AALBORG UNIVERSITET

Guide to the General Data Protection Regulation in relation to research

Table of contents

1. BACKGROUND AND PURPOSE 4

2. DEFINITIONS AND CONCEPTS 4

3. THE BASIC PRINCIPLES OF THE GENERAL DATA PROTECTION REGULATION (GDPR) 6

3.1 Good data processing practice 6

3.2 Purpose 7

3.3 Data minimisation 7

3.4 Accuracy 7

3.5 Storage limitation 7

3.6 Processing security 7

3.7 Documentation 8

4. THE RIGHTS OF THE DATA SUBJECTS 8

4.1 Obligation of providing information 8
4.1.1 Obligation to provide information when the data are collected from the data subject 8
4.1.2 Obligation to provide information when the data are not collected from the data subject 8
4.1.2.1 Deadlines 9
4.1.2.2 Exceptions to the obligation of providing information 9

4.2 Right of access 9

4.3. Right to rectification 9

4.4 Right to erasure 9
4.4.1 Background 9
4.4.2 Exceptions 9
4.4.3 Duty of notification 10

4.5 Right to restriction of processing 10

4.6 Right to object 10

5. AAU'S REGISTRATION PROCEDURE 10

5.1 The aim of the registration procedure 10
5.1.1 Record 10
5.1.2 Transparency and documentation 10

5.2 What must be registered? 11

5.3 Who can and must register projects at Grants & Contracts? 11
5.3.1 Registration procedure 12
5.3.2 Regarding storage of personal data 12

6. DATA PROCESSORS 12

6.1 Data processing agreement 13
6.1.1 Standard data processing agreements 13
6.1.2 Procedure for data processing agreements 13

7. SHARING 13

7.1 What is sharing? 13

7.2 Rules on sharing 13
7.2.1 Different rules apply depending on for what purpose the personal data are collected 14

7.4 Reusing research data that include personal data 14
7.4.1 Conditions for reusing personal data 14

7.5 Data subjects' rights in the event of sharing 14
7.5.1 Request for erasure 15
7.5.2 Receiving research data 15

7.6 The difference between data processing and sharing 15

8. AAU'S TECHNICAL SUPPORT FOR RESEARCH 15

8.1 Storage and sharing solutions 15

8.2 Future solutions and support 15

9. SECURITY INCLUDING SECURITY BREACHES AND IMPACT ASSESSMENTS 15

9.1 Data security 15

9.2 Data processing and storage 16

9.3 Control 16

9.4 Completion of the project 17

9.5 Security breaches 17
9.5.1 What is a security breach? 17
9.5.2 What to do in case of a security breach 17

9.6 Impact assessments 17

10. AMENDMENTS 17

1. Background and purpose

The purpose of this guide is to provide an introduction to the General Data Protection Regulation (GDPR) which has replaced the Act on Processing of Personal Data as of 25 May 2018. The new data protection regulations are stipulated in the GDPR adopted by the European Parliament and the Council and in the Danish Data Protection Act, which comprises supplementary provisions to the GDPR.

The general purpose of the data protection regulations is to protect individuals against personal data breaches. Aalborg University (AAU) has a responsibility and obligation to protect the personal data stored or processed by the University. This includes all personal data entrusted to AAU, such as the personal data of students, staff members, individuals whose personal data are used in research or others affiliated with AAU. Personal data are not ours to keep, we merely borrow the data for a limited period of time, and we must ensure that we store and process the data carefully. We must be careful when we provide documentation of which personal data we process, and we must make sure that no personal data are lost or leaked in our systems or processes.

Non-compliance with the GDPR may have serious consequences – not only for the individual whose personal data have been leaked but also for AAU. Our reputation, our credibility and our opportunities for cooperation are all at stake.

The GDPR applies when a company or organisation processes personal data automatically or electronically or when personal data are processed manually and the data are stored.

2. Definitions and concepts

The General Data Protection Regulation (GDPR): The 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 (General Data Protection Regulation) with subsequent amendments.

The Danish Data Protection Act: The Danish supplementary provisions to the GDPR on the protection of natural persons in connection with the processing of personal data and the free movement of such data.

The data protection regulations: The General Data Protection Regulation, the Data Protection Act and any executive orders issued in accordance with the General Data Protection Regulation and the Danish Data Protection Act, case law, as well as decisions made by the Danish Data Protection Agency.

Personal information/personal data: Any information that relates to an identified or identifiable living individual. The identification does not necessarily have to be carried out by the data controller or data processor.

Examples:

- Data from Statistics Denmark (Statistics Denmark is able to identify individuals)
- Names, emails, telephone numbers
- Health data
- Civil registration numbers

Personal data may be categorised into general, confidential and sensitive personal data.

Examples of general personal data:

- Names
- Emails and addresses
- Education and job title
- Gender and date of birth

Examples of confidential personal data:

- Unlisted address
- Grades
- Civil registration numbers

- Account number

Examples of sensitive personal data:
- Health data
- Political opinions or religious beliefs
- Trade union membership

Anonymised personal data (in accordance with the Danish Data Protection Act) Any information relating to an individual who cannot be identified.

If a researcher has replaced identifying data, such as name, civil registration number, address etc., with a code and has stored a 'key' which may be used to identify natural persons, the personal data are not anonymised in accordance with the Danish Data Protection Act.
If a researcher has received personal data from Statistics Denmark through Research Support Services (Forskerservice), these personal data are not anonymised in accordance with the Danish Data Protection Act since Statistics Denmark may be able to identify the natural persons.

Pseudonymisation: Personal data have been pseudonymised when personal data (names, civil registration numbers etc.) have been replaced by serial numbers and a document has been created in which these serial numbers are linked back to individuals.

Pseudonymised personal data may still be used to identify individuals and are thus still personal data.

Pseudonymisation is a security measure. Pseudonymisation can reduce the risk of identification in that an unauthorised person would need both the pseudonymised personal data and the 'key'(the document which links serial numbers to individuals) in order to be able to identify individuals.

Processing: Any operation performed on personal data or personal information.

'Processing' refers to registration, storage, transfer, collection, organisation, adaptation, alteration, use, sharing, dissemination, aggregation, retrieval, consultation, use, alignment, analysis, restriction, erasure, destruction, etc.

Data controller: The data controller decides how the personal data are processed and for what purpose. When AAU researchers conduct research as part of their employment at AAU, AAU is the data controller.

The data controller is always responsible for safeguarding the rights of the data subject and for complying with the GDPR.

Data subjects: The individuals whose personal data are processed as part of a research project.

Data processor: The data processor processes personal data on behalf of and on instructions from the data controller.

Examples of data processors and data processing tasks:
- Students not employed by AAU who are transcribing an interview.
- A hospital that performs scans to be used as part of a research project
- Rambøll's SurveyXact platform, which is used by a project manager for the collection of data (from questionnaires).
- Gallup, who collects data by agreement with the project manager.
- Statistics Denmark, who stores and aggregates data.
- A cloud solution.

Data processing agreement: A data processing agreement is a formal agreement made between the data controller and the data processor. The data processor agrees to comply with the data protection regulations and to process personal data on behalf of and on instructions from the data controller.

Sharing: When personal data or copies of personal data are entrusted to a third party (such as a researcher not employed at AAU), and when this third party uses the personal data for their own interests, it constitutes sharing.

Different rules apply to the sharing of research data and personal data collected for purposes other than research. Further information is available in section '7 Sharing'.

Reusing personal data: When an AAU researcher reuses sets of personal data for a new AAU research project, it constitutes reuse of personal data.

However, if the sets of personal data are reused for a research project at another university, it constitutes sharing.

Further information about the requirements for reusing personal data for a new AAU research project is available in section 7.4.1.

Project manager: The AAU researcher with the overall responsibility for the research project.

PhD students are the project managers of their own PhD projects.

AAU's registration procedure: AAU's registration procedure allows AAU researchers to register research projects that include the processing of personal data in accordance with a number of core principles of the GDPR.

Project managers with a split employment (for example a person employed by both the University Hospital and AAU) must register projects in accordance with AAU's registration procedure if the projects are carried out in an AAU context.

3. The basic principles of the General Data Protection Regulation (GDPR)

When processing personal data, including general, confidential and sensitive personal data, the basic provisions of the data protection regulations must be complied with.

3.1 Good data processing practice

All personal data processing, including storage, analysis, deletion, etc., must be lawful, fair and transparent.

The data controller is responsible for assessing whether the processing of personal data is reasonable for the data subject.

The processing of personal data is lawful when a legal basis for the processing exists and when this is based on the principles of the data protection regulations or other relevant legislation. Legal or lawful basis is a legal concept which refers to a legal reason to process personal data.

The GDPR lays down a specific legal basis for research, according to which general, sensitive and confidential personal data can be processed for scientific, statistical and
research purposes, provided that the following conditions are met:

- That the research is necessary for reasons of public interest (in general, research is conducted in the public interest, and therefore, most research projects comply with this principle).
- That the processing of personal data is necessary for achieving specific purposes.
- That technical and organisational measures are taken to ensure the protection of data.
- That measures are taken to ensure that only the necessary amount of personal data are processed.

In addition to using research purposes as the legal basis for processing, consent may also be used as the legal basis for processing general, confidential and sensitive personal data. The following conditions apply to using consent as the legal basis for processing personal data:

- Consent must be collected in accordance with the principles of the Danish Data Protection Act.
- That the project allows for consent to be withdrawn or altered.
- That the processing of personal data is necessary for achieving specific purposes.
- That technical and organisational measures are taken to ensure the protection of data.
- That measures are taken to ensure that only the required amount of personal data is processed.

Please note that if you collect consent in order to comply with other regulations or standards of good practice, you may still use research purposes as the legal basis for processing.

Thus, a project may be reported to the Danish Scientific Ethical Committee for which consent has been collected in accordance with the Committee Act while research purposes is used as the legal basis for processing personal data in accordance with the Danish Data Protection Act.

In addition to the principles of lawfulness and fairness, personal data must also be processed in a transparent manner in relation to the data subject. This implies that the person whose personal data is processed must be informed that their personal data will be processed, the purposes of the processing and the types of processing activities to be carried out. Compliance with the data controller's obligation to provide information, as described in the section '4.1 Obligation of providing information' helps ensure transparency.

The data controller is obliged to document transparency for the data subject.

3.2 Purpose

Personal data must only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes. Thus, collection of personal data without a specific purpose is illegal.

Whether a specific collection of personal data is legitimate depends on the type of research for which the collected personal data will be used. Thus, what is legitimate for one researcher may not necessarily be legitimate for another.

Personal data originally collected for other purposes than research and statistics (for example patient record data) may be reused for research and statistics, as the regulations lay down that research and statistical purposes are not incompatible with the original purpose. In concrete terms, this means that using data for research purposes is compatible with the original purpose. It is therefore possible for companies and institutions to disclose data for research purposes.

3.3 Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Thus, any processing, including collection, storage etc., may not include more than what is required for the purpose.

This rule contributes to safeguarding against unnecessary hoarding of personal data.

3.4 Accuracy

The data controller must ensure that inaccurate personal data are not processed. If inaccurate personal data are processed, these must be erased or rectified without undue delay.

Moreover, the data controller is responsible for ensuring that personal data are processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss.

3.5 Storage limitation

Personal data must be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

When it is no longer necessary for the researcher to store the personal data, the data must be erased, archived in accordance with the Archives Act or anonymised in a way that precludes the identification of individuals.

3.6 Processing security

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss.
Find further information in the section '9. Security', which includes security breaches and impact assessments.

3.7 Documentation

If you process personal data, you are obliged to ensure that the above principles are complied with, which must be documented electronically and in writing.

4. The rights of the data subjects

The data subjects, i.e. the persons participating in research projects, have a number of rights to be observed by the researcher.

4.1 Obligation of providing information

The first right of the data subjects is the right to be informed of who will be processing their data and the purpose of the processing. The objective of this right is to ensure transparency for the data subjects, so that they know what their data will be used for.

4.1.1 Obligation to provide information when the data are collected from the data subject

When data are collected directly from individuals, participating in a research project, i.e. the data subjects, the researcher is obliged to provide certain information in writing in plain language at the time when the data are collected.

4.1.1a The following information must always be provided:

- The identity and contact details of the data controller (AAU is the data controller)
- The contact details of AAU's data protection officer
- The purpose of the processing of the collected personal data
- The legal basis for processing. Further information is available in the section '3.1 Good data processing practice'.
- Potential recipients or types of recipientsof the personal data (data processors and other external people or institutions)
- Information on whether the personal data will be shared with countries outside the EU/EEA.

4.1.1b It must be considered whether the following information is relevant to the data subjects:

- The period of time the personal data are stored or alternatively the criteria applied to determine this period of time.
- Information on the right to request access, rectification, erasure, restriction of processing and the right to object to processing.
- If the processing is based on consent, then the right to withdraw consent.
- The right to submit a complaint to the Danish Data Protection Agency.
- Whether the data subject is obliged to provide certain information.
- Whether automated decision-making is carried out, including information on why and a description of the expected consequences.

If the data subject is already familiar with some of the information that must be provided and if this is documented in writing, the obligation to provide information does not apply as for the information already familiar to the data subject.

Example:

- A researcher is working on a project examining women's wellbeing in Danish prisons and in that context, the researcher will be interviewing ten female prisoners.
  The researcher must comply with the obligation to provide information with reference to each of the ten prisoners thus providing all the information stated in section 4.1.1a and considering whether the information stated in section 4.1.1b should be provided as well. The obligation of providing information must be complied with at the time when the ten participating prisoners have been found.

4.1.2 Obligation to provide information when the data are not collected from the data subject

When personal data not collected directly from the data subject are received, the obligation to provide information generally also applies. Thus, there is an obligation to provide the same information as when collecting data directly from the data subject.

Example:

- A researcher receives a dataset. The dataset consists of video recordings on which 50 test subjects each carry out a physical test. In addition, the dataset consists of different test results from each of the 50 test subjects.
  The researcher receiving this dataset must comply with the obligation to provide information towards the 50 test subjects who participated in the physical test.

4.1.2.1 Deadlines

The obligation to provide information must be complied with within a reasonable period of time, but no later than a month after the data have been received.

In case the data will be used for contacting the data subjects, the obligation to provide information must be complied with already at the time of the first communication with the data subject.

In case the data will be used for other purposes that the one the data were originally collected for, the obligation to provide information must be complied with before a new purpose is implemented.

4.1.2.2 Exceptions to the obligation of providing information

In cases where data are not collected directly from the data subject, there may be situations where the obligation to provide information may be dispensed with.

If it is not possible or if it will require a disproportionate effort, particularly with regard to processing in relation to public interests, including research and statistical purposes, the obligation to provide information may be dispensed with if the following conditions are met:

- technical and organisational measures must be taken
- the principle of data minimisation must be observed, and
- if possible, the data must be pseudonymised.

4.2 Right of access

If the personal data are processed solely for research and statistical purposes, the data subjects do not have the right to obtain confirmation of whether their data are processed. Consequently, the data subjects do not have the right of access either.

4.3. Right to rectification

If the personal data are processed solely for research and statistical purposes, data subjects do not have the right to have their data rectified.

4.4 Right to erasure

4.4.1 Background

As a general rule, data subjects have the right to have the data controller erase their personal data without undue delay, if one of the following conditions is met:

- The personal data are no longer necessary to fulfil the purposes for which they were collected or otherwise processed.
- If the legal basis for processing the personal data is consent, and the consent is withdrawn and there are no other possible legal bases.
- Personal data are processed illegally.

If the conditions for complying with a request for erasure are met, the data controller must make sure the requested personal data are erased.

4.4.2 Exceptions

If the personal data are processed for research and statistical purposes and it is significantly problematic or impossible to fulfil the intended research or statistical purpose, the data controller is exempt from having to erase the personal data.

4.4.3 Duty of notification

In cases where the data controller has received a request for erasure of personal data, the data controller must inform all the researchers to whom the data have been disclosed, unless this proves impossible or unreasonably difficult.

Data subjects have the right to be informed of to whom their personal data have been disclosed.

4.5 Right to restriction of processing

If personal data are processed solely for research and statistical purposes, data subjects do not have the right to have the processing of their data restricted.

4.6 Right to object

Data subjects can raise objections to having their personal data processed for research and statistical purposes, after which the data controller, as a general rule, may not process the data anymore.

If the data subjects' data are significant or crucial for the completion of the project, the interests of all parties must be considered and balanced. It should be considered how important the research is for public interest relative to the data subjects' interest and reasons for objecting to having their personal data processed.

5. AAU's registration procedure

As of 2015, AAU has had one joint notification on research at the Danish Data Protection Agency. The aim of the joint notification was to have researchers notify Grants & Contracts about research projects in which confidential personal data were to be processed. Grants & Contracts would subsequently process the notification and register the project on AAU's internal list in accordance with the guidelines set forth by the Danish Data Protection Agency.

With the new GDPR, the notification obligation no longer applies. Rather, it is replaced with the obligation to keep an internal record of all processing activities. Within the research area at AAU, the notification procedure is replaced with a registration procedure. Thus, researchers processing personal data are obliged to register their research projects via AAU's registration procedure.

The former notification procedure covered only confidential personal data, whereas the registration procedure covers all types of personal data, including general personal data such as names, gender, age and email addresses.

5.1 The aim of the registration procedure

The aim of the registration procedure is to provide AAU's researchers with a tool that enables them to comply with a number of central rules of the GDPR, including the obligation to keep a record, the obligation to provide information, the principle of transparency, documentation, etc. In practice, the registration procedure is essentially an electronic questionnaire guiding researchers through a number of considerations that they are obliged to take into account in connection with processing of personal data in their research. However, the registration procedure has its limitations, since compliance with the GDPR requires researchers to maintain continuous focus and attention towards complying with the rules in their daily work.

5.1.1 Record

As the data controller, AAU is obliged to keep an internal record that includes all processing of personal data. The GDPR includes a number of specific points that must be registered, including purpose, legal basis, type of data etc. As part of the administrative process, the processing activities are divided into overall groups, and the record is prepared in advance and updated regularly. This is not possible within the research area, since research projects always differ from project to project. Therefore, each research project will be registered on AAU's record individually.

5.1.2 Transparency and documentation

Two of the cornerstones in the GDPR are:

1. it must be transparent for the data subjects what will happen to and with their data, and
2. the data controller must be able to document that the processing is compliance with the GDPR.

The registration procedure contributes to creating transparency, since the individual researcher via a number of questions describes how the personal data are processed, and Grants & Contracts, AAU Innovation, ensures that the data are filed for documentation.

5.2 What must be registered?

All research projects and income-generating activities, for which AAU is the data controller, databases and registers, in which personal data are processed, including general, confidential and sensitive personal data must be registered in AAU's registration procedure.

This is a significant extension to the former Danish Act on Processing Data, which stated that only research projects processing *confidential* personal data were to be registered.

In addition, all biobanks that include or will include human material must always be registered.

Personal data include all information that identifies or can identify an individual It need not necessarily be the data controller who can identify the individual. This is why data from Statistics Denmark are considered personal data.

Examples of personal data:

- Civil registration numbers
- Health conditions
- Basic information such as gender and age
- Political opinions
- Significant social problems
- Trade union membership
- Sexual matters
- Nationality
- Names
- Email, telephone numbers or address
- Position, place of employment or salary

The list is not exhaustive.

Examples of projects requiring registration:

- A researcher collecting data by means of a questionnaire distributed via email. The questionnaire includes questions concerning the respondents' attitudes and opinions towards social media. (The project must be registered as personal data are processed, e.g. email addresses).
- A researcher using data from Research Support Services at Statistics Denmark for use in a registration project. (The project must be registered as Statistics Denmark is able to identify the individuals about whom the researcher has information).
- A researcher wants to examine the exercise habits of people with depression. In connection with recruitment of participants for the research project, inclusion and exclusion criteria are prepared. One of the inclusion criteria is the diagnosis 'depression'. (The project must be registered as health data are processed in connection with recruitment).

5.3 Who can and must register projects at Grants & Contracts?

AAU's registration procedure covers the research projects, biobanks, databases and registers for which AAU is the data controller. Projects that are set up as income-generating activities must in some cases also be registered in AAU's registration procedure. The decisive factor is whether AAU is the data controller or data processor.

Staff members with split employment can register projects in AAU's registration procedure if the projects are carried out under the auspices of AAU.

Students cannot register their master's theses and student projects in AAU's registration procedure because they are each the data controller of their own projects;

nor can visiting researchers and PhD students enrolled at but not employed by AAU
register their own projects in AAU's registration procedure, since AAU is not the data controller of their projects. They should instead contact their employer.

5.3.1 Registration procedure

During registration, researchers must state:

- Department, project title and the name of the project manager
- Purpose and legal basis
- Type of registration (research project, database, biobank, etc.)
- Type of personal data and processing
- The life cycle of the dataset
- Approximate number of individuals about whom data are processed
- Whether external persons will be processing personal data
- Where the personal data will be stored
- Date for the commencement and end of processing the personal data
- Whether the personal data are erased, archived or anonymised by the end of the processing.

Staff from Grants & Contracts, AAU Innovation will go through the registration and contact the researcher if necessary. This may be in cases where a data processing agreement must be made.

5.3.2 Regarding storage of personal data

The data protection regulations require for technical and organisational security measures to be implemented when managing and storing personal data.

To ensure that AAU comply with these rules, AAU offers a number of standard solutions for secure storage of personal data. Read more about this in section '8. AAU's technical support for research'.

If one of AAU's standard solutions are not chosen as storage solution, administrative procedures will often be prolonged, since compliance with the data protection regulations must be examined and documented for the specific storage solution.

6. Data processors

If a researcher entrusts the processing, including storage, collection etc. of personal data to an external party, the external party becomes a data processor unless the personal data are processed in the party's own interest. If external parties will be processing personal data in their own interests, the dataset must be shared in accordance with the rules on sharing. See the section '7. Sharing'.

Examples of data processors:

- A hospital that performs scans of ten individuals to be used as part of a research project
- Statistics Denmark storing and aggregating data
- Gallup collecting data by agreement with a researcher
- Rambøll collecting questionnaire data via the service SurveyXact
- Various external cloud solutions (often illegal, since it is not possible to make data processing agreements in connection with such solutions).
- A student not employed by AAU who transcribes an interview
- A visiting researcher who helps analyse data.

6.1 Data processing agreement

A data processing agreement is a formal agreement made between the data controller and the data processor. The data processor agrees to comply with the data protection regulations and to process personal data on behalf of and on instructions from the data controller.

The GDPR requires that a data processing agreement to be made with every data processor to whom data processing tasks are entrusted. It is also required to perform regular controls with the data processor.

6.1.1 Standard data processing agreements

Within the research area, there are two standard templates for data processing agreements:

- *General data processing agreement for research*
  This template is to be used when a project manager entrusts the processing (including collection, storage, analysis, etc.) of personal data to a collaboration partner or subcontractor.
- *Student data processing agreement for research*
  This template is to be used for students who will be carrying out isolated smaller data processing tasks (for instance the transcription of an interview) on behalf of a project manager. The agreement template is not to be used if the student is employed by AAU.

6.1.2 Procedure for data processing agreements

Please refer to 'Guidelines for managing data processing agreements for research'.

7. Sharing

Please note: The following description of the rules on sharing is preliminary, since the rules are based on a draft bill currently under discussion by the Danish Parliament. This guide will be updated when the rules have been adopted by the Danish Parliament and the Danish Data Protection Agency lays down guidelines.

7.1 What is sharing?

When personal data or copies of personal data are entrusted to a third party and when this third party uses the personal data in their own interests, this constitutes sharing. In this context, a third party can be a collaboration partner, a colleague from another university, a student, etc. There may also be situations where the ceding and the receiving researcher must cooperate on the dataset for the same project, but where sharing is necessary because both parties must contribute to defining the purpose and design of the project.

Please note that in case researchers change jobs and in that connection wish to bring personal data with them to their new work place, it constitutes sharing. The reason is that the individual researcher who is not the data controller; the data controller is the researcher's employer. Thus, AAU is the data controller for the research conducted by AAU researchers.

The legal effect of sharing is that both the ceding researcher's institution and the receiving researcher's institution are data controllers.

Personal data included in research data cannot be used for other purposes than research and statistics. This means that a researcher who has collected personal data cannot disclose the data to a third party who will be using the data for other purposes than research or statistics.

Example:

- A researcher wishes to examine upper secondary school pupils' wellbeing and collects data by means of a questionnaire. One of the responding upper secondary schools wishes to receive a copy of the pupils' responses, in order for the school to improve wellbeing. The researcher cannot hand over data to the school, since its purpose for processing the data is not for research but rather a wellbeing effort. However, the school may receive a report including the aggregated results.

7.2 Rules on sharing

Research data including personal data may be shared with researchers from other institutions if the requirements in the data protection regulations are met.

Data collected or received for the purpose of research or statistics, can only be used for research or statistics[1]. Thus, research data must never be shared with other purposes than research purposes.

In the following cases, sharing of research data including personal data to a third party requires prior permission from the Danish Data Protection Agency:

- If the receiver will be processing data outside of the EU/EEA.
- If the research data are human biological material.
- If research data will be shared with a publisher in connection with a publication in a recognised scientific journal or the like.

Please note that the rules on sharing also apply if the data are not personally identifiable to the receiver. The decisive factor is whether it is possible in any way for anyone to connect the personal data to identifiable individuals.

The draft bill proposes that the Danish Data Protection Agency should have the opportunity to establish terms for sharing, including cases in which a permission from the Danish Data Protection Agency is not required. Thus, the Danish Data Protection Agency is expected to establish such terms. To ensure that these terms will be observed, an internal approval process at AAU will presumably be established.

7.2.1 Different rules apply depending on for what purpose the personal data are collected

A distinction has to be made between personal data that are already research data and personal data that are collected for other purposes.

Example 1: Personal data collected for other purposes than research

- A municipal department will be processing applications for funds for people with disabilities. The data collected by the municipality from the application form, among others, are collected for the purpose of making decisions. These personal data can unrestrictedly be used for research purposes.

Example 2: Personal data collected or used for research purposes

- When students collect personal data for their master's theses, they process data for research purposes. The students' purposes are thus research (or research-like). Sharing of personal data used in students' master's theses must comply with the rules on sharing outlined below. Thus, students' supervisors may not receive a copy of the personal data for the purpose of using them in their research.

The rules outlined in the section '7.2 Rules on sharing' concern only the situation described in 'Example 2: Personal data collected or used for research purposes'.

Personal data collected in a situation as described in 'Example 1: Personal data collected for other purposes than research' can be used for research without complying with the rules outlined below. Occasionally, a non-sharing agreement may be made for formal reasons.

7.4 Reusing research data that include personal data

If a researcher employed by AAU either entrusts personal data to a colleague (employed by AAU) or reuses the data for a new research project, it is not sharing but rather reuse of personal data.

7.4.1 Conditions for reusing personal data

If the set of personal data is to be used for a new project, this project must be registered in AAU's registration procedure. If the set of personal data is to be used for an existing project that is already registered, the existing registration must be updated in order for the reused dataset to be covered by the registration. Read more about how changes are made in existing registrations in section '10. Amendments'.

7.5 Data subjects' rights in the event of sharing

If an AAU researcher either receives or discloses research data that include personal data, both the researcher and the receiving researcher must remember to comply with the rights of the data subjects. Read more about this in section '4. The rights of the data subjects'.

[1] The draft bill for the Danish Data Protection Act proposes that, after negotiations with the Danish Minister for Justice, the Danish Minister for Health may lay down rules stating that data processed for the purpose of conducting health science research can later be processed for other purposes than research and statistics, provided that the processing is necessary to the vital interests of the data subject.

7.5.1 Request for erasure

If AAU receives a request for erasure
from a data subject, AAU has an obligation to inform any potential receiver of the personal data that a request for erasure has been received, unless this proves impossible or unreasonably difficult.

7.5.2 Receiving research data

If an AAU researcher receives research data that include personal data, the researcher must remember to comply with the duty of sharing.

If the received research data are to be used for a new project, this project must be registered in AAU's registration procedure. If the received research data are to be used for an existing project that is already registered, the existing registration must be updated.

7.6 The difference between data processing and sharing

When a third party (a company, student, collaboration partner, etc.) not employed by AAU is processing personal data on behalf of and on instructions from an AAU researcher, it constitutes data processing. A data processor is obliged to erase personal data upon request from the data controller. An example of a data processor is Gallup that collects questionnaire data on behalf of a researcher.

If a researcher wishes to be in charge of how personal data are to be processed, including when they are to be erased, it is necessary for the personal data to be shared with this researcher.

Thus, the key difference between data processing and sharing is that data processing entails acting on instructions from the data controller, whereas sharing entails two data controllers since the receiver also has the right to determine how the received personal data are to be processed.

8. AAU's technical support for research

The GDPR requires for appropriate technical and organisational security measures to be implemented. The data controller is obliged to assess what is appropriate. This assessment must include considerations on which category the personal data belong to and what risks may jeopardise the rights of the data subjects.

AAU offers a number of solutions to be used for storage and dispatch of personal data. These are described in details in 'List of storage solutions', which includes the categories of personal data (general, sensitive and confidential) that may be stored. The list is regularly updated by IT Services.

8.1 Storage and sharing solutions

The solutions that AAU offers are to be found here.

8.2 Future solutions and support

At the beginning of 2018, a project called CL**AAU**DIA was initiated as a collaboration between Aalborg University Library (AUB) and IT Services. The project aims to develop technical solutions, including storage solutions for research data, and to establish an advisory function for researchers with regard to technical solutions.

9. Security including security breaches and impact assessments

9.1 Data security

When processing personal data in connection with research, the personal data included in the research must be kept separate from the University's regular administrative procedures.

The researcher must ensure that personal data are not accidentally or illegally destroyed, lost or damaged. This can be ensured by performing regular backups. If the personal data are stored on an AAU drive, backups are performed automatically. Backups are saved for three months as a standard practice.

Moreover, personal data must not be stored in a way that makes it possible to identify the data subjects for a longer period of time than necessary for the completion of the project. If possible, project managers must ensure that the personal data are pseudonymised.

Presentation and communication of the results of the research project must be carried out in a manner that makes it impossible to identify individuals.

If processing of personal data is conducted on IT equipment outside of AAU's locations (or on equipment which is not part of the University' regular systems), the researcher must ensure that the necessary security measures are taken. Any questions regarding the above may be directed to AAU IT Services.

9.2 Data processing and storage

The researcher must ensure that only personal data covered by the registration are processed, and that personal data are not subject to any unauthorised sharing or misuse.

Processing of personal data must only be carried out by the researcher or on behalf of the researcher, which means that the researcher is responsible for the processing. If a research project necessitates processing of personal data by one or several subcontractor(s) or collaboration partner(s), including public authorities, companies and other universities, a data processing agreement must be made prior to this processing. Templates for data processing agreements can be downloaded on https://www.informationssikkerhed.aau.dk/english/personal-data/.

Upon sharing personal data via the internet or other external networks, the researcher must ensure that the necessary security measures are taken in order to prevent unauthorised disclosure. AAU's standard solutions should be used whenever possible. See section '8.2. Standard solutions for sending or sharing personal data'. Please note that it is safe to send emails from one AAU email address to another AAU email address, since all AAU emails are sent in a closed system. It is illegal to use Dropbox or similar solutions.

The researcher is at all times responsible for ensuring that personal data, whether electronic or physical, are stored in accordance with the principles outlined below:

- Physical folders with personal data must be store in locked cabinets or drawers to which only the researcher or research group who will be using the data have a key.
- As a rule, personal data that will be stored electronically must be stored on one of the solutions provided by AAU.
- If personal data are not stored on one of AAU's standard solutions, the researcher must ensure that the personal data are stored in a secure manner so that unauthorised persons cannot gain access to the data. In certain cases, storage outside of the solutions provided by AAU requires for the AAU chief information security officer's approval.
- To the greatest possible extent, personal data must be processed in a form that is not personally identifiable, for instance in a pseudonymised or encrypted form. IT Services can help with encryption.
- Gaining access to personal data must only be possible with a confidential password. Passwords must be changed at least once a year or when necessary.
- When using internal networks, it must be ensured that unauthorised persons cannot gain access to the personal data.
- If personal data are stored on detachable and portable data media, including USB keys or external hard drives, it must be ensured that unauthorised persons cannot gain access to the data on the portable data media in case it is lost or stolen. This can be ensured with strong encryption.
- Only persons with a legitimate need should be able to gain access to personal data. This should be as few persons as possible.

Personal data included in a research project, database or biobank must only be used for research and statistics.

9.3 Control

AAU's data protection officer and chief information security officer must regularly carry out internal spot checks to ensure that the data protection regulations, AAU's information security policies and the above conditions are complied with.

The Danish Data Protection Agency carries out unannounced and announced inspection visits.

9.4 Completion of the project

According to the GDPR, personal data must not be stored longer than necessary in relation to the purpose that the personal data were collected or received. Therefore, at the time when the data are no longer necessary, the researcher or research group must ensure that the data are erased or anonymised in a manner that makes it impossible to identify individuals or that the data are shared with the Danish National Archives in accordance with the Archives Act.

Erasing personal data from electronic media must be done in a manner that prevents the data from being restored. Physical folders must be destroyed by shredding.

In connection with the registration, the researcher must state when the processing is completed, including storage of personal data. If the processing of personal data has not yet been completed, it is possible to apply for an extension of the end date.

9.5 Security breaches

9.5.1 What is a security breach?

A security breach is an accidental or intentional loss, alteration, publication or unauthorised disclosure of or access to personal data. Such breaches may include:

- Your computer is hacked
- Links in 'fake' emails are opened (phishing)
- Faulty leak of staff members' social security numbers.
- A complaint by a student that has been left in the printer.
- Theft of exam lists or applications etc., or
- If the crash of an IT system prevents execution of exams
- A lost USB key on which personal data are stored.

9.5.2 What to do in case of a security breach

In the event of a personal data security breach, you must report it to the DPO as soon as possible; AAU is obliged to report personal data breaches to the Danish Data Protection Agency without undue delay and **no later than 72 hours** following the discovery of the breach, if the breach puts the rights and freedoms of natural persons at risk. This means that as soon as you become aware of a security breach, regardless of whether you assess it to put the rights and freedoms of natural persons at risk, you must report it via the web form 'Internal reporting of personal data breaches' which can be found here (link).

9.6 Impact assessments

An impact assessment is an assessment of the consequences it will have for the protection of personal data to execute the planned processing of personal data.
In certain situations, for instance when large amounts of sensitive personal data are processed, an impact assessment is obligatory. If the assessment indicates that the rights and freedoms of the data subjects are at high risk, the processing must be approved by the Danish Data Protection Agency before the processing can be commenced. Guides and templates for impact assessments will be prepared as soon as possible.

10. Amendments

If amendments are carried out after the researcher or research group has registered the project, these amendments must be registered.

Examples of amendments that must be registered:

- Extension of the project, including extension of the deadline for the personal data to be erased, anonymised or archived.
- Extension of the period in which the researcher wishes to retain an established database or biobank.
- Amendments to how the personal data are processed after the processing has been completed (erasure, archiving or anonymisation).
- Amendments to the number of individuals about whom data are processed.

- New data processor(s)
- New project manager or project title
- Project manager changes department.
- Adding a new dataset to a pre-existing project.