UNIVERSITY OF COPENHAGEN
FACULTY OF HEALTH AND MEDICAL SCIENCES
FACULTY OF SCIENCE

GDPR guide for research projects in which personal data is processed

February 2023

Introduction

This guide has been prepared by GCP Coordinator Lene Stevner (NEXS, SCIENCE) along with in-house lawyers at SUND and SCIENCE Marianne Dichow and Pernille Wigh. If you have any comments regarding the content, we would like to hear from you.

Please contact:
Lene: less@nexs.ku.dk
Marianne: marianne.dichow@sund.ku.dk
Pernille: pernille.wigh@sund.ku.dk

In this guide, you will find checklists that describe, in chronological order, how to process the personal data of respondents/test subjects before and during the project as well as after the data collection, including the collection of biological material, if applicable, has been completed.

The checklist procedures apply to the entire project period – from before personal data is collected until it can be anonymised, erased, or destroyed. Handling of biological material is also subject to the procedures.

The Principal Investigator (PI)/project manager is responsible for ensuring that personal data, including any biological samples, is processed lawfully throughout the entire project life cycle.

If you are unsure about anything related to the processing of personal data, you can always ask the in-house counsel at SUND or SCIENCE or your local contact person.

Find your contact person
Glossary

The pages 3-9 shows the checklist in the different stages of the project. You can use the "go to" section below on each page to navigate through the stages. From page 11 beginning with a content overview you can find further information. The content overview you can find by using the three small lines beside the page numbering.

What must I do before the start of the project? (The preparation phase)

This content has been organised for you to use as a checklist in order to ensure the correct use of the GDPR data collected throughout your research project ☑

- ○ Research data management (RDM) is a collective term for activities undertaken with research data before, during and after a research project. Please read UCPH Policy for Research Data Management describing what is expected of researcher and research support staff. Projects including GDPR data shall also comply with UCPH Policy for Research Data Management and Data Management Plans (DMP) must be developed and documented before any physical materials and/or digital data are collected, observed, generated, created or reused.

- ○ It is important to clarify roles and data responsibility with all parties involved in a collaborative project before starting the data collection. You must identify and clarify the flow of personal data in the project. In most situations will the university be data controller/data responsible in the project e.g by a transfer of data within the project. However the Processing of data can also be as joint data controlling or by use of an external data processor. Read more about collaboration with external parties with need for access to each other's data. Also read more about roles and data responsibility in the joint guidelines between regions and universities (in Danish only)

- ○ If it is known from the outset that data is to be shared with partners or data processors in non-secure third countries, EU standard contracts should be sent to the external party before the collaboration is finally agreed. In this way, the collaborative party will be made aware of and have accepted the legal obligations associated with receiving the data. Read more about the sharing of personal data with partners in non-secure third countries. Alternatively, the basis for transfer can be consent. Read more about consent.

- ○ Always make sure to register the research project in the records of research projects involving personal data. After registration of the project, you will receive a letter of registration from the faculty secretariat. Once you have received the registration letter, and other applicable approvals, you may recruit respondents/test subjects and start the data collection. Please use use the registration form found on KUnet. Read more about registering research projects in the records.

- ○ Check whether you need any additional regulatory approvals and registrations (in particular for health science research projects, scientific research projects using health data and drug trials). Read more about other notifications/approvals, registrations and regular reports.

- ○ Registering a project in the records of research projects involving personal data also includes an impact assessment and a GDPR risk assessment of your project. Read more about GDPR risk assessments and impact assessments.

- ○ In connection with registering the project, you must decide when the personal data may/must be erased/anonymised, and this timing must be stated in the registration form. Personal data must only be erased in accordance with all relevant guidelines and legislation. What legislation is relevant depends on the type of project. If you want to store personal data for longer than stipulated in the legislation, you need explicit consent from the respondents/test subjects. Read more about when personal data may be anonymised.

- ○ When collecting personal data, you must always provide your respondents/test subjects with an informed basis for participating (duty of notification) – regardless of whether your work is based on a GDPR declaration of consent or not. Read more about the duty of notification and research with and without GDPR consent.

- ○ For example, if you want to have the opportunity to summon the same respondents/test subjects in a future project, you also need consent allowing you to recontact your respondents/test subjects.

- ○ Remember that images/audio recordings/videos of respondents/test subjects are personal data. If, for example, you wish to publish images from a research project, you must be aware of this. Read more about use of images and video material.

What must I do before the start of the project? (The preparation phase)

- ◯ Create a folder on the S-drive (a group drive ordered through KU-IT) or find an equally secure solution to store sensitive files. Read more about the storage of physical (including printed) and electronic documents.
- ◯ Think about future-proofing and how to retrieve data when you set up user access to data so that other researchers or your immediate supervisor, for example, can find/retrieve data if you are unable to complete your tasks or you leave UCPH. Read more about future-proofing access to data. You also need to consider and comply with UCPH Policy for Research Data Management.
- ◯ The following documents, as a minimum, must be filed in WorkZone: The approval from UCPH/the faculty secretariat, the protocol/amendments for the project, collaboration agreements, regulatory approvals (VEK-LMS, i.e. the Research Ethics Committee and the Danish Medicines Agency), data processing agreements/agreements on joint data controlling and disclosure agreements. Follow the procedure for filing documents on cases in case group 514 (in Danish only) as well as the department's guidelines for setting up S-drives or other similar guidelines.
- ◯ Special rules apply to data processors in non-secure third countries, for example the USA and Greenland. Read more about data processors in non-secure third countries.
- ◯ A guest declaration and a related data processing agreement must be made when non-UCPH staff (including emeriti, students, interns, guests or loosely affiliated persons) are to participate in a project with access to data. Read more about students, visiting researchers and other loosely affiliated persons.
- ◯ Please remember that the PI/project manager must guide students, interns, guests or loosely affiliated persons in the handling of personal data before they may access the data. Read more about points of special attention in relation to students, visiting researchers and other loosely affiliated persons.
- ◯ In the UCPH Policy for Research Data Management it is also described what is expected of students, researchers, research leaders and research support staff when managing research data at UCPH.
- ◯ Researchers who work at Danish universities and who carry out research projects that fall within the scope of the Executive Order on the Reporting of Digital Research Data Generated by State Authorities must register information about their research projects and/or digital research data sets with the National Archives. Read more about this obligation.
- ◯ If a grant has a clause stating that data must apply the FAIR principles/Open Science. Read more about uploading data to publicly available databases.
- ◯ If you process data of which UCPH is not the data controller. Read more about where UCPH is data processor for external data controllers.

What must I do regularly during the project? (Ongoing projects)

This content has been organised for you to use as a checklist in order to ensure the correct use of the GDPR data collected throughout your research project ☑

- ◯ If making a pre-screening, the personal data from the persons deemed not relevant and who are therefore never invited to the oral information meeting, or included in the project, must be destroyed immediately. However, the total number of pre-screened persons must be noted, as it must be reported when publishing data.

- ◯ PLEASE NOTE: A pre-screening is the selection of potential test subjects that is conducted during the recruitment phase and should not be confused with the screening that the test subjects undergo face to face with investigator/PI when making the final decision on whether to include them. Read more about the storage of physical documents.

- ◯ Remember to be aware of your duty of notification when you collect personal data from respondents/test subjects. Read more about the duty of notification and research with and without GDPR consent.

- ◯ If you have assessed that you choose to process data on the basis of consent, the consent must be obtained from all respondents/test subjects. The duty of notification and the GDPR consent may be gathered in one document. Read more about the duty of notification and research with and without GDPR consent.

- ◯ Email correspondence with respondents/test subjects must be erased from Outlook within 30 days at the latest. If the email contains information that is essential to the project and you need to be able to document this later on, you should before deleting the email transfer a copy of the email to the S-drive (your secure drive) or another UCPH-approved storage location. Read more about the storage of physical (including printed) and electronic documents.

Take good care of your respondents/test subjects' information:

- ◯ Create a printed or an electronic ID log. Assign a unique ID number to each respondent/test subject when screening and including them in the project. Read more about ID logs.

- ◯ All printed and electronic documents containing personally data must be processed in pseudonymised form and stored with a high level of security and always separately from the ID log. If the ID log is electronic, it and other files containing personally identifiable data must be stored on the S-drive or another UCPH-approved storage location. Read more about the storage of electronic documents.

- ◯ Biological samples from test subjects may only be identified with their ID number

- ◯ Biological human material must be stored in locked temperature-monitored freezers with an alarm. Read more about biological material.

- ◯ If significant changes are made in regard to the data processing in the project, the changes must be registered in the records of research projects involving personal data. Read more about changes to the UCPH notification.

- ◯ For health science research projects, all Serious Adverse Events must be reported continually and an annual report of all side effects must be reported to the Research Ethics Committee. Read more about other notifications/approvals, registrations and regular reports.

What must I do regularly during the project? (Ongoing projects)

- ◯ The following documents, as a minimum, must be filed in WorkZone: The letter of registration from UCPH/ the faculty secretariat, the protocol for the project, the registration and the faculty secretariat's registration of significant changes in data processing/the project, protocol amendments, cooperation contracts, regulatory approvals (VEK-LMS, i.e. the Research Ethics Committee and the Danish Medicines Agency), data processing agreements/agreements on joint data controlling and recipient statements in connection with the disclosure of personal data to other parties outside UCPH. Follow the procedure for filing documents on cases in case group 514 (in Danish only) as well as the guidelines for the storage of personal data on the S-drive or another secure platform for the storage of personal data. Further info: Safe storage of personal data and biological material – KUnet.

- ◯ Make sure to continually future-proof access to data so that other researchers can gain access to data if, for example, you are unable to complete your tasks or leave UCPH. Read more about future-proofing access to data.

PLEASE NOTE:
It is important to clarify the roles and data responsibility of all parties involved in a project before data collection begins with a view to clarifying whether the flow of personal data is to be processed by joint data controlling, use of an external data processor or transmission of data. Read more about collaboration with external parties with need for access to each other's data. Also read more about roles and data responsibility (in Danish only). If you are data processor for an external data controller, then please: Read more about where UCPH is data processor for an external data controller.

- ◯ During all phases of your project you need to consider the consequences if e.g. a collaboration partner or an employee leave the project. Read more about future-proofing access to data.

Remember to enter into agreements on data processing:

- ◯ A data processing agreement must always be entered into before data, including biological material, is made available to an external data processor. This also applies if you use a cloud-based IT solution and personal data is to be uploaded to the IT solution. Before using a data processor you need to make an impact assessment and a GDPR risk assessment of the data processor. Please read more about GDPR risk assessments. Read more about data processing agreements.

- ◯ UCPH has entered into a general data processing agreement with the Capital Region of Denmark, Statistics Denmark and the Danish Health Data Authority. A general data processing agreement has also been entered into with Rambøll on the use of the system SurveyXact and with DTU on the use of Computerome 2.0. You must also be aware of whether your faculty or department has entered into a general data processing agreement with, for example, a supplier of a cloud-based IT system. Read more about general data processing agreements.

- ◯ Special rules apply to data processors in non-secure third countries, for example the USA and Greenland. Read more about data in non-secure third countries

- ◯ Data processing agreements must be entered into when non-UCPH staff, for example, emeriti, students, interns, guests or loosely affiliated persons, are to participate in a project and process data. If the loosely affiliated persons participate in the project and receive access to view personal data without processing data, you must enter a confidentiality agreement with them. Read more about students, visiting researchers and other loosely affiliated persons.

- ◯ Please remember that you as PI/project manager must guide students, interns, guests or other loosely affiliated persons – including researchers who have left UCPH – in the handling of personal data before they may gain access to the data. Read more about points of special attention in relation to students, visiting researchers and other loosely affiliated persons. In the UCPH Policy for Research Data Management it is also described what is expected of students, researchers, research leaders and research support staff when managing research data at UCPH.

CHECKLIST

What should I do immediately after the data collection has been completed (Last Patient Last Visit)?

This content has been organised for you to use as a checklist in order to ensure the correct use of the GDPR data collected throughout your research project ☑

- ○ When you report payments to the respondents/test subjects to UCPH accounting never use the project title. Instead, you have to use the project alias and project account.
- ○ If, as PI/project manager, you are encouraged to upload your data in public databases by journals, grant donors and/or partners, then please read more about uploading to publicly available databases.
- ○ Health science research projects must be reported complete to the relevant authorities. Read more about other notifications/approvals, registrations and regular reports.
- ○ During all phases of your project you need to consider the consequences if e.g. a collaboration partner or an employee leave the project. Read more about future-proofing access to data.

What should I do when the data processing (the analysis work) has been completed?

This content has been organised for you to use as a checklist in order to ensure the correct use of the GDPR data collected throughout your research project ☑

- ◯ When the registration with the faculty secretariat expires, personal data must be anonymised or erased. If you continue to have an objective justification for storing data in a personally identifiable state for a longer period of time, you may request the faculty secretariat for an extension of the processing period. Read more about changes to the UCPH notification.

- ◯ Please note that if you wish to transfer data etc. from a research project to a public available database with a view to future research you need consent from the respondent/test subject. Read more about uploading data to publicly available databases.

Destroy any remaining biological material in the research biobank (and make sure that all data processors/partners do the same) when:

- ◯ The analyses described in the protocol have been carried out and quality-assured and,

- ◯ The date of the destruction stated in the protocol has been reached. Read more about research biobanks.

- ◯ You are only allowed to transfer excess biological material from the research biobank to a biobank (an organised collection of human biological material that is stored with a view to future unspecified research) if you have specific consent to do so from the test subject. Otherwise, it must be destroyed. Read more about biobanks for future research.

To anonymise data, you must ensure that:

- ◯ All printed documents containing personal data are shredded (e.g. name, civil registration number, or any other information that in itself or in combination with other information becomes personally identifiable). If any data (e.g. documents containing measurement results) is to be kept, it must be anonymised manually by either tearing or blacking out all personal data (after blacking out text, make a copy of the document, save the copy and shred the original).

- ◯ Project staff and/or collaborating parties who have participated in the processing of respondents/test subjects and/or their data must be informed that the project will now be anonymised, so that their documents, etc. from the project containing personally identifiable data too is shredded or erased.

- ◯ All project folders containing pseudonymised data (meaning ID numbers/codes instead of personal data) are checked to ensure that there are no personally identifiable data. Also check external systems for personally identifiable data.

- ◯ The project S-drive must be deleted and the owner of the S-drive used for the project must request UCPH IT to delete the project S-drive. Files that are to be kept must be completely cleared of personally identifiable data and the project folder moved to a less secure drive.

- ◯ Project-related shared mailboxes in Outlook must be reviewed and the mailbox should be closed. Read more about the storage of physical (including printed) and electronic documents.

- ◯ If biological material has been transferred to a Biobank, the person responsible for the biobank must be informed that the project has been anonymised.

- ◯ During all phases of your project you need to consider the consequences if e.g. a collaboration partner, an employee or your self leave the project. Read more about future-proofing data.

- ◯ If you have data that must be transferred to the Danish National Archives. Read more about archiving research data.

What should you do with your anonymised data?
When all personal data has been destroyed/deleted and it is no longer possible to retrieve the identity of the respondent/test subject, your data/your material is no longer regulated by the GDPR, the Danish Data Protection Act and the Danish Act on Committees on Health Research Ethics (Komitéloven).

What should I do when the data processing (the analysis work) has been completed?

Anonymous data can be shared freely and used for research without the approvals of various authorities, but you must be aware of any limitations in relation to other agreements and other legislation, for example, cooperation agreements and the Danish Copyright Act.

It must be clear in all archives and from the folder names on shared drives that the project has been anonymised. Due to limited storage facilities, you must regularly consider whether anonymised printed data and biological material should still be stored.

Content overview

Notification/registration of the trial at UCPH 12
Non registred project 12
Changes to the UCPH notification 12

Other notifications/approvals, registrations and regular reports 13
The Research Ethics Committee (VEK) 13
The National Committee on Health Research Ethics (NVK) 13
The Danish Medicines Agency (LMS) 13
Annual reports 14
Reports at the end of the trial 14
Clinicaltrials.gov 14
Research Ethics Committee of SCIENCE and SUND 14

GDPR risk assessment and impact assessment 15
General guidelines 15
When may personal data be anonymised and/or deleted? 15
Research data management 16
Table of different types of projects 17

Collaboration with external parties with need for access to each other's data 18
Collaboration with external parties 18
Regarding being independent data controller 19
Regarding joint data controlling 19
Regarding data processing 19
Regarding disclosure of data 19

Data processing agreements 20
General considerations 20
Data processing agreements 20
General data processing agreements 21
Where UCPH is data processor for an external data controller 21
Students, visiting researchers and other loosely affiliated persons 21
Points of special attention in relation to students, visiting researchers and other loosely affiliated persons 22
Data processors in non-secure third countries 23

Duty of notification and research with and without GDPR consent 24
Duty of notification and research without GDPR consent 24
Duty of notification and research with GDPR consent 24
Few exceptions from the duty of notification 25
Disclosure of personally identifiable data without consent 25

Storage of physical (including printed) and electronic documents 26
Storage of electronic documents 26
Storage of physical documents 26

Biological material is personal data and therefore subject to the GDPR 28
Biological material 28
Research biobank 28
Biobank for future research 28

Pseudonymisation – Confidentiality and security 30
Pseudonymisation 30
ID log 30

Uploading data to publicly available databases 32

Anonymisation 33
Anonymisation 33
Data has been anonymised when 33

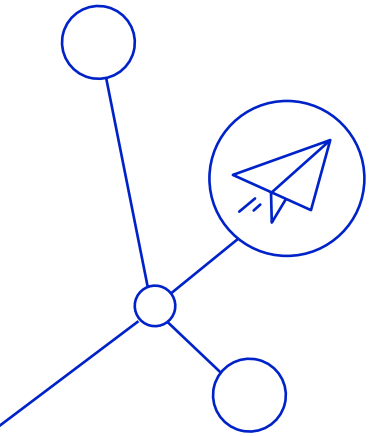
Breaches of security and future-proofing access to data 34
Breaches of security 34
Future-proofing access to data 34

Local contact persons 35
Abbreviations and glossary 36

Notification/registration of the project/trial at UCPH

TOPICS

› Non registred project
› Changes to the UCPH notification



All projects must be registered in the University's joint records by the faculty secretariat before initiating the data collection/project.

Non registred project

Projects that have not been registered before they started must be registered immediately – unless the project is so old that the data from the project must be anonymised. When registering a project with retroactive effect, you must specify the original start date in the 'start date' field and write in the comment field on the registration form that 'the project has unfortunately not been registered on time' or that 'the project has previously been covered by an approved umbrella/joint notification for the Faculty or has been reported to the Danish Data Protection Agency before 1 October 2015'.

Register the project via the registration form on the research portal on KUnet.

- The registration form contains help text that may help you fill in the form;
- The registration form must state, among other things, which personal data is to be processed and when the data from the project can be anonymised. Likewise any data processing agreements – that already are in place and have been signed – may be attached.

When the faculty secretariat has registered the project, an registration will be sent to the PI/project manager and the project will be registered in the statutory records of research projects that involve the processing of personal data.

The faculty secretariat archives/files the letter of registration and any attached data processing agreements in WorkZone.

Changes to the UCPH notification

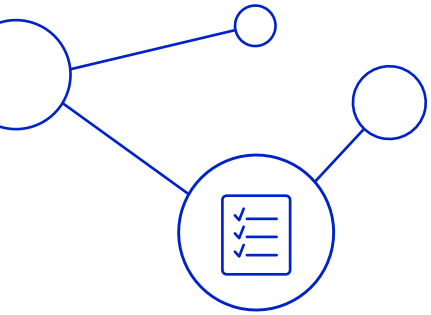
If, after the project has been registered, any significant changes are made to the project, these must be registered using the form specific for your faculty. When the form is submitted, the faculty secretariat will receive it as a request for registration of the changes to the project. Significant changes could be:

- New PI/ project manager
- Changes in data collected,
- Changes in the number of respondents/test subjects
- Extension or shortening of the processing period
- New data processor(s)
- If in doubt about whether a change is significant, please contact the in-house counsel.

Other notifications/approvals, registrations and regular reports

TOPICS

- The Research Ethics Committee (VEK)
- The National Committee on Health Research Ethics (NVK)
- The Danish Medicines Agency (LMS)
- Annual reports
- Reports at the end of the trial
- Clinicaltrials.gov
- Research Ethics Committee of Science and SUND



The PI/project manager is responsible for ensuring that the project has obtained all relevant statutory approvals and that it is registered in all the relevant places prior to initiation. See more about medical science projects.

The Research Ethics Committee (VEK)
Health research projects and database research projects involving biological material must be notified to and approved by VEK prior to initiation.

If patient record data is included in your project, the PI/project manager must make sure that it is stated in the project protocol and approved by VEK that the doctor responsible for treating the patient will share patient record data with the project. Read more in the guidelines "*Inter-institutional health data collaboration between regions and universities 2018*" under Collaboration with regions on the UCPH Research Portal.

The National Committee on Health Research Ethics (NVK)
Research in diagnostic imaging and genetic database data must be notified to and approved by NVK. Read more about scientific research projects using health data on the research portal on KUnet: Medical science projects – KUnet.

Changes to an already-approved project that have an impact on the data quality and/or test subject security must not be initiated until they have been approved by VEK in the form of a supplementary protocol.

If a Serious Adverse Event (SAE) occurs during the trial (in non-drug trials), it must be reported to VEK no later than 7 days after you become acquainted with it. Use this form for the report (in Danish only).

The person responsible for the trial must notify the Committee within 90 days after the completion of the project (Section 31 (1) of the Danish Act on Committees on Health Research Ethics). The project is considered complete when the last test subject has finished. Use this form for the notification of completion (in Danish only).

Once a year during the entire trial period, the investigator must submit a list of all serious expected and unexpected adverse reactions and all serious events that have occurred in the period. The report must be accompanied by an assessment of the safety of the test subjects. Use this link to the external NVK form (in Danish only).

If the project is stopped before planned, the Committee must be notified within 15 days from the time when the decision to discontinue the project was made. The reasons for stopping the project must be given. The Committee may demand a reasoned explanation from the investigator.

The Danish Medicines Agency (LMS)
Clinical trials of medicines (drug trials) and clinical investigations of medical devices must be notified to and approved by the Danish Medicines Agency (LMS), before they are initiated. Read more about Clinical trials of medicines Read more about clinical investigations of medical devices here (in Danish only).

Annual reports
Once a year throughout the entire trial period, the sponsor investigator must prepare a list of all serious suspected adverse reactions that have occurred during the trial period and a report on the safety of the test subjects in which all serious events should be included in the assessment. The list and report must be submitted to VEK, LMS and the pharmaceutical authorities and ethics committees (unless otherwise stipulated in national law) in the countries in which the experiment is conducted.

Reports at the end of the trial
All events and adverse reactions are to be reported at the end of the trial in the final registration in EudraCT and in the report to VEK if they have asked for this.

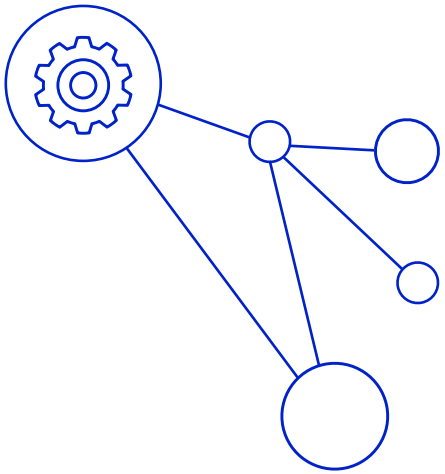
Clinicaltrials.gov
The investigator must register and regularly update the project in Clinicaltrials.gov or in a similar database. It is very important to update the registration with new secondary outcomes that are to be implemented in the study following changes/supplementary protocols.

Research Ethics Committee of SCIENCE and SUND
The Research Ethics Committee for SCIENCE and SUND issues ethical reviews of research projects or publications if it is required by the Funding organization or the journal in question. The Research Ethics Committee for SCIENCE and SUND does not review projects and publications approved by the regional Health Research Ethics Committee (VEK). Read more about Research Ethics Committee of SCIENCE and SUND.

GDPR risk assessment and impact assessment

TOPICS

› General guidelines
› When may personal data be anonymised and/or deleted?
› Research data management
› Table of different types of projects



General guidelines
UCPH, as a data controller, has a duty to process and store personal data with an appropriate level of security. The appropriate level of security is determined by assessing the risks that data processing may pose to the respondents/test subjects whose data is being processed. This is called a GDPR risk assessment.

As data controller, UCPH is obliged to carry out an impact assessment when personal data is processed and when/if it is processed in a way that is likely to result in a high level of risk to the rights and freedoms of the data subjects. The analysis must clarify what consequences it may have for the respondent/test subject if data is lost, changed or misused.

The registration form incorporates the necessary elements from the GDPR risk assessment and questions regarding any consequences for the data subject. When you fill in the registration form, you may trigger additional questions from the person who approves your registration, and if that is the case, you will be contacted directly. If you fill in an impact assessment because the project entails a high risk for the data subjects, the impact assessment must be approved by the head of department. Please contact in-house legal for guidance. You will receive an email from the data protection officer with an approval or supplementary questions or comments if you have carried out an impact assessment in connection with registering the project.

If you have registered the research project before 1 October 2020, when the risk and impact assessment were incorporated into the registration form, you can find a form to carry out the assessment/analysis on the research portal on KUnet on the page on GDPR risk assessment and impact assessment. This may become relevant if, for example, grant donors, partners or government agencies ask for a GDPR risk assessment or impact assessment. Please also remember that when you add a new data processor to your project a risk assessment must be completed. Contact the in-house legal for assistance.

Further info: Risk and impact assessment – KUnet. The impact assessment is also called DPIA, which is short for Data Privacy Impact Assessment, and, in practice, this abbreviation is often used instead of the term 'impact assessment'.

When may personal data be anonymised and/or deleted?
Respondents'/test subjects' personally identifiable data must be erased/anonymised as soon as processing the data for the purpose for which it was collected is no longer necessary.

Examples of rules, legal requirements or consent to the continued availability of personal data/biological (see also overview table).

Please note that the personal data processed in the research projects is also the project's source data. Source data is essential for the subsequent evaluation of the execution of the project, the quality of data and the final research results. Legislation other than the GDPR may influence how you must process your source data. Among other things, source data is required to be available after the end of the project and/or after publication, so that the author-

ities and/or other researchers can access them. What other legislation imposes requirements on source data availability depends entirely on the individual project type, and requirements may therefore vary from project to project.

1. The Danish Code of Conduct for Research Integrity stipulates that source data must be stored for five years after publication. The code applies to all research projects conducted at a Danish university.

2. The public patient compensation scheme recommends storing source data for 10 years after Last Patient Last Visit (LPLV):
   - All test subjects participating in health science research projects carried out in Denmark are insured by the public compensation scheme/the Danish Patient Compensation Association.
   - The Patient Compensation Association recommends that source data shall be available for 10 years after the test subjects have completed their participation (LPLV), as this is the ultimate time period during which the test subject can apply for compensation for an study-related injury after their participation in the project. Source data at an individual level will be important documentation for UCPH in the event of legal action brought by a previous test subject.
   - If the PI/project manager anonymises the project earlier than that, the PI/project manager must be able to objectively state the reasons that the methods and/or intervention used cannot lead to injury.

3. The ICH-GCP regulation applies to all trials of medicinal products and necessitates that all source data is available for inspection by the authorities for 25 years.

4. Trials of medical devices are regulated by the ISO standard ISO 14155:2020, which is in line with the ICH-GCP regulations.

5. The consent of the respondent/test subject may affect how long the data may be processed, including whether the person has consented to being contacted again, for example, in connection with a new project or whether the biological material may be added to a biobank.
See examples in table next page.

Research data management
Research data management (RDM) is relevant through out the entire project timeline and cover all activities undertaken with research data before, during and after a research project. Projects including GDPR data shall comply with UCPH Policy for Research Data Management and Data Management Plans (DMP) must be developed and documented before any physical materials and/or digital data are collected, observed, generated, created or reused. The UCPH Policy for RDM shall also be followed in projects with GDPR data and must be developed and documented. Read more about UCPH Policy for Research Data Management.

Table of different types of projects
The guidelines in the table below have been adjusted to fit the rules that apply to different types of projects:

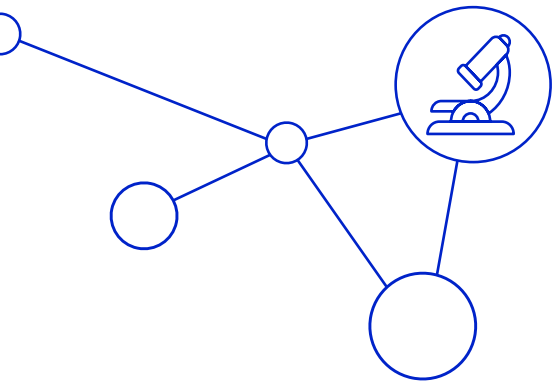
PROJECT TYPE:	SOURCE DATA MUST NOT BE ANONYMISED UNTIL:	EXCEPTIONS:
Social science and health science database research projects that do not include the use of biological material/questionnaire and/or interview studies that do not include biological material.	**5 years after publication** See the Danish Code of Conduct for Research Integrity[1].	A longer storage period requires the express consent of the respondent/test subject. This could be, for example, if you want to be able to recontact the respondent/test subject for follow-up projects.
Health science database research projects that include biobank and/or health data from genetic and image diagnostic databases.	**5 years after publication** See the Danish Code of Conduct for Research Integrity[1].	
Health science research projects (non-drug trials).	**10 years after Last Patient Last Visit (LPLV)** See the Danish Patient Compensation Association, which covers all test subjects who participate in clinical trials in Denmark.	A longer storage period requires the express consent of the respondent/test subject. For example: › May be recontacted for follow-up projects › Biobank – read more about biological material.
Drug trials – trials of medicinal products that are to be marketed or new experiments with medicinal products that have already been marketed).	**25 years after Last Patient Last Visit (LPLV)** See the GCP regulation, which is expected to come into force at the beginning of 2022.	If the contract with the sponsor states that the data must be stored for longer.
Clinical trials of medical devices – clinical trials of non-CE certified Medical Devices.	**Up to 25 years** See ISO Standard 14155 (which is akin to the GCP regulation).	If the contract with the sponsor states that the data must be stored for longer.

1. Det danske adfærdskodeks for forskningsintegritet — Uddannelses- og Forskningsministeriet (ufm.dk)

Collaboration with external parties with need for access to each other's data

TOPICS

› Collaboration with external parties
› Regarding being independent data controller
› Regarding joint data controlling
› Regarding data processing
› Regarding disclosure of data



Collaboration with external parties
It is important that the role allocation and data responsibility has been agreed between the parties before initiating a collaboration with an external party and/or entering into a cooperation agreement.

When clarifying the roles of the project participants in accordance with the data protection law, the starting point will be that the research institution, represented by the PI, is data controller, due to the fact that the researcher in most cases will be responsible for determining the purpose of the researchers own processing of data and the means used to process data in the research project, cf. freedom of research. However, there must always be a specific assessment of the participants' roles in each project.

It is also important to assess the roles based on each individual processing of data within the project. This means that all of the collaborating parties may be considered independent data controller for a specific process in the project; meaning that there might be more than one data controller in each project.

The collaborative model chosen is of great importance to:

› how data can subsequently be shared within and outside the project and which contracts must be entered into between the parties involved in this connection.

› the content of the GDPR consent, if relevant, which must be obtained from the respondents/test subjects. The PI/ project manager must consider whether consent must be obtained for data transfers – regardless of whether the data is directly personally identifiable or pseudonymised – and biological material between partners, both inside and outside the EU/EEA, as well as data processing outside the EU/EEA. Read more about the duty of notification and research with and without GDPR consent.

Make an overview of the agreed data flow in the project before contacting the Tech Transfer Office or the in-house counsel. Inspiration on how to develop a dataflow please see Research Portal and the site about Data Management Plans.

The legal advisors must be provided with information about all planned sharing of data and the agreed role allocation in order to make an adjusted collaboration agreement and provide advice on other agreements. Examples of the role allocation between UCPH and external partners:

› Sharing data controlling – joint data controlling – Article 26 of the GDPR
› Data processing – the roles as controller/processor – Article 28 of the GDPR (Requirement for data processing agreements with instructions)
› UCPH as independent data controller
› UCPH as data processor
› Disclosure of data

Regarding being independent data controller
The party 1) determining the purpose of the research project in general or the specific part of processing of data and 2) deciding the means to be used when processing the personal data shall be considered the data controller.

It is important to assess the roles based on each individual processing of data within the project. This means that more than one of the collaborating parties may be considered independent data controller for a specific process within the project; meaning that there might be more than one data controller in each project.

Regarding joint data controlling
It is joint data controlling when sharing personally identifiable research data within a research collaboration in which both/all parties determine the purpose and means of the research collaboration together.

— It is joint data controlling
› When there are two or more data controllers,
› When the cooperation agreement describes a common/joint purpose of the research collaboration, and
› When the cooperation agreement defines the research method, the purpose of processing personal data and determines the means of processing the personal data in the research project.

In cases of joint data controlling, the parties must enter into an agreement on joint data controlling in addition to a cooperation agreement. Here you can find a draft agreement.

Regarding data processing
— Data controller
The institution in which the project is anchored determines for what purpose and by what means data may be processed. At the institution, the main responsibility lies with the PI/project manager.

— Data processor
The institution or natural person who processes personal data on behalf of the data controller and on instructions from the data controller.

In cases of data processing, the parties must enter into a data processing agreement before the data may be exchanged – read the entire section on data processing agreements.

Regarding disclosure of data
Disclosure is when personally identifiable data is transferred to the recipient and they process this data on their own behalf for their own purposes.

It is possible to transfer data from one data controller to a new independent data controller within a research project. This can be necessary if the parties has been assessed independent data controllers. Such transfer/disclosure must be clear in the information (duty of notifications) given to the respondents/data subjects.

The general rule is that disclosing data within the EU/EEA does not require approval from the Danish Data Protection Agency.

— Exception from the main rule
The Danish Data Protection Agency must approve the disclosure of personally identifiable data in the case of:
› Transfer of biological material
› All data disclosed to countries outside the EU and EEA
› Disclosure with a view to publishing personal data in a reputable scientific journal or the like.

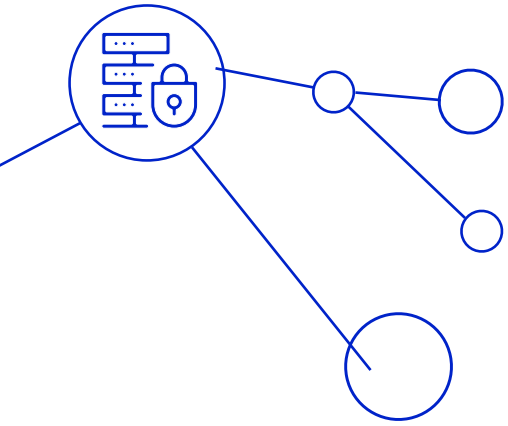
If the case of disclosure of data to a new independent data controller, the recipient must sign a recipient statement before the data may be disclosed. Read more about sharing and disclosure of research data.

The data controller must assess whether there is a legal basis for the disclosure in Section 10 of the Danish Data Protection Act or whether the processing/disclosure may be performed based on GDPR consent. Please ask the in-house counsel if you are in doubt.

Data processing agreements

TOPICS

- General considerations
- Data processing agreements
- General data processing agreements
- Where UCPH is data processor for an external data controller
- Students, visiting researchers and other loosely affiliated person
- Points of special attention in relation to students, visiting researchers and other loosely affiliated persons
- Data processors in non-secure third countries



General considerations

When clarifying the roles of the project participants in accordance with the data protection law, the main rule is that the research institution, represented by the PI/project manager, is the data controller, due to the fact that the researcher in most cases will be responsible for determining the purpose of the researchers own processing of data and the means used to process data in the research project, cf. freedom of research. However, there must always be a specific assessment of the participants' roles in each project.

Data processing agreements

Data processing agreements must **always** be entered into when you use an external data processors, and this must be done **before** handing over data or biological material to them. An external data processor is defined as a non-UCPH employee or an external institution/company. Using an external data processor the PI also need to do a Risk Assessment.

A data processor is a natural or legal person, public authority, agency or other body which processes personal data and biological material on behalf of and by instructions from the data controller.

When UCPH uses a data processor, the PI/project manager is always obligated to supervise the data processor. In the University's standard agreement for data processing in research projects, Appendix C contains a document that is to be used in connection with the supervision of the data processor.

Examples of data processors:

- Laboratories
- The system owner of the external system in which data is entered into either directly by the respondent/test subject or by project staff (for example, for diet registration, interest forms, questionnaires and/or eCRFs)
- Partners that only analyse data on behalf of UCPH and according to instructions
- Statisticians
- Students who need to access and process research data in connection with their bachelor's project/master's thesis
- Visiting researchers and other loosely affiliated persons who need to access and process research data in connection with their stay at UCPH.

Data and biological material must always be sent to the data processor in pseudonymised form. The respondent's/test person's personal data and/or ID log must not be disclosed to the data processor.

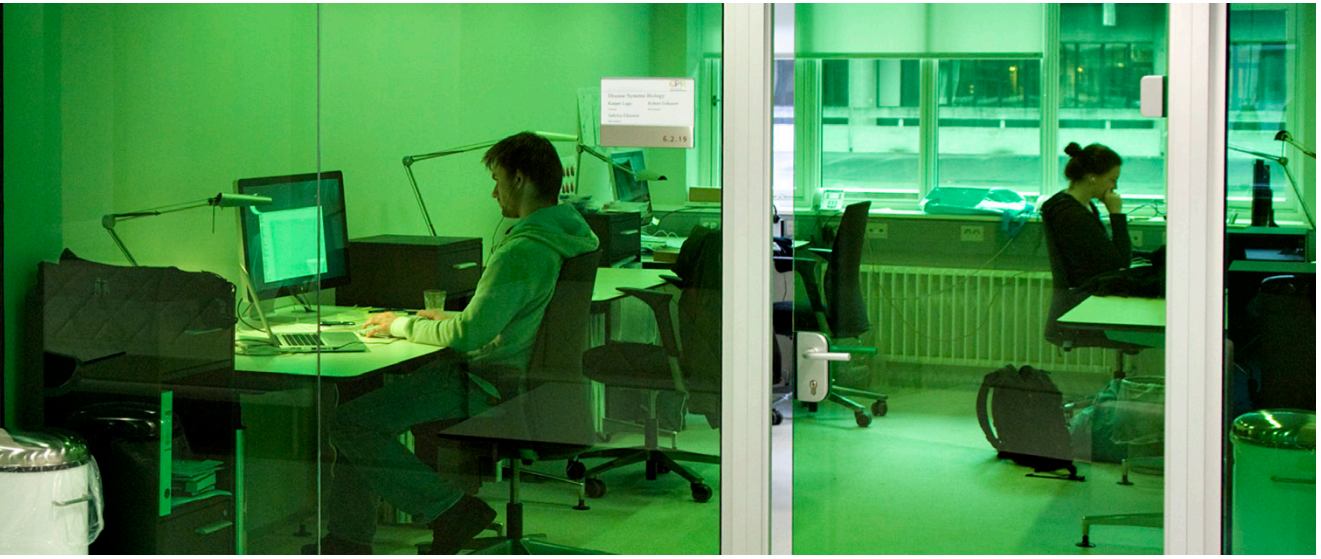
If sending/exchanging data files electronically, they must be sent either encrypted or via a UCPH system that has been approved for this purpose, for example, SIF.

You can find the UCPH standard template for data processing agreements on KUnet.

The data processing agreement and the Risk Assessment must be signed by the head of department.

The data processing agreements that have been entered into before the start of the project must be attached to the registration form that is to be completed when registering the project. Data processing agreements and the Risk Assessment entered into during the project must be archived in accordance with the procedure for filing documents on the research project case in case group 514 (in Danish only).

If there is any doubt related to data processing, you can always contact either the in-house counsel or the Tech Transfer Office (TTO email: techtrans@adm.ku.dk) provided that the TTO has negotiated the cooperation agreement to which the data processing agreement is related.



General data processing agreements
UCPH has entered into a number of general data processing agreements. If such an agreement exists, it is not necessary to enter an additional data processing agreement.

Read about the general data processing agreements that UCPH has entered into. Among others, UCPH has an agreement with the Danish Health Data Authority on the Research Machine, with Statistics Denmark on access to pseudonymised personal data via their microdata schemes; with the Technical University of Denmark on the use of Computerome 2.0 and a general data processing agreement with the Capital Region of Denmark. Processing data under the general data processing agreement with the Capital Region of Denmark (Region Hovedstaden) it is still necessary to exchange specific instructions if the Capital Region of Denmark is the data processor for UCPH. Find template for the specific instruction here.

Where UCPH is data processor for an external data controller
If UCPH processes data on behalf of others, a data processing agreement between the data controller and UCPH must likewise be entered into. UCPH must process data in accordance with the data controller's instructions, and the data must be processed – including stored – in accordance with the University's information security guidelines.

The data processing agreement must be recorded in Workzone under case group 515. UCPH must process data in accordance with the data controller's instructions, and the data must be processed in accordance with the rules on information security. Read more about UCPH as data processor. Read more about UCPH as data processor.

A general data processing agreement has been entered into concerning the processing of personal data for the Capital Region of Denmark. If you process personal data for the Capital Region of Denmark, you will receive instructions that must be uploaded along with the registration form that can be found on KUnet: UCPH's general data processing agreements and collaborations – KUnet.

Students, visiting researchers and other loosely affiliated persons
When a student, a visiting researcher or another loosely affiliated person works with personal data, it must be clarified who the data controller is – UCPH or the student, the visiting researcher or another loosely affiliated person.

If the student, visiting researcher or other loosely affiliated person collects and processes personally identifiable data by, for example, sending out questionnaires or by obtaining data directly from the test subjects, the person in question is an independent data controller. On the study pages, all students can read about the processing of personal data – including what they must do if they are the data controller. See an example of a specific study page.

If the student, guest researcher or other loosely affiliated person needs access to personal data from a research project where UCPH is the data controller, an agreement must always be entered into. Depending on the specific situation, this may be either 1) a guest declaration including a data processing agreement, 2) a guest declaration without data processing or 3) an agreement on the disclosure of data.

1. Guest declaration including data processing agreement: UCPH is the data controller and the student, the visiting researcher or other loosely affiliated person acts on instructions. The template for the agreement can be found on KUnet and is referred to as a guest declaration with data processing agreement. The agreement regulates the research project tasks of the student, visiting researcher or the other loosely affiliated person and imposes an obligation of confidentiality on the student, visiting researcher or loosely affiliated person in relation to personal data and other confidential information.

2. Guest declaration without data processing: If personal data is not going to be processed, the template 'guest declaration' is to be used even if the student, visiting researcher or loosely affiliated person has access to see personal data in the project. It appears from the guest declaration that data from the project must be treated confidentially. The agreement also includes a regulation of the rights to the results that the student, the visiting researcher or the loosely affiliated person creates during their affiliation with the research project. Results and inventions will belong to the student, visiting researcher or loosely affiliated person if a guest declaration has not been made.

3. Agreement on disclosure: In cases of disclosure of personally identifiable data to the student, visiting researcher or other loosely affiliated person, it must be ensured beforehand that such disclosure is lawful in accordance with the rules set out in the General Data Protection Regulation and the Danish Data Protection Act. Read more about sharing and disclosure of research data.

PLEASE NOTE:

› For scholarships – If attaching a student with a scholarship to the project – the following procedure must be followed (in Danish only).

› For administrative extensions of PhD students – When a PhD student's employment ends and the PhD student still needs access to the faculty/department's systems, an administrative extension must be made. At SUND and SCIENCE, such a contract is currently being incorporated into the administrative system PhD Planner. Be sure to check whether this implementation in PhD Planner has been activated. Otherwise, please contact your respective PhD Office.

Points of special attention in relation to students, visiting researchers and other loosely affiliated persons

› Data processing may only be done using IT equipment that complies with the University of Copenhagen's requirements for security, including password protection requirements. Also remember to do a risk assesment if processing is not done on UCPH equipment. Read more about information security.

› If, in connection with the data processing assignment, it becomes necessary to send sensitive or confidential personal data by email, this must be done by the loosely affiliated person using a KUmail to send the email to the project manager's (or others') KUmail. The loosely affiliated person must not send the personal data to any other email addresses, and the loosely affiliated person is therefore also obliged to demand that their KUmail account is not set up so that emails are automatically forwarded to another email address.

› All communication about the project with respondents/test subjects shall be done by using KUmail. Sensitive and confidential communication shall be send encrypted. You are not allowed to use or forward to gmail/hotmail/messenger/facebook or unsecure means of communication.

› Data storage media (e.g. USB keys) and prints must be stored securely and must, where technically feasible, be protected by passwords, so that they are not accessible to unauthorised persons. USB keys must be encrypted.

— For students

› Students can share data files via OneDrive. See the guide (in Danish only) – including encryption instructions.

› Before students start processing personal data in their projects, they must read the guidelines on KUnet. All

students can read about the processing of personal data on the study pages. The guidelines are relevant regardless of whether the students are to assist in the handling of personal data in an ongoing project, to be provided with personal data from a previous project or do their own project.

› All students working with personal data shall also complete the on-line GDPR course found on the KUnet.

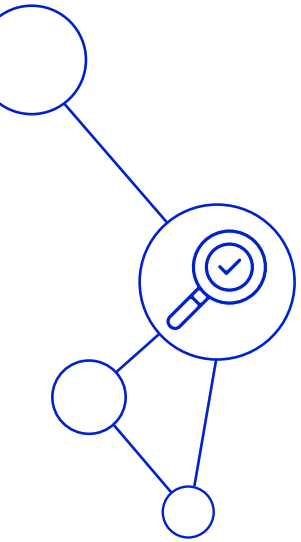
› If entering a guest declaration including data processing agreement with a student, the agreement must be negotiated and entered into before access to the data is provided.

Data processors in non-secure third countries
Research data may only be shared – including transferred to a scientific journal – with researchers in countries outside the EU/EEA if there are a legal basis. Read more about sharing personal data with parties in countries outside the EU/EEA.

Duty of notification and research with and without GDPR consent

TOPICS

- Duty of notification and research without GDPR consent
- Duty of notification and research with GDPR consent
- Few exceptions from the duty of notification
- Disclosure of personally identifiable data without consent



Processing personal data you need a legal basis for the processing. Two main possibilities within the area of research are "research without GDPR consent" and "research with GDPR consent". Below you can read more about the difference between the two possibilities.

You always have to consider the best solution for your research project and the integrity of the respondents/test subjects. Both possibilities come with limitations.

Regardless of whether or not a GDPR consent is used as a basis for processing data in a research project, you have a duty of notification towards the respondents/test subjects. The information sheet (duty of notification) has to be adapted to fit the specific project. You can use the information sheet (duty of notification) available on KUnet.

If you work with kids or other vulnerable groups the assessment in regard to conducting research with or without consent is important also from a research ethical point of view. If in doubt please seek further information.

Duty of notification and research without GDPR consent
The General Data Protection Regulation also facilitates the collection and processing of personal data in research projects without obtaining the participants' consent to processing personal data. Research data collected without consent may only be used for research and statistics.

If you assess that the personal data in the research project is to be processed without consent, you still have an obligation to provide the participants with a range of information under the personal data protection rules. Read more about the duty of notification and find the information sheet to be used for the duty of notification.

Duty of notification and research with GDPR consent
As a general rule, personal data can be processed once the respondent/test subject has given their informed consent.

This means that the respondent/test subject must be aware of what they consent to. You must therefore make clear what information is collected and used, the purpose of the processing, any recipients of data (e.g. partners or data processors) including all planned and future processing. When the processing of personal data is based on consent, it is important to obtain consent to all of the processing activities included in the research project, including transfer to partners within the EU/EEA or partners in countries outside the EU/EEA. If personal data from the project is to be used for other purposes after the completion of the project, e.g., for teaching students, this information must also be included in the consent.

E.g. if the GDPR consent allows sharing of research data or subsequent reuse of research data in new projects within related research, disclosure or reuse of data is possible without renewed consent. Read more about consent and the duty of notification/the content of the duty of notification.

When interpreting the scope of the consent, it is important to include other material given to the participants in the experiment, as this material may contain information about sharing or disclosure of personal data that can either

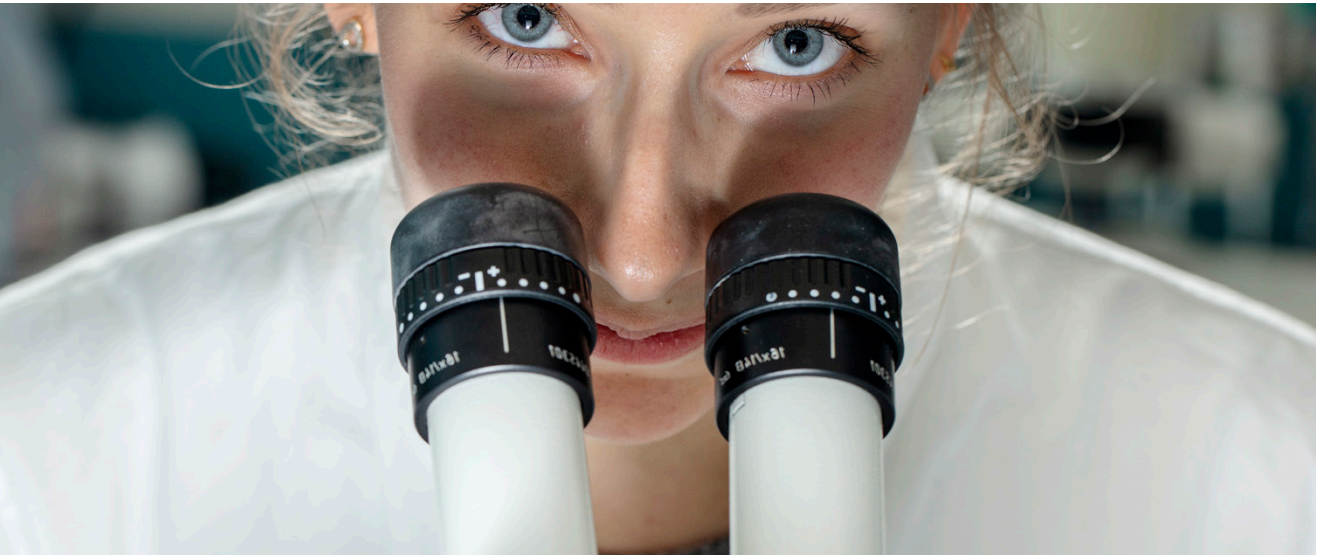
support or prevent the lawfulness of the sharing or reuse of data. **If in doubt, please ask the in-house counsel.**

In addition to the GDPR consent, health science research projects that must be approved by VEK shall also have a declaration of consent (VEK consent) that shall be approved by VEK.

The VEK consent is the informed consent in which the respondent/test subject consents to participating in the specific project on an informed basis, but thereby also implicitly consents to the processing of their personal data and/or biological material (the research biobank) in connection with the project.

The GDPR consent that is used for research projects that process personal data on the basis of a consent includes the respondent/test subject's consent(s) to specific and specified data processing so that their data can be processed in compliance with the GDPR. Read more and find templates for GDPR consent and information sheet (duty of notification) on KUnet.

Few exceptions from the duty of notification
There are a few exceptions for when the duty of notification does not apply, for example, if it would be impossible or require a disproportionate amount of effort to provide the information or if the information would significantly prevent the purpose of the project being fulfilled – for example, when using data from a database (registerdata).



Disclosure of personally identifiable data without renewed consent
— Data from a database (registerdata)
If the personal data is from an approved/lawfully collected register/database or from an approved/lawfully collected biobank, research data may be shared without renewed consent of the respondent/test subject.

Research into health data from genetic registers and in image diagnostic material have to be approved by the Danish Committee on Health Research Ethics.

When biological material from a biobank is to be used in a new health science project, the new project must be notified to VEK as a database research project with biological material. When applying for approval of the new project, you also lodge an application with VEK for an exemption from obtaining a VEK consent from the test subjects.

The processing of data in a new project must always be approved as a new project at UCPH.

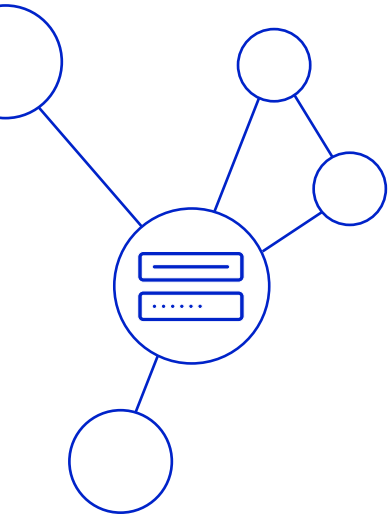
— Sensitive data
In order to process sensitive data without the consent of the data subjects, the following conditions must be met: Processing must be proportionate to the aim pursued, the processing respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. In addition, data must be processed in pseudonymised form, and the principle of data minimisation must be applied.

Sensitive data is information relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, state of health, sex life or sexual orientation.

Storage of physical (including printed) and electronic documents

TOPICS

- Storage of electronic documents
- S-drive, personal network drive, SIF and other secure storage
- Storage of physical documents



Data preservation/data archiving/storage of data is the act of ensuring that research data are kept long-term (years to decades) in a way in which they remain available and usable to the persons who should have access to the data. Read more about UCPH Policy of research data management and Data preservation.

Storage of electronic documents
— S-drive, personal network drive, SIF and other secure storage
Strict security requirements apply when handling, processing, sharing and storing personal data electronically. Files containing personally identifiable data such as name, address, email, CPR number, telephone number or other information that can identify the data subject at the individual level must be stored on the S-drive, a personal network drive, SIF or at a similarly secure location until the personally identifiable data can be erased and the project anonymised. Read more on the research portal about safe storage of personally identifiable research data: Safe storage of personal data and biological material – KUnet.

If using solutions other than those mentioned on the research portal, this use must be approved by UCPH IT/Information Security. Examples of electronic files containing personally identifiable information:

- Pre-screening forms
- Email correspondence (the email that contains sensitive information about a respondent/test subject must be erased from Outlook after 30 days at the latest).
  Read more about the storage of personal data
- ID logs (if relevant, screening/randomisation logs)
- Master data sheets
- Images
- Video/audio files
- Other

Storage of physical documents
All physical – including printed – documents that contain personally identifiable personal data such as name, CPR number, address, email, telephone or anything else that can identify the respondent/test subject at the individual level must be stored in a place locked with a special key during the entire processing period until the project is anonymised and shredded, so that no unauthorised persons have access to it.

A place locked with a special key could e.g. be a room that can only be accessed by less than five people. If more than five people have access to the room, the key to the room is a "common key" – meaning that physical – including printed – documents must be placed in a cupboard/drawer that can only be unlocked with a special key and separated from the printed documents containing pseudonymised data. Printed documents containing pseudonymised data could be:

- CRF/working papers
- Questionnaires and diaries
- Medical history, concomitant medications, adverse events, etc.
- Prints from various devices (e.g. DXA, ECG)

Example of physical documents containing personally identifiable data:

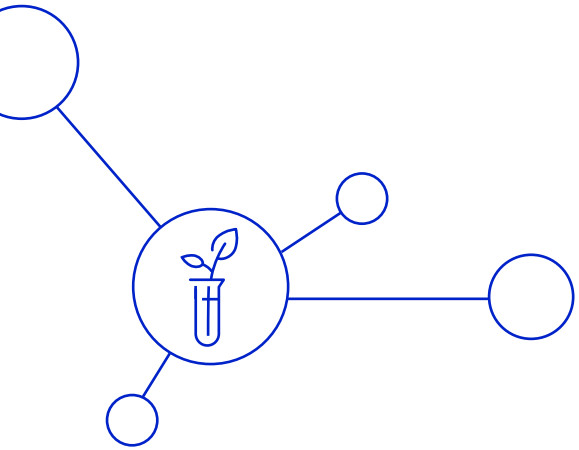
- Pre-screening forms (the form must be shredded if the person is found not suitable for screening in the pre-screening). Note the number (consort guidelines)
- Printed email correspondence (the email containing information about the person must be deleted in Outlook at the latest after 30 days)
- ID logs (if relevant, screening/randomisation logs)
- Master data sheets
- VEK declarations of consent
- Power of attorney statements
- GDPR (biobank) declarations of consent
- Images
- Video/audio recordings
- Other

Read more on KUnet about the storage of personally identifiable research data: Safe storage of personal data and biological material – KUnet.

Biological material is personal data and therefore subject to the GDPR

TOPICS

- Biological material
- Research biobank
- Biobank for future research



Biological material
Biological material, e.g., blood, saliva, biopsies, urine and faeces, is personal data and is subject to the GDPR. The processing of biological material, including handling, sharing and storage, must therefore be in accordance with the same rules that apply to personal data in printed and electronic documents.

Read more on KUnet about the storage of personally identifiable research data: Safe storage of personal data and biological material – KUnet.

Containers with biological material must be pseudonymised so that respondent/test subject cannot be identified based on the sample alone.

Until destroyed, the material must be stored at the correct temperature in a locked freezer without access for unauthorised persons. The temperature in the freezer must be monitored to ensure the quality of the sample. This must be documented and critical deviations such as thawing must be registered.

Biological material may only be sent to external parties in pseudonymised form and the ID log/key for the code must never be handed over.

In clinical studies, a distinction must be made between 'research biobank' and 'biobank'.

Research biobank
The research biobank is the biological material collected for analysis in connection with the specific trial/protocol/project.

While the study is in progress, applications for approval of new analyses can be made to VEK using a supplementary protocol.

The biological material in the research biobank must be handled in pseudonymised form from collection until destruction.

When all analyses described in the protocol have been performed and quality assured, the research biobank must be destroyed. Destruction must take place no later than at the time specified in the approved protocol under 'Biological material'.

The material in the research biobank must be stored at the appropriate temperature in locked freezers, connected to an alarm and temperature monitoring, in locked rooms. Any surplus material can be transferred to the biobank provided that the test subject has consented to the donation of excess material to future research projects.

Biobank for future research
The biobank is the biological material stored for use in new future research projects. It can be either the excess material from the research biobank or extra material

collected only for the purpose of usage in future research projects.

The biological material may only be stored in a biobank provided that the respondent/test subject has given a consent.

Before being initiated, database research projects that include biological material from the biobank must be registered in UCPH's data processing records and the protocol must be approved by VEK as a database research project with biological material. At the same time, you also lodge an application with VEK for an exemption for obtaining new consent from the test subjects.

The material in the biobank must be stored at the appropriate temperature in locked freezers, connected to an alarm and temperature monitoring, in locked rooms.
The material in the biobank may be stored for as long as the respondent/test subject has consented to.

If personal data from the project is going to be anonymised before the consent to the storage of the material in the biobank expires, the PI /project manager must ensure that the material in the biobank is also anonymised.

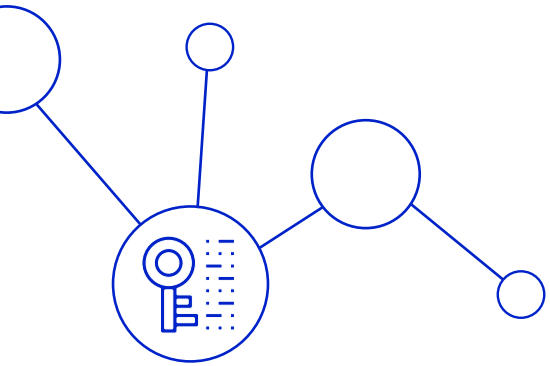
As the interpretation of the law is right now, biological material can be irreversibly anonymised and will, after the anonymisation, no longer be subject to various legislation and research into the material may be done without regulatory approvals.

Read SUND's guidelines for biobanks on KUnet.

Pseudonymisation – Confidentiality and security

TOPICS

› Pseudonymisation
› ID log



Pseudonymisation

In order to ensure the respondent's/test subject's confidentiality and security, their data in both printed and electronic documents and their biological material must, as far as possible, only be processed in pseudonymised form from collection until anonymisation/erasure.

From the outset, you must assign a code (a unique project ID number) to the respondents/test subjects, and subsequently, the code must be the only thing identifying them in, printed and electronic documents containing data and on the containers containing their biological material.

The respondent's/test subject's personally identifiable data, including name, CPR number (social security number), address, email, phone number or anything else that can identify them at an individual level, may only appear in the ID log in which the data is associated with the code.

For data files and containers with biological material to be properly pseudonymised, it is a requirement that they can only be traced to the person using the additional tools (ID log/the key to the code).

Pseudonymised printed documents, including:

› CRF/working papers
› Questionnaires, VAS and diaries
› Medical history, concomitant medications, adverse events, etc.
› DXA prints

may be stored in locked offices or locked cabinets, but never together with ID logs or other printed documents that contain personally identifiable data and that may be used to decode the pseudonymised data.

Electronic documents that are pseudonymised and where the respondent's/test subject's is only identified via a code may be stored on the I-drive/N-drive/shared drive that only employees with a legitimate purpose can access.

The folder must be password protected and the password may only be disclosed on a need to know basis. For the purposes of futureproofing of the access to retrieve data it is suggested that more than one person has the password; e.g. PI/Project Manager and Head of Department. If electronical means are used for storage of the password, please be aware of the user right/access right.

If the data and the ID log are stored in the same office, only a few authorised persons must have the key to the office. If the office can be unlocked with a shared key that all the employees have, the ID log must be stored in a cabinet locked with a special key.

ID log

The ID log is the document that connects the test-specific ID to the personal data, such as name, address, CPR number (social security number), email, telephone number, etc.

The ID log must be implemented from the start of the project and must be updated continually as test subjects are screened and given a test-specific ID code.

Code examples:

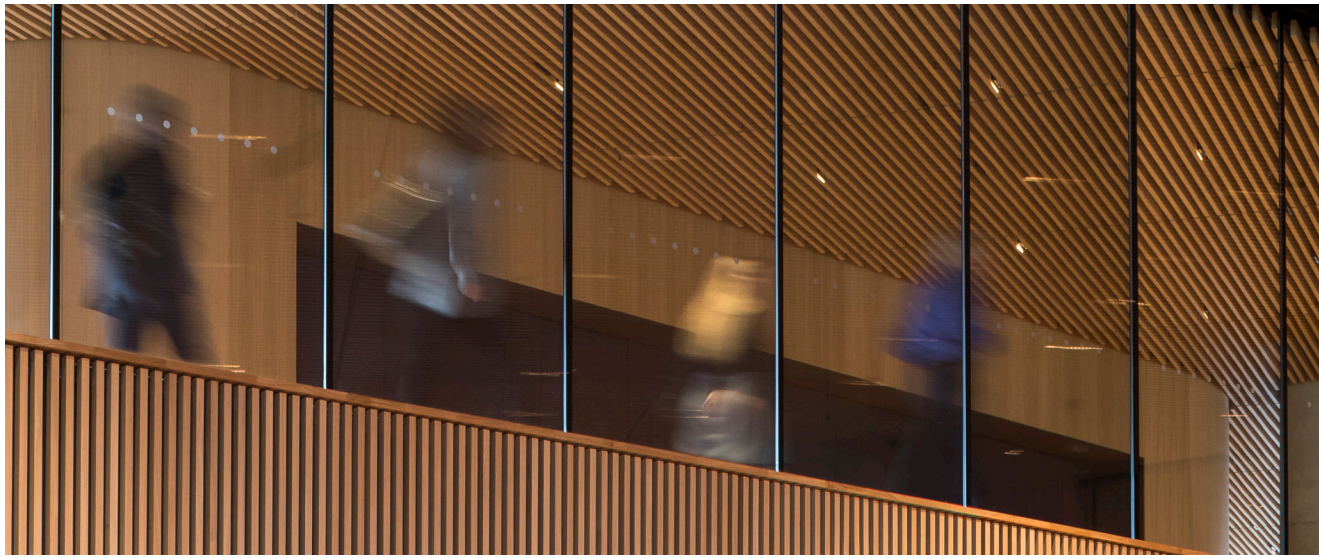
1. Initials + date of birth (the latter of the two, however, only in cases where it is strictly necessary, e.g. for DXA scans)
2. A random number or a number code
3. Screening/randomisation number

If the ID log is an electronic file, it must be stored in a secure location throughout the entire processing period so that unauthorised persons cannot access it.

If the ID log is a printed document, it must be stored, throughout the entire processing period, in a location where unauthorised persons cannot access it: For example, rooms or cupboards that only authorised persons have the key to ID logs must never be handed over to third parties, for example, data processors and/or partners/sponsors.

The ID log must be shredded when the project is anonymised.

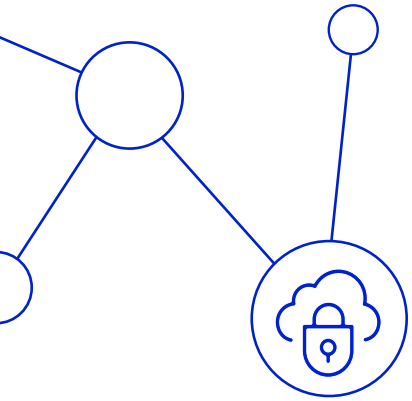
If you use randomization as coding tool it is strongly recommended that the randomization numbers /code you create is done in a way that you don't unlock all participants if you in case of emergency etc. have to identify a single participant



Uploading data to publicly available databases

TOPICS

› Uploading data to publicly available databases



Uploading data to publicly available databases
As a researcher, you will more often be encouraged to upload source data by:

› Grant donors – e.g. EU projects (FAIR)
› partners
› journals

When asked, the Danish Data Protection Authority (datatilsynet) has stated that if not covered by wording of the project purpose there is no legal basis for disclosing and uploading data to publicly available databases. It is there argumentation that the researcher/data controller cannot 'control' the use of the personal data if data is uploaded to a publicly available database.

It may be possible to upload data to publicly available databases if consent to this is given in the GDPR consent of the respondent/test subject.

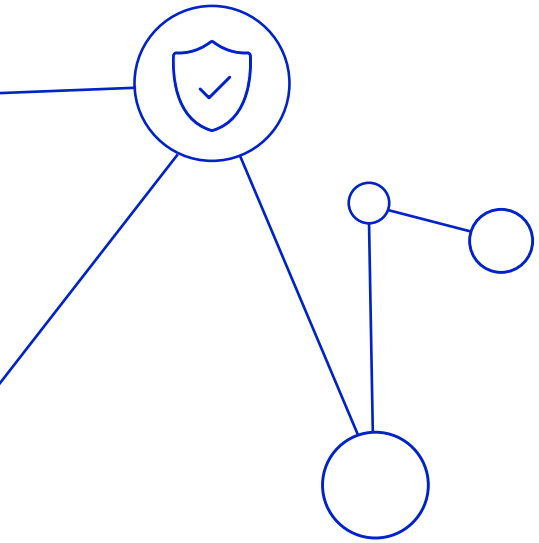
Consent must be voluntary, and the respondent/test subject must be able to choose or opt out of this option on the consent form so that it is not a condition for participating in the study. Please note that it may be a requirement from the grant donor (e.g., the FAIR principles) that data is transferred to a publicly available database, and in that case, consent must be obtained on basis of information given to the respondents/test subjects. It may therefore be a prerequisite for participation that the respondent/test subject consents to this.

Once the data has been **irreversibly** anonymised, the data may be uploaded without consent.

Anonymisation

TOPICS

› Anonymisation
› Data has been anonymised when



Anonymisation
When the UCPH registration of the research project expires, the data/biological material must be anonymised.

› All printed documents containing personal data must be shredded, including:

1. The ID list
2. Pre-screening forms
3. Master data sheets
4. Declarations of consent and power of attorney statements. In the case of printed documents, additional to what is mentioned above, that appear to contain personally identifiable data, for example, food diaries, VAS, questionnaires, printed email correspondences, lab forms, these must either be shredded or manually anonymised by tearing or blacking out all personal data.

› Project staff who have participated in the processing of the respondent/test subject and/or their data must be informed that the project will be anonymised and if they have documents from the project containing personally identifiable data, either in printed documents or in electronic files on their H-drive, these MUST be shredded/erased.

› All project folders containing pseudonymised data files must be double checked for personally identifiable data.

› It must be double checked that personal data has been deleted in external systems (for example, MADLOG, EasyTrial or the like).

› The project folder on the S-drive must be reviewed. If there are still files that need to be saved, they must be completely cleared of personally identifiable data and moved.

› The project folder on S-drive must be deleted, including all files containing personally identifiable data, and UCPH IT must be asked to delete the S-drive, unless it is used for a new project. It is not possible to use an S-drive for multiple simultaneous projects, as doing so gives people with access to the S-drive access to data that they do not have a legitimate need to use.

› If biological material from the respondent/test subject has been transferred to the biobank, the person in question must be informed that the project has been anonymised.

Data has been anonymised when
Data has been anonymised when all identifiable personal data has been destroyed and it is no longer possible to retrieve the identity of the respondent/test subject.

Anonymous data and/or biological material is no longer categorised as personal data and is therefore no longer regulated by the GDPR or other legislation.

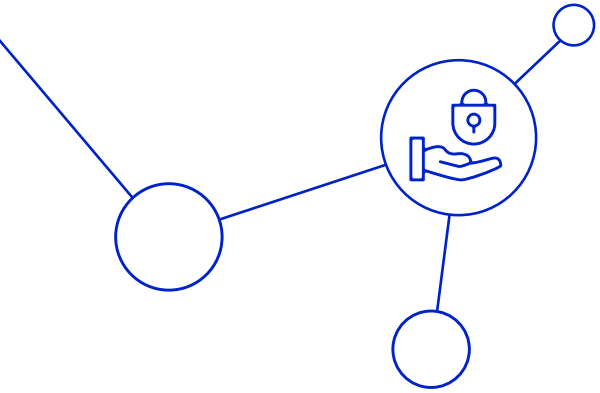
Anonymous data may be shared freely and used for research without the approvals of various authorities.

When anonymisating data take into the consideration what has been agreed in the Data Management Plan.

Breaches of security and future-proofing access to data

TOPICS

› Breaches of security
› Future-proofing access to data



Breaches of security

Both during and after the project, the PI/project manager is obliged to react if there is a security breach, for example, if:

› Sensitive or confidential personal data is leaked and ends up with unauthorised persons accidentally or through theft or hacking.
› Personal identifiable data has been made public available without the data subject's consent, e.g. on a website.
› A freezer breaks down to such an extent and for such a duration that the biological material has been spoiled and must be destroyed.

In the event of a breach of personal data security, you shall use this form for reporting. Handling of security incidents – KUnet. You can also read about when to inform the people affected by the personal data breach about the breach.

PLEASE NOTE

Remember to brief the local Information Security Officer:

› SCIENCE: Your Local Information Security Committee (LISU) member – see the overview here (in Danish only)
› SUND: Send an email to informationssikkerhed@sund.ku.dk.

Future-proofing access to data

It is important that the PI/project manager makes sure to future-proof the access to ongoing and completed projects. in accordance with the project Data Management Plans. All relevant information, status, documents and research data must be disclosed in a responsible manner and in a manner that allows the work to be continued.

Future-proof the access to data shall be done in order to protect the information from any sudden changes in the PI's/project managers personal circumstances, including death, long-term illness, termination or long-term leave.

At a minimum, continual decisions regarding the following points must be made:

› The status of tasks and areas of responsibility, including where the responsibility for current and completed projects is placed.
› An agreement on continued permission to use the research data and the procedure for the practical circumstances associated with it, such as access to UCPH servers and UCPH email account, permissions from VEK and UCPH, etc.
  › Source data and other essential documents from both completed projects and current projects must be up-to-date, intelligible and stored in such a way that they are available and can be found.
› The status and planning of future responsibility for the supervision of PhD students and other students.
› It is strongly recommended to set up your manager (e.g. the head of section) as a user on all electronic platforms where data is stored.

There may be department-based administrative procedures /agreements in this area that must be followed. Always make sure to check this with your manager/department administrator.

Read more about research data management at UCPH.

Local contact persons

SCIENCE
Generally, you can contact the in-house counsel at SCIENCE at jura@science.ku.dk.
If you are from NEXS, you can also contact GCP Coordinator Lene Stevner.

SUND
You can contact the in-house counsel at SUND at sund-hr-husjurist@sund.ku.dk

Local contact Persons
Department of Experimental Medicine – Birgitte Bagge Verium/Peter Bollen
Department of Biomedical Sciences – Filip Skovgaard Nielsen
BRIC – Susanne Nielsen/Christian Hestbæk
Centre for Translational Neuromedicine – Anne Helene Asklund/Ann Lee Berger Christensen
ReNEW – Helle Hegelund/Thomas Poulsen for HUB'en/Omar Khalidan
Department of Immunology and Microbiology – Johan Hellstrand
Department of Neuroscience – Anette Studsgård
GLOBE Institute – Sanne Louise Christoffersen
Department of Cellular and Molecular Medicine – Mette Kjær Schou/Mette Vase
Department of Pharmacy – Birthe Wielandt Houe/Jane Elvekjær
Department of Public Health – Bibi Trommer Ahlfors
Department of Veterinary Clinical Sciences – Camilla Louise Høgenhav Mikkelsen
Department of Drug Design and Pharmacology – Birthe Wielandt Houe/Jane Elvekjær
Department of Veterinary and Animal Sciences – no contact person
School of Oral Health Care – Annika Thrane Sørensen
Novo Nordisk Foundation Center for Basic Metabolic Research – Stina Lerche Serup
Novo Nordisk Foundation Center for Protein Research (CPR) – Nina Lynge
Department of Odontology – Maria Julie Kvetny
Department of Forensic Medicine – Stéphanie Maria Palombi

Abbreviations and glossary

Anonymous data	Data files containing a person's measurement results are also considered personal data. No one, not even the researcher, must be able to link anonymous data to a natural person. The Danish Data Protection Agency refers to anonymisation as the removal of the possibility to identify individual persons in datasets – in other words, an irreversible de-identification.
Biobank	A structured collection of human biological material that is stored for the purpose of future unspecific research and which is accessible according to specific criteria and where data linked to the biological material is attributable to individual persons.
CRF	Case Report Form. A printed or electronic document intended for collecting, at trial subject level, the data specified in the protocol.
Data controller	The person who decides why (for what purpose) and how (with what tools) personal data is processed.
Data processor	Processes personal data on behalf of the data controller – that is, on instructions from the data controller.
External party	External party refers to a non-UCPH employee, for example, a bachelor or master's degree student or an external institution/company.
GCP	Good Clinical Practice.
GDPR	General Data Protection Regulation
ID log	The printed or electronic document that connects the test subject's personally identifiable data with the unique trial ID number.
LMS	The Danish Medicines Agency.
Loosely affiliated person	All non-employees – for example, students becoming affiliated with a project, scholarships, visiting researchers, emeritus professors, affiliate professors and affiliate associate professors as well as employees who have left their position and still need access to the University's systems.
NVK	The National Committee on Health Research Ethics.
Processing of personal data	Processing of personal data refers to all activities involving personal data from collection, analysis, sharing, disclosure, storage and erasure/anonymisation.

Abbreviations and glossary

Pseudonymised data	Pseudonymised data refers to data in which all personally identifiable information such as name, CPR number, address, email and telephone number have been replaced by a code, so it is not directly possible to identify the person behind the data. The pseudonymised data is still personal data because it can still be linked to one natural person.
Research biobank	A structured collection of human biological material that is stored for the purpose of a specific health science research project and which is accessible according to specific criteria and where data linked to the biological material is attributable to individual persons (Section 2 (13) of the Danish Act on Committees on Health Research Ethics).
TS	The test subject.
VEK	The Research Ethics Committee.
Workzone	WorkZone is the digital archiving, workflow and document management system at the University. See more here: https://kunet.ku.dk/arbejdsomraader/journalisering/Sider/default.aspx?searchHitHighlight=workzone