processor risk being subject to sanction (fines). These are determined by the supervisory authority and are imposed by the courts. The magnitude of the fines is to be such that they are effective, proportional and deterrent. Such fines may be extremely costly for LiU. The supervisory authority is responsible for examining the processing of personal data by LiU, and for dealing with complaints made by data subjects.

3.2 The data protection officer (DPO)

The function of “data protection officer” has been created at LiU. The data protection officer is to hold an independent position and examine the processing and protection of personal data within the university, to monitor compliance with the Data Protection Regulation, and act as help and support for the operations. The officer is to be point of contact for the supervisory authority, and is to consult and collaborate with this authority as required. Furthermore, the data protection officer is to be available to deal with questions and complaints from data subjects.

The data protection officer can be contacted at dataskyddsombud@liu.se.

4 General information

4.1 Application

The Data Protection Regulation is an EU regulation that is directly applicable as legislation in all member states. Supplementary Swedish legislation, such as the Data Protection Act[3], contributes to create a comprehensive regulatory framework for data protection. Certain Swedish fundamental laws, such as the Public Access to Information and Secrecy Act[4] and the Fundamental Law on Freedom of Expression[5], however, remain in force.

The provisions of the Data Protection Regulation apply to such processing of personal data that is wholly or partly carried out by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of some type of filing system.

Processing that takes place for private purposes or for journalistic, academic, artistic and/or literary expression is not subject to the regulations.

4.2 Personal data

Personal data are information of any form that can be related directly or indirectly to a living individual. This means not only such data as name and personal identity number are personal data, but also username, email address, photograph, sound recording, film recording, biometric and genetic information, physiological information, etc. Also combinations of data may constitute personal data if the combination makes it possible to connect the data to a natural person.

Data that cannot in any way be related to a living natural person are not personal data, and the Regulation thus does not apply to such data.

Data that have been provided with, for example, a code key, and in this way can no longer be related to a specific person without the use of additional data, are known as *pseudonymised* data. As long as the additional data can be used to identify a person from the data, independently of whether the additional data are present at LiU or not, the data are considered to be personal data. Thus, pseudonymisation is not equivalent to making the data anonymous: it does, however, constitute effective

[3] Act (2018: 218) with Additional Provisions to the EU General Data Protection Regulation
[4] Public Access to Information and Secrecy Act (2009:400)
[5] Fundamental Law on Freedom of Expression (1991:1469)

protection for personal data. When assessing whether data are personal data or not, consideration should be taken of whether someone, with reasonable technical aids, can identify a person with reasonable probability.

4.3 Fundamental principles for the processing of personal data

The Data Protection Regulation establishes a number of fundamental principles that must always be followed when processing personal data. It is, therefore, necessary that all who process personal data are familiar of these, and use them as a basis when assessing whether a processing operation is permitted or not. The fundamental principles are as follow:

Lawfulness, fairness and transparency. Personal data may only be processed if a legal basis exists. All information and communication related to the processing of personal data are to be readily available, such that the data subject understands how and why the personal data are being processed. “Fairness” in this context is defined as the personal data being treated according to good professional ethics.

Limitation of purpose. Personal data may only be processed for clearly specified purposes, and they may not subsequently be processed for any other incompatible purpose. The description of the limitation of purpose is to be documented, and this is to set the limitations for the processing. There are some exceptions to this principle, which is known as the “principle of finality”. Further processing of personal data for archiving purposes, statistical purposes or research purposes is considered not to be incompatible with the original purpose, provided that the further processing is necessary for these purposes.

Data minimisation. Only personal data that are required to achieve the purpose may be processed. Data that are collected because they “might come in useful” may not be stored. This means that only the data required to achieve the purpose are to be collected, and that only those persons, within or outside the organisation, who require access to certain personal data have access to these data, and the data are not unnecessarily disseminated.

Accuracy. Personal data are to be accurate, i.e. correct, and, if necessary, updated. It is the responsibility of LiU to take reasonable measures to ensure that data not required for the purpose are erased, corrected or updated as rapidly as possible.

Storage limitation. Personal data may not be stored in a manner that allows identification for a longer period than that necessary for the purposes of the processing. When data are to be archived, they must be separated from ordinary

operations, in order to satisfy the requirements set by this principle. This principle sets requirements onto the operations, since it is necessary to have time limits for erasure or control at regular intervals *(see Section 4.23)*.

Privacy and confidentiality. Personal data are to be protected by appropriate technical and organisational measures such that they cannot be accessed by unauthorised persons, destroyed or damaged. This principle makes it clear that the security of personal data is a necessary condition for the protection of the privacy of the data subject.

Accountability. As controller of personal data, LiU must be able to demonstrate that the principles described above are followed. This places more stringent requirements for documentation for the people who are responsible for the processing of personal data during university operations.

The person who creates or adapts a filing system or collection of personal data is responsible for ensuring that all processing takes place in accordance with the Data Protection Regulation and these guidelines, and it is this person who is to ensure that the fundamental requirements are satisfied both when a filing system is created and during the period it exists.

4.4 Legal basis for the processing of personal data

A legal basis is required for the processing of personal data. The permitted legal bases for the processing of personal data are listed below. (It is only necessary that **one** of them be satisfied in order for the processing to be lawful.)

- Consent. The data subject has given informed consent to the processing. The consent must be documented and may be withdrawn at any time.
- The processing is necessary for the performance of a contract to which the data subject is or will become party.
- The processing is necessary for compliance with a legal obligation.
- The processing is necessary in order to protect interests that are of fundamental importance for the data subject.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- The processing is necessary for the purposes of the legitimate interests of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Note that the possibility of using this legal basis is severely limited for government agencies.

The requirement that the processing be necessary in these contexts principally means that it must not be possible to assess that the processing in question can be

replaced by other measures, such as through the processing of completely anonymous information.

Much of the work carried out by LiU is the exercise of official authority, including, for example, education and conducting examinations. The legal basis for processing personal data when conducting research is, in most cases, the performance of a task carried out in the public interest. In general, the legal basis of the processing of personal data that students carry out in examined tasks and degree projects should be consent given by the data subjects. Other legal bases may be relevant, depending on the circumstances in the particular case. In the event of any uncertainty, the data protection officer should be contacted *(see Sections 6 and 7)*.

4.5 Consent

One of the legal bases for the processing of personal data is consent. "Consent" denotes here any type of voluntary, specific and unambiguous indication of the data subject's agreement. The consent must be documented, which may take place in various ways, such as written or digital means. In most cases, obtaining consent is a necessary condition for the processing of sensitive personal data.

When consent is obtained from a data subject, he or she must always receive comprehensive information about what the data are to be used for, etc. *(see Section 4.11)*. Personal data that have been obtained on the legal basis of consent may be processed only for the purpose to which the data subject has consented. If the data are to be used for another purpose, further consent must, in the normal case, be obtained.

Note that the data subject may withdraw consent at any time. If this is done, processing of the personal data must be interrupted, and no new data collected from the data subject. For this reason, consent that has been obtained must be carefully organised. Certain other conditions apply in research with respect to the withdrawal of consent *(see Section 7)*.

4.6 Collection and processing of personal data

During the collection of personal data, the purpose for which they are to be used must be determined, in order to prevent more data than required being collected. A justified purpose for the processing of the personal data must also be defined, and it must be decided how long the data will be used (although it is not necessary to specify an exact termination date). It is necessary that the person who is responsible for the processing of personal data is familiar with the legal bases and the duty to inform data subjects. It is also necessary that this person follow the principles and register the processing in the list of processing being conducted at LiU.

When collecting personal data, information is to be provided to the data subject concerning:

- the identity and contact details of the person who is responsible for the processing of personal data at LiU
- contact details of the data protection officer
- the purpose of the processing and the legal basis on which this is based
- the identity or identities of the person or persons who will have access to the data, and
- information about transfer to countries outside EU/EEA (where relevant), and information about the level of protection at the recipient.

The duty to provide information applies also if the data are not collected directly from the data subject, since information about the source of the data is to be given. Exemptions may be made if the data subject has been previous informed, if it is impossible or very difficult in practice to inform the data subject, or if the transfer of the data is stipulated by legislation.

4.7 Extract from records

One of the rights that a data subject has is that of knowing which data LiU processes. A data subject always has the right to request an extract from the records from the controller of personal data. Such a request is to be sent to the registrar.

Questions of confidentiality are governed by the Public Access to Information and Secrecy Act. This act specifies also that public documents are to be registered, which most often means that personal data will be processed. When a request for an extract from records is made, it must be reviewed also with respect to the Public Access to Information and Secrecy Act.

4.8 Processing sensitive personal data

The following data are classified as “sensitive”: data revealing 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 sex life or sexual orientation.

The basic rule is that the processing of sensitive data is prohibited.

A number of exceptions from this prohibition of the processing of personal data have been made.[6] The following exceptions are the most relevant for LiU:

- The data subject has given explicit consent to the processing.
- The processing is necessary for reasons of substantial public interest and are proportionate to the aim pursued.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

It is necessary when processing sensitive personal data that appropriate protective measures are taken *(see Section 4.21)* and for most of the exceptions, in addition to consent, it is necessary to have the support of Swedish or European legal provisions in order for the processing to be permitted.

Swedish legal provisions[7] state that sensitive personal data may be processed by a government agency

- in block text if the data have been provided in a case or are necessary for the handling of a case
- if the data have been provided to the government agency and their processing is required by legislation, or
- in other cases, if it is unconditionally necessary for the purpose of the processing, and the processing does not lead to undue infringement of the privacy of the data subject.

4.9 Rights of the data subject

The data subject, whose personal data have been registered, has the right to:

- receive clear and unambiguous information about the purpose of the processing
- be informed of how long the data are to be stored
- withdraw consent that has been given, without needing to specify a reason
- gain access to the data that have been registered about him or her, from an extract from the records
- object to the processing
- have inaccurate personal data concerning him or her rectified without delay

[6] Article 9.2 contains a list of all exceptions.
[7] One such is the Data Protection Act, which contains legal provision that make the processing of sensitive personal data possible.

- have personal data erased or the processing of them terminated if used longer than is necessary and legal requirements do not specify otherwise. Such legal requirements may be, for example, regulations concerning the management of public documents or processing of personal data for purposes of research of general interest.
- obtain the personal data held in digital form such that he or she can, for example, exchange one service for another, without the loss of information, and
- present complaints to the supervisory authority.

On the request of an individual data subject, the person who is responsible for the processing of personal data shall without delay correct or limit the processing of, or erase, such personal data as have not been processed according to the Regulation and these guidelines. Where applicable, third parties, to which the data have been disclosed, shall also be informed about the corrections made.

4.10 Limitations to the rights of data subjects

The right to erase data and the right to limit processing are not unconditional rights. LiU may be subject to legal requirements that prevent certain data being erased, and prevent LiU from following the wishes of the data subject. LiU's operations are subject to, among other regulations, the Public Access to Information and Secrecy Act and the Archives Act[8]. Other legislation that leads to, for example, the duty to provide reports, also influences the possibility of data subjects having data erased. In the event of doubt concerning what is to be erased and what is to be preserved, the data protection officer should be contacted. For questions associated with archiving and selective disposal the LiU archivist should be contacted.

Special regulations govern the right of data subjects to have data erased when used in research *(see Section 7.4)*.

4.11 Information to data subjects when data are collected

The person responsible for processing personal data has a duty to provide the data subject with information about the processing when the data are collected. The term "collect" denotes all possible methods by which individuals can disclose information about themselves. This is straightforward when the data are collected directly from the data subject, but this requirement also normally applies in cases in which the data are obtained from another source (such as the combination of data from

[8] The Archives Act (1990:782)

different filing systems, from media or the internet). In these cases, the information is to be passed to the data subject when the data are recorded, and within one month of the recording. Information is to provided about:

- the purpose of the processing
- the source of the data
- the legal basis of the processing
- how long the data are to be used
- the identity or identities of those who will use the data
- a statement that LiU is the controller of personal data
- a statement that the data subject has the right to gain access to the data and to have errors corrected, and
- the availability of a data protection officer, with the contact email address: dataskyddsombud@liu.se, and that it is possible to contact the supervisory authority with any complaints if LiU and the data subject cannot reach an agreement.

Some **exceptions** from the duty to provide information have been defined. If information about the processing has been provided on one occasion, it is not necessary to provide new information in cases in which the personal data that have been collected are used for new purposes that are not incompatible with the purposes for which the data were originally collected. Nor is it necessary to provide information to the data subject concerning such processing of personal data that the data subject already knows about.

Furthermore, it is not necessary to provide information about the processing of personal data if it becomes apparent that it is impossible to do so, or if doing so would require a disproportionately large amount of work. When carrying out such an evaluation, other measures that the person responsible for the processing of personal data carries out in order to provide information about the processing – through, for example, advertising, information leaflets or internet information – are to be considered.

4.12 Notification of processing of personal data

LiU is the controller of personal data for all processing of personal data that occurs within the university operations, covering everything from a degree project of an individual student to huge administrative systems. The university is legally obliged to maintain a list of all ongoing processing of personal data in order to ensure that it is aware of all such processing, and to be able to report all such processing to the supervisory authority. The person who initiates a processing of personal data must provide notification of this to the LiU list. Notification must also be made when the processing of personal data terminates.

Notification is to take place using a form according to instructions from the data protection officer. The notification must not contain any of the material that is processed; it may contain only information about the processing and the identity or identities of those carrying it out. The following information is to be included:

- the purpose of the processing
- contact details for a person carrying out the processing
- a description of the types of data collected
- how long the data are to be processed (if it is possible to specify this)
- the categories of recipient to which the personal data are to be disclosed
- information whether the personal data are to be transferred to a third country (which may be the case, for example, when IT services are used that have their servers outside the EU, or during international collaboration), and
- a description of technical and organisational protective measures.

4.13 Documentation

The person responsible for processing of personal data is to document how the processing is to be carried out. This means that it must be ensured, before the processing starts, that sufficient protective measures are in place, that the security is sufficient, that contracts have been entered into with personal data processors (where relevant), and that all who are involved in the processing carry it out in a correct and legal manner. It must be possible to demonstrate this, and it is therefore important that detailed documentation is kept. If it has been established that an impact assessment as described in Section 4.14 is not necessary, this must be made clear by the documentation.

4.14 Impact assessment

If it is assessed that processing of personal data is likely to result in a high risk for the rights and freedoms of data subjects, an impact assessment must be carried out before the processing starts. This may be relevant, for example, during the processing of personal data that involves large amounts of personal data, or during particularly risk-filled processing in which sensitive personal data are present. The person responsible for the planned processing is also responsible for ensuring that an impact assessment is carried out. The assessment is to be documented in writing, and is to take place in collaboration with the data protection officer. If it is unclear whether the planned treatment is “likely to result in a high risk”, the data protection officer should be consulted.

4.15 Personal data processor

In cases in which an actor (natural or legal person) outside of LiU processes personal data on behalf of LiU, this actor is known as a "personal data processor". A personal data processor must be able to provide sufficient guarantees that the processing satisfies the legal requirements of the Data Protection Regulation, and it must be established before a processor is commissioned to act for LiU that the rights of the data subjects are protected.

The personal data processor and personnel employed by the processor may only process personal data as specified by instructions from LiU. A written contract of personal data processing must always be drawn up, which must state, among other things, instructions given by LiU and the requirements on security. Such contracts must be officially registered at LiU and must be kept in an organised manner, such that they can be produced when necessary. LiU has templates to be used when drawing up contracts to be used for personal data processors. The data protection officer may be consulted when entering into such contracts.

A written contract for a personal data processor must also be drawn up in cases in which LiU processes personal data on behalf of another party. In such cases, LiU is itself a personal data processor. Such contracts governing personal data processing in which LiU is personal data processor must be registered with the data protection officer.

In certain situations it may be difficult to determine who is the controller of personal data and who is processor. The way in which responsibility is assigned is determined by the actual circumstances in each particular case, and depends on the degree to which each party determines the nature of the processing. The responsibility for the processing of personal data may in certain cases be determined by legislation, case-law or a decision. When it is not possible to determine which party determines to a greater degree how and why processing is carried out, which may be the case in, for example, research collaboration, it may be the case that the parties are joint controllers of personal data. In such cases, a contract of personal data processor is not required.

4.16 Personal identity numbers

Personal identity numbers and co-ordination numbers may be processed without consent only when it is clearly justified by consideration of the purpose of the processing (such as the keeping of medical records within health and medical care), the importance of reliable identification (such as concerning the payment of the correct salary to the correct individual in a salary payment system or the

registration of the correct study results for the correct individual in the Ladok student registry), or any other justifiable reason.

Note that personal identity numbers are to be used in a restrictive manner, in particular with respect to data that are published. Personal identity numbers may not, for example, be specified in lists of exam results or course-participant lists that are posted on the noticeboard of a department or on the website (if such has been created) of the programmes. It is recommended that name and year of birth are used in such cases. Personal identity numbers must never be published on the internet.

4.17 Social media and the internet

The Higher Education Act places on LiU an obligation not only to conduct teaching and research, but also to collaborate with the surrounding world and provide information about its operations. It is, therefore, permitted to present ongoing research, etc., on the university website or by activity in social media. The fundamental preconditions required for the processing of personal data must always be satisfied in order for such publication to be acceptable. From this point of view, the LiU website and the university's activity in social media do not differ. When, for example, publishing general photographs from an event, consent is to be obtained, if possible, from individuals who can be identified. Photographs of casual socialising at events may be published, if it has been made clear in advance that such photographs will be taken and published. No sensitive or offensive data may be published.

4.18 Email

Nearly all email messages contain personal data. The email address itself is generally personal data, and the text in the body of the email message may contain personal data. Processing of processing of personal data by email is not exempted from the Data Protection Regulation, and is subject to its requirements.

When email is handled, there is always a risk that others than the intended recipient obtain access to it. Email that contains sensitive personal data must, in nearly all cases, be handled with special security measures, such as encryption. The LiU guidelines for information security give further details of how email is to be handled. Note also that special conditions must normally be met before the data may be sent to countries outside the EU/EEA *(see Section 4.22)*.

4.19 Personal data and the principle of public access to official documents

The principle of public access to official documents and the right of access to official documents are regulated in legislation. This legislation will continue to be in force. Data that are handled at LiU may be subject to a request for them to be disclosed as public documents. One condition that must be satisfied before the data may be extracted from a filing system or equivalent is, however, that the handling satisfies the requirements of permitted handling, and that it takes place in accordance with the purpose specified. If an examination concludes that the handling is not permitted and that a public document exists, an assessment is to be made whether the data are subject to confidentiality or not, before they may be disclosed.

It is normally necessary to have legal grounds before personal data are disclosed by direct access, independently of the provisions of the principle of public access. There may also be limitations to the circumstances in which data may be disclosed electronically by any other method than direct access. Data from the Ladok student registry, for example, may be disclosed in a form that allows automated processing only to certain, specified recipients.

4.20 Storage of personal data

Personal data must be stored in a secure manner as specified in the LiU guidelines for information security. The guidelines also specify the conditions that must be satisfied before cloud-based services may be used for the processing of personal data.

4.21 Security of working methods

The number of people who have access to personal data during the processing of the data must, in general, be kept to a minimum. A person who does not need the personal data in order to carry out his or her duties should not have access to them.

The protective measures and security measures that must be taken depend on the nature of the personal data to be processed, their degree of sensitivity, whether a large quantity of personal data is to be processed, etc. The LiU guidelines for information security specify which security measures are to be taken for various categories of personal data. Examples of protective measures and security measures are given below.

Pseudonymisation. Pseudonymised data are such data that are not coupled directly to an individual during the processing: a separate key is required to be able to couple the individual to the data. The data are still formally considered to be

personal data, but the processing in this case takes place with greater security. Personal data that are processed during research are in general pseudonymised or protected in an equivalent manner, if the purpose of the processing can be achieved when this is done.

Encryption and coding. Encryption or the coding of data is one way to keep any damage that occurs in the event of data leakage to a minimum, and these methods constitute good technical protection.

Anonymisation. If it is no longer possible for LiU or any other external actor to directly or indirectly link the data to an individual, the data are said to have been anonymised, and are from a formal point of view no longer personal data. The data are no longer subject to the provisions of the Data Protection Regulation. Anonymised data are to be used in all cases in which it is possible to do so.

Control of access privileges. Establishing and documenting regulations for who is to have access to the data that have been collected is an administrative measure that should be used. Regulations about who is permitted to do what with the data are included in this control. This involves such matters as who may read, search within or modify that data, and in which parts of it.

Logging and follow up. It is possible to ensure that no unauthorised persons gain access to the data by keeping a log of the people who access the personal data and taking action when required. Keeping a log and the associated follow up have a preventive effect against unauthorised access.

Physical isolation of servers, backup copies, etc. The Regulation does not require that data be covered by technical protection to prevent their loss in the event of various types of computer incident. This may, however, be extremely important for an individual researcher. It is an absolute minimum that the data are stored in such a manner that backup copies are kept.

Selective disposal and erasure. Personal data that are longer required for processing are to be erased. Comply with decisions concerning selective disposal, and consult the archivist if necessary.

4.22 Transfer of personal data to a third country

The transfer of personal data to a third country, i.e. countries outside the EU/EES, is permitted only with the consent of the data subject. If this consent has not been given, special requirements are posed in order for a transfer to be permitted. Note that the use of certain cloud-based services or other IT services from global

suppliers to store or adapt personal data may be considered to be transfer to a third country.

The possibility of transfer of personal data as described below must always be examined in each individual case, and if necessary in consultation with the data protection officer.

Transfer to a third country may be permitted if:

- The EU Commission has concluded that the country has an adequate level of protection for personal data (examples are Switzerland, Argentina, New Zealand, etc.).
- The personal data are transferred with the support of a contract that contains standard contractual clauses laid down by the EU Commission[9].
- The transfer is based on binding corporate rules that have been approved by the EU Commission or a regulatory authority.
- The supervisory authority has passed down special permission based on contractual clauses between LiU and the recipient of the data.
- The transfer is necessary in certain individual cases, for example for the performance of a contract at the request of the data subject or to defend legal claims.
- The recipient is located in the US and is connected to Privacy Shield.
- The data subject has consented to the transfer, after having been informed of the risks associated with it.

Further exceptions have been laid down in the Regulation that may apply in certain cases. Contact the data protection officer for advice.

4.23 Selective disposal of personal data

Personal data may be processed only for as long as is necessary to satisfy the purpose for which they were collected. As soon as the personal data are no longer required for their purpose, they must undergo selective disposal. If, however, the personal data are included in an official document, Swedish legislation relating to public access to official documents has priority. This means that selective disposal regulations that specify the circumstances for selective disposal and archiving have

[9] 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC
2001/497/EC: Commission Decision of 27 December 2004 amending the decision of standard contractual clauses for the transfer of personal data to third countries
2010/87/EU: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

higher priority than the Regulation. If other legislation specifies that the processing is to continue, this also has higher priority that the Regulation. Consult the archivist in the event of doubt.

4.24 Archiving

LiU is a government agency and thus responsible for keeping archives. Keeping archives consists of preserving information that is constituted by official documents. These documents in many cases contain personal data.

Personal data are not to be preserved for longer than is necessary with consideration of the purpose of the processing. This legal provision, however, does not prevent a government agency archiving and preserving official documents, nor does it prevent the university's archived material subsequently being managed by an official archive authority. The legal basis is considered to be the performance of a task carried out in the public interest.

In addition to the requirements for preservation set out by the Archives Act, it is also necessary to preserve information in order to satisfy LiU's requirement of being able to follow up its operations through concluded and archived cases and projects. If questions arise about which documents are to be archived and how this is to be done, contact the archivist.

4.25 Notification of personal data breaches

A personal data breach is a security incident that may involve a data subject losing control of the information about him or her, or his or her rights being compromised. Examples of detriment that may arise following a personal data breach are a loss of confidentiality or breach of professional confidentiality, identity theft, fraud, spread of damaging rumours and financial loss. A personal data breach has occurred when, for example, information about one or several data subjects has been destroyed or otherwise lost, or fallen into unauthorised hands. A breach may also have occurred when:

- an unauthorised party has gained access to the personal data, such as may occur when, for example, someone has sent personal data to recipients who are not intended to receive the information
- digital media, such as computers, mobile phones and USB sticks, that contain personal data have been lost or stolen
- someone has modified personal data without permission, or
- the personal data are not available for the person who requires them, and this leads to negative consequences for the data subjects.

Independently of whether the incident is the result of intention or accident, it is considered that a personal data breach has occurred.

Certain personal data breaches are to be reported to the supervisory authority. This must take place within 72 hours of the breach being discovered. A person who discovers that a personal data breach has taken place must immediately notify the data protection officer. The data protection officer will assess whether it is necessary to report the incident to the supervisory authority, and will determine whether further measures must be taken to minimise the negative effects. The data protection officer is responsible for the further management of notified personal data breaches at LiU. Personal data breaches that occur at a personal data processor are also to be reported to the data protection officer.

4.26 Further details of liability and fines

The person within LiU who is responsible for a processing of personal data operation is the one who primarily is responsible for ensuring that the data are correctly processed. The supervisory authority may decide that a controller of personal data that violates the provisions of the Data Protection Regulation is to pay an administrative fine. The magnitude of the fine depends on which legal provision the violation relates to, and on the circumstances of the particular case. The factors that determine the magnitude include the seriousness of the violation, the magnitude of the damage that has been caused, whether sensitive personal data are involved, and whether the violation has been intentional. The maximum fine that LiU can be required to pay is SEK 10 million.

The supervisory authority may also issue warnings and reprimands, if a processing of personal data operation violates or is expected to violate the legal provisions. In addition, LiU may be obliged to, for example, cease processing of a certain type.

LiU may also become liable to compensate the data subject for damage and infringement of personal privacy that processing of personal data contrary to the Regulation has caused.

5 Personal data within administration, etc.

5.1 Introduction

Several different types of processing of personal data take place within the administrative systems of the university, all of which are subject to the provisions of the Data Protection Regulation. All processing of personal data must have an unambiguous and approved purpose and the person whose data are processed has the right to information about the processing. It is not permitted to collect more data than necessary, nor is it permitted to retain data longer than necessary. *Section 4 contains for more information about the fundamental principles for the processing of personal data.*

5.2 Legal bases

Each processing of personal data that is undertaken must have a legal basis. For the processing of personal data carried out during personnel management, the principle basis is that the processing is necessary for compliance with a legal obligation or that it constitutes part of the exercise of official authority carried out by LiU. These two legal bases cover the majority of the administrative functions at the university, and thus do not entail any direct changes in the practical work of the administration.

The processing of personal data is also in many cases subject to Swedish legislation that the university must continue to follow when carrying out processing of personal data, such as the Accounting Act[10], the Archives Act, the Working Hours Act[11], the Employment Protection Act[12], the Work Environment Act[13], The Discrimination Act[14], Employment (Co-Determination in the Workplace) Act[15], the Parental Leave Act[16], the Annual Leave Act[17], the Act on Sickness Payments[18], etc.

[10] Accounting Act (1999:1078)
[11] Working Hours Act (1982:673)
[12] Employment Protection Act (1982:80)
[13] Work Environment Act (1977:1160)
[14] Discrimination Act (2008:567)
[15] Employment (Co-Determination in the Workplace) Act (1976:580)
[16] Parental Leave Act (1995:584)
[17] Annual Leave Act (1977:480)
[18] Act on Sickness Payments (1991:1047)

5.3 Types of personal data and their processing

The types of personal data that are collected in an administrative context are principally name, address, personal identity number, tax and bank information. The first three types are to make it possible to ensure correct identification of the employee, and the two latter types are to make it possible to pay salary and remuneration with the correct tax deduction. The personal identity number is data that must be managed with care, and only if it is necessary to be able to reliably identify a person (which is normally the case in the LiU administrative systems). It is possible in certain systems, such as the personnel management system, for the individual employee to record further personal data voluntarily. The legal basis of this processing of personal data is consent, since the data subject has disclosed information voluntarily and can erase the data at any time.

When health data are processed, this takes place with the support of the Act on Sickness Payments, with the purpose that the employee is to receive the correct remuneration. These data must subsequently be subject to selective disposal.

The processing of personal data may take place also in, for example, application documents, a contract of employment, information about termination of service, various forms of university decision, salary information, annual statements of salary and tax, receipts, statements relating to sickness, etc. The legal basis for processing of this nature is that it is necessary for the performance of a contract to which the data subject is party.

Accounting systems collect personal data from individuals, such as guest lecturers who are to receive a fee, and from various suppliers of goods and services. These data constitute tax and banking data, and other data that may be required to ensure correct payments. Also in these cases is the legal basis the performance of a contract.

5.4 General administrative filing systems

In the central units of the university and in all faculties and departments (or their equivalent), diverse general administrative filing systems are in use in which personal data of minor significance are processed. Examples of such filing systems are: telephone lists and catalogues of the organisations and personnel in the university, participants in decisions and various bodies, distribution lists and similar for employees and students or other people who have expressed a wish to receive certain material such as magazines, minutes of meetings, theses, etc., and lists of group members, course participants, etc., for students.

Personal data related to name, work address, work telephone number and work email address may be published on the internet. Publishing photographs on the website that show identifiable natural persons, however, generally requires the consent of the individual. Personal identity numbers should not be included in these contexts.

5.5 Personnel management filing systems

The computer-based personnel management at LiU consists of the salary payment system, and support systems for the management of travel expenses claims, employment cases, salary negotiation, etc. The system is used at the university both centrally and locally to calculate and pay salaries and other contractually agreed benefits, to calculate and pay PAYE tax, and to send reports to the Swedish Tax Agency, the National Government Employee Pensions Board (SPV), etc. All of these require individual or statistical data concerning the university personnel. In addition, the system is used to derive statistics that serve as background information for work with the budget, salary negotiations, etc.

When a person enters employment (or on an equivalent occasion) the person being employed is to be informed that this processing of personal data will take place, the extent of the processing, and the rights of the data subject to information.

For those already employed at the university, corresponding information is to be continuously provided. This may take place in correlation with salary statements or equivalent documents, through information in the personnel magazine, on the website, or in another manner that is certain to reach all employees.

5.6 University records

The university records, such as LiU-Dok, constitute in themselves a filing system that contains personal data and must be managed on the basis of the provisions of the Data Protection Regulation and other specified regulations, including the Public Access to Information and Secrecy Act. Contact the Archives and Records Management Office for information about the university records.

6 Personal data within education

6.1 Personal data within education

Personal data must be processed in order to be able to carry out education. It is necessary to know the identities of the students being taught and to be able to record and report the progress the students make in their education. Just as it is in all other areas, the processing of personal data in education is subject to the provisions of the Regulation.

In order to be permitted to collect and process personal data, a legal basis and an expressed purpose for the processing must exist. The purpose must be specific, which means that LiU must be able to specify why the processing is necessary, in order to be permitted to carry it out. The basic principle is that the data subject must be able to predict what is going to happen with the data that are processed. The data collected must be adequate and relevant for the purpose for which they have been collected, and they may not be more extensive than necessary. It is also important that the data are correct and, where relevant, up-to-date. Erroneous data shall be rectified or erased. *Section 4 contains more information about the fundamental principles for the processing of personal data.*

The principal rule is that it is not permitted to store or in any other way process personal data for a longer period than necessary. The data must after this be erased or anonymised. There may be other considerations relating to retaining the data, examples of this are the Archives Act, the Public Access to Information and Secrecy Act, and the "Ladok Ordinance", etc. [19]

6.2 Legal bases

The starting point is that most cases of the processing of personal data in education are carried out with one of the three following legal bases: the performance of a task carried out in the public interest, the exercise of official authority, and compliance with a legal obligation.

Obtaining consent for the processing of personal data from the data subject constitutes an alternative legal basis. In cases in which the data subject is in a position of dependence to the controller of personal data, however, the legal basis of consent cannot be used. This is the case in education. The processing of the

[19] Ordinance (1993:1153) concerning the Reporting of Higher Education Studies etc. at universities and university colleges

personal data of students, therefore, may be based on consent only in exceptional circumstances. The fact that the education is undertaken voluntarily does not affect this assessment. Consent can be used as a legal basis only if no negative consequences, of any form, arise as a result of consent being withheld.

Public interest. "Carried out in the public interest" is a valid legal basis for the processing of personal data. In order for the legal basis of public interest to be applicable, this must be expressed in Swedish legislation, either through an act of parliament, an ordinance, regulations issued by a governmental agency, or collective agreement. Furthermore, it must be necessary to process the personal data in order to achieve the interests of the public and in order for it to be possible to use this as legal basis of the processing.

Exercise of official authority. If an action within the framework of the exercise of official authority at the university requires that personal data be processed, this is to be taken as the legal basis of the processing. Examples of this are activities that the university carries out that are specified in the Higher Education Ordinance, such as conducting examinations. It is important, however, to remember that the processing of personal data must have a clear connection to the exercise of official authority. If it is possible to carry out the activity without processing personal data, this must be done.

Legal obligation. In order for compliance with a legal obligation to be used as the legal basis for the processing of personal data, it is necessary that the obligation be established in Swedish legislation, including collective agreements and decisions from the government and government agencies. The difference in this case when compared to the two legal bases discussed above is that the legal obligation must be sufficiently clear that the individual can understand the type of processing that will be carried out with the support of the legal obligation. An example of such a legal obligation is the Ordinance concerning the Reporting of Higher Education Studies etc. at universities and university colleges (also known as the "Ladok Ordinance").

6.3 The Ladok student registry

The Ladok student registry is used at LiU with the legal support of the Ladok Ordinance. This ordinance stipulates, among other things, that every institution of higher education is to provide data about those who apply for education at the institution and whether they are admitted to the education. It must also maintain a register of students and specify individual data in this for every student. The register may be maintained with the aid of automatic computer processing.

For LiU, the rules about the register of students are most relevant. The ordinance makes it clear that the purpose of the register is to ensure that data about applicants

to education, studies carried out, grades awarded for education, and degrees awarded are preserved. Furthermore, the register is to form the basis of follow-up and evaluation, for administration within the university, for statistical purposes, to make decisions about the distribution of resources, etc. It is also there specified which data may be collected with the support of the ordinance.

The use of the Ladok student registry, thus, is based on regulations in a particular ordinance and does not therefore require any other legal basis, as long as the processing is carried out in accordance with the Ladok Ordinance. In this case, consent from the individual student is not required.

Note that if data are extracted from the Ladok student registry and subsequently supplemented with data from another source, it is possible that a new register (which in the GDPR terminology is known as a “filing system”) has been created that must be examined whether it has a legal basis. A purpose for the new filing system must be defined. It is possible that the consent of the data subject is required in this case.

As the definition of the purpose of the register makes clear, the Ladok student registry system can be used for administrative tasks across a relatively broad framework within the university, not only centrally, but also in faculties, departments and other units. Data from Ladok, thus, can be used to construct course lists, various types of distribution list, summaries of courses and groups, etc., without it being considered that a new processing operation has arisen. Data from Ladok are also used as background information for the assignment of email addresses and other access privileges, such as Lisam and the student portal. Such data are also used to create an account for borrowing from the University Library, and in the issuing of keycards, etc.

The Ladok Ordinance stipulates that as soon as an application for higher education is made, information about processing must be given to the applicant. This information is to contain a statement that the legal provisions governing the register are laid down in the ordinance. It is to have the same extent as the information that the Data Protection Regulation specifies should be given.

Students who have previously been admitted are to be given the above information continuously – appropriate occasions are when registering for examinations, on the student portal and in the student catalogue.

Note that personal identity numbers are to be used in a restrictive manner, in particular with respect to data that are published. Personal identity numbers, for example, may not be specified on result lists from examinations that are posted on departmental notice boards. Only name and year of birth should be used in such

contexts. *More information about personal identity numbers is given above, Section 4.16.*

The Ladok Ordinance specifies the situations in which data may be distributed on media for automated processing. The data may not be distributed in such a manner to anyone except in the circumstances listed there.

6.4 Other study administration

Material that is produced for the administration of ongoing teaching or for an examination, and that contains personal data, constitutes working material. Such material may be produced as part of the exercise of official authority by the university. When the graded activities of a student in a particular course are complete, the grades are to be recorded in Ladok, and other material either registered or discarded. Material of the study guidance counsellor that contains personal data is generally to be registered or retained in another, well-organised, manner.

6.5 Processing of personal data carried out by students

LiU is controller of personal data also for processing of personal data carried out by students, provided that the processing is part of the education or a component of it subject to examination. The student is obliged to follow the components that are specified in the syllabus for the programme and course, and undergoes examination by the university. Even if it is possible for a student to select a subject, the choice must be approved by the university and examiner. A corresponding argument can be made for doctoral students, with the difference that the faculty boards are responsible for research education. Each doctoral student has a supervisor and an individual study plan, both of which are always associated with the university. In this way, LiU has a decisive influence over the choice of subject and whether the processing of personal data is to be carried out as part of the work. Thus it can be argued that not only undergraduate students but also doctoral students have such a relationship with the university that they are, in this context, equivalent to employees, and cannot be regarded as independent, formal controllers of personal data. In cases in which degree projects are financed by external actors, the question may arise whether the financing actor is controller of personal data. For this to be the case, however, the financing actor must have significant influence over the purpose *(see Section 4.15).*

When a student carries out processing of personal data in the circumstances described above, the same regulations apply as for other processing by LiU. Also in cases in which data are collected as background material to the final work without being a part of it, the processing is subject to the Regulations. The processing must

rest on a legal basis; the principles must be followed (the processing must be legal, open, fair and serve a definite purpose, while the data processed must be kept to a minimum); the data subjects must be informed; and the processing is to be included in the university list of processing operations *(see Section 4)*. The person who has the role of supervisor or examiner is responsible for ensuring that students manage personal data in the correct manner. In the event of any uncertainty, the data protection officer should be contacted.

It may be difficult to define any other legal basis for processing carried out during the students' work than consent, which makes it particularly important that the students understand the importance of providing correct information to the data subjects, collecting consent forms, and preserving them. It should be considered whether it is necessary that the work contain personal data or whether anonymous data can be used instead. If personal data are not used, the requirements of the Data Protection Regulation do not apply.

There is no limit to the data that a student may collect using consent as the legal basis of the processing, but the data may not be more extensive than necessary and they must be collected for a specific, expressed purpose. Collection, management and storage must take place in a secure manner that corresponds to the sensitivity of the data, and an impact assessment must be carried out in exactly the same way as for other processing operations, if it is probable that the processing can result in a high risk for the register rights and freedoms of the data subjects. The data protection officer is to be contacted if there is any uncertainty about the circumstances in which an impact assessment is necessary, and for help with the assessment itself in cases in which it is.

7 Personal data used in research

7.1 General information

When personal data are processed for research purposes, the same conditions in general apply to the processing as for all other processing of personal data. In addition to the Data Protection Regulation, supplementary Swedish legislation applies, and it is necessary that researchers are familiar with this. It includes the Act Concerning the Ethical Review of Research Involving Humans[20], the Public Access to Information and Secrecy Act, and the Archives Act. The Data Protection Act[21] supplements the Regulation with Swedish legal provisions, and the Research Data Inquiry[22] can provide a certain amount of guidance. Note that the Data Protection Regulation does not apply to deceased persons, in contrast to the Act Concerning the Ethical Review of Research Involving Humans.

Research carried out in another country than Sweden is to be subject to ethical vetting in that country, independently of the location of the responsible research body, but the Data Protection Regulation and the supplementary regulations apply to all research carried out at Linköping University – independently of where the research takes place.

The term "research" is not defined either in the Data Protection Regulation or the Data Protection Act. These documents instead use concepts such as "scientific or historical research purposes". The term "research" is defined in the Act Concerning the Ethical Review of Research Involving Humans as *scientifically experimental or theoretical work intended to result in new knowledge and development outcomes on a scientific basis, excluding work that is performed within the framework of higher education at the basic or advanced level."*

The term "personal data for research purposes" is used to denote all work that is or is considered to be a part of the research process, including preparative and concluding activities, documentation for use in research, and the archiving of research material.

A person who intends to process personal data in research must ensure that the processing has a legal basis *(see Section 4.4)*, that the principles of the Data

[20] Act (2003:460) Concerning the Ethical Review of Research Involving Humans
[21] Act (2018: 218) with additional provisions to the EU General Data Protection Regulation
[22] SOU 2017:50 Personal Data Processing for Research Purposes

Protection Regulation are followed *(see Section 4.3)*, and that the personal data are processed in a secure manner *(see Section 4.21)*. The definition of what is considered "a secure manner" depends on the nature, extent and context of the personal data. A separate assessment must be made in each situation. In the event of doubt concerning this assessment, the data protection officer should be contacted.

It is important to remember that personal data are not only information by which it is possible to identify a person directly: the regulations apply also to pseudonymised and coded information as long as the code key exists. This is the case even if the researcher has access only to anonymised data, while another actor (such as, for example, another government agency or caregiver from whom the data have been obtained) can identify the individuals through supplementary information or a process of elimination.

Sound, such as recorded interviews, and images also constitute personal data as long as the quality of the sound makes it possible to directly or indirectly identify an individual using reasonable technical aids. If it is possible using reasonable means to achieve the same quality and results from the research by working without collecting personal data or by using completely anonymous data, this should be done.

The duration for which the personal data must be retained should be determined when they are collected. The data are to be retained as long as it is necessary to ensure the quality of the research, and no longer than this. If possible, the components of the personal data that must be stored, i.e. archived, and which components of the data can be made anonymous or erased, in order to make it possible to draw conclusions from the research, should also be determined when they are collected.

7.2 Conditions that justify the processing of personal data

7.2.1 In the public interest

Conducting research is considered to be a task in the public interest, with which LiU has been charged in its role of institution of higher education for which the government is accountable authority, as specified by the Higher Education Act. It is thus permitted to process personal data for research purposes. This is valid provided that the processing of personal data is necessary for the purpose that is specified for the specific research activity, and that it is not possible to achieve results of the same quality and reliability without the use of personal data. When making this assessment of necessity and reasonableness, it must be considered whether reasonable alternatives to using personal data are available that enable

research results of the same quality to be obtained. If this is the case, processing of personal data is not permitted.

7.2.2 Consent

One legal basis that can always be used for research, and that is a natural choice for reasons of research ethics, is that the data subject has consented to the processing. In order for consent to be a valid legal basis, it must be a case of freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent must be unambiguously directed at the processing of personal data, and must not be mixed with other explanations, or decisions that the individual takes.

The requirement of consent may be problematic in cases in which the power relationship between the data subject and the controller of personal data is unequal, due to a position of dependence or similar. Such a situation may arise in the relationship between student and institution of higher education, or between employee and employer. In order for an expression of consent to be valid, an unambiguous description of the data that are to be collected and the purpose for which they are to be used must be given. The person who intends to process the personal data is responsible for the formulation of the description of the purpose *(see Section 4.5)*.

7.2.3 Exception from the limitation of purpose

For research, there is an exception with respect to the purpose that is to be specified when obtaining consent. Since it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection, a data subject may provide consent for the processing of personal data in certain areas of scientific research. A condition for this, however, is that accepted ethical standards for scientific research are followed, and that appropriate technical and organisational protective measures are taken. This means in practice that research can be carried out using material that has been previously collected, on the condition that the new research is compatible with the purpose for which the material has previously been collected.

7.2.4 Documentation and withdrawal of consent

Consent given is to be documented in an appropriate manner (in written or digital form) and it must be possible to produce it when required. The documentation is also to make it clear that the consent has been given in the correct manner, including such aspects as, for example, that it has been preceded by unambiguous information to the data subject.

Consent can be withdrawn by the data subject at any time without any need of justification, and it is then no longer permitted to continue to process the personal data of the data subject using consent as the legal basis. Situations may arise in which the processing of personal data is initially based on consent as its legal basis, but another legal basis for the processing becomes relevant as the work progresses. This may be the case, for example, when research results are published or archived. The archiving is undertaken in order to comply with a legal obligation, and the publication of research results is considered to be a task carried out in the public interest.

The right to withdraw consent that has been given and the consequences of such a withdrawal place high demands on a person who is using personal data in research. This person must have efficient tools to be able to identify personal data that have been provided using consent as the legal basis, and to be able to erase the personal data when necessary.

7.2.5 Consent as a measure to enhance privacy

In cases in which the statement that the research constitutes a task carried out in the public interest is used as legal basis, there may be reasons of research ethics to request that the data subject provide consent to the processing of personal data. The information provided to the data subject is to be transparent and unambiguous, particularly when describing the consequences that withdrawal of consent once given may have.

7.3 Processing sensitive personal data

In general, the processing of sensitive personal data is prohibited unless there is a legally justified exemption from this prohibition. The term “sensitive personal data” is used to denote personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, a person’s sex life or sexual orientation, genetic data, and biometric data for the purpose of uniquely identifying a person. Personal data concerning criminal convictions should be considered equivalent to sensitive personal data.

Several exemptions from the prohibition against processing sensitive personal data have been defined. One of these is that the data subject has expressed consent to the processing. For this exemption, the information given above applies, with the extra provision that the consent must be expressed. Furthermore, approval must have been obtained as specified in the Act Concerning the Ethical Review of Research Involving Humans.

Further exemptions from the prohibition have been established, such as that the processing is necessary for, among other things, scientific purposes or statistical

purposes (which is the legal basis that will in most cases be the natural one to use for research at LiU), or that the processing is necessary for an important public interest. The processing of personal data must always be of such a nature that it is proportional to the purpose for which it is carried out.

When sensitive personal data are to be processed, special protective measures of technical and/or organisational character are to be applied in order to ensure increased protection of privacy, and the principle of data minimisation, in particular, is to be used *(see Section 4.3)*. Pseudonymisation of personal data should be a compulsory measure, on the condition that the purpose of the research can be achieved with pseudonymised data. *More information about protective measures is given above, Section 4.21.*

Ethical vetting constitutes an expressed appropriate protective measure (and this is true also for criminal convictions) and should thus be compulsory for all processing of sensitive personal data in research. Approval from an ethical review board may contain conditions that also can be considered to constitute appropriate protective measures.

The Regulation uses the concept of "academic expression", and concludes that the processing of personal data for this purpose is not subject to certain legal provisions. "Academic expression" does not include research and can never lead to the regulations for the processing of personal data not being applicable in research.

7.4 The rights of the data subject and the limitation of such in research

A data subject has the right, among others, to obtain information about the processing of personal data, the right to be informed of the personal data that are processed, and to obtain an transcript of the data relating to him or her that are processed, the right to have erroneous data rectified, and the right to have person data erased (if there is no legal basis for retaining them) *(see Section 4.9)*. These rights are subject to certain restrictions in research activities:

- The right to erasure does not apply if continued processing of personal data is necessary for, among other things, the research purpose.
- The right to access (a transcript of the data) is limited in cases in which LiU can demonstrate that it is not possible to identify the data subject. This may be the case, for example, when solely pseudonymised or coded personal data are processed. In addition, data that may not be disclosed to the data subject according to legislation, such as the Public Access to Information and Secrecy Act, are not to be disclosed to the data subject.

- The right to rectification does not apply to such personal data as have already been processed for research purposes if they are subsequently preserved solely in order to document research that has been carried out. Otherwise the right to rectification applies without exception.
- The right to limit the processing does not apply when the data subject contests the correctness of the data during the period of investigation that is required to determine whether the personal data are correct, if this leads to an inability to carry out the research or to the research being delayed or made more difficult to a significant degree. The same provision applies when the data subject objects to the processing, while waiting for it to be determined whether LiU's legitimate reason has greater weight than the legitimate reason of the data subject.

7.5 The processing of personal data in collaboration with a third party

When LiU commissions another party to process personal data on its behalf, or when LiU processes personal data on behalf of another party (as part of, for example, commissioned research or other collaborative research), what is known as a situation with a "personal data processor" arises. In such situations, a written contract (personal data processor contract) must be drawn up that specifies, among other things, the purpose of the processing and instructions for how the processing of personal data is to be carried out. *More information about personal data processors is available in Section 4.15.*
In the event of any doubt, the data protection officer should be contacted.

Note that there is a difference between a situation in which the disclosure of personal data is requested with the support of the Public Access to Information and Secrecy Act and the case in which a personal data processor has been commissioned.

7.6 Notification of processing of personal data

LiU maintains a list of the processing of personal data operations that take place in research in which the personal data of research subjects are processed. When processing of personal data commences during research, the university list over the processing of personal data in research is to be notified. A special procedure has been specified for this *(see Section 4.12)*. When the processing has been terminated, it is to be removed from the list.