Samen aanjagen van vernieuwing

DISCLAIMER

This translation was produced using Deepl. The original document was written in Dutch. Please refer to this Dutch version in the event of any discrepancies in interpretation.

Guidance on personal data in research

A practical step-by-step guide for researchers in higher education on how to comply with the GDPR

Colophon

This document is intended as a practical guide for researchers in higher education and deals with the handling of personal data in research. It is intended as a tool to help comply with data protection legislation.

Intended for

This document is specifically intended for researchers in the education and research sector, as well as for data managers and privacy professionals who support and advise researchers.

Compilation and management

This document was produced after the Dutch Data Protection Authority ('AP') explicitly called on educational institutions and Data Protection Officers ('DPOs') in the sector, in its sector report, to collaborate on practical guidance[1] on how educational institutions should handle research data. This was achieved through SURF's Privacy Expertise Centre in collaboration with the multidisciplinary working group 'Personal Data in Research' ('PGO working group') and a review group comprising privacy and data professionals from the education sector (higher education). The AP has noted this initiative favourably.

Special thanks go to the working group members:
- Jan van den Berg, Data Protection Officer – Amsterdam University of Applied Sciences
- Iris Goes, Research Data Manager – Windesheim University of Applied Sciences, Almere/Zwolle
- Floor May-Smit, Data Protection Officer – NHL Stenden Leeuwarden
- Anita Polderdijk-Rijntjes, Data Protection Officer – Windesheim University of Applied Sciences Zwolle
- Maartje Ridder, Research Data Management Specialist – Amsterdam University of Applied Sciences

Helma de Boer, Lead at the Privacy Expertise Centre, contributed on behalf of SURF.

and to the review group:
- Sarah Coombs, Open Science Advisor – Saxion University of Applied Sciences, Deventer and DCC-PO
- Esther van der Ent, Data Protection Officer – HAN Arnhem/Nijmegen
- Esther Eisen-Tijssen, Data Steward – Windesheim University of Applied Sciences, Zwolle
- Marlon de Jong, Data Steward, Privacy & Data Protection, University of Groningen
- Anke van Gorp, Researcher and Privacy Officer – Utrecht University of Applied Sciences
- Jan-Willem Oordt, Chief Privacy Officer – University of Groningen
- Raoul Winkens, Data Protection Officer – Maastricht University

Licence

Version control

Version	By	Date	Explanation/change
1.0	PGO and PEC Working Group	28 November 2025	Initial draft
1.1	SURF in collaboration with the PGO Working Group	11 December 2025	Various minor corrections/clarifications/links
1.2	SURF based on feedback	5 March 2026	Various minor corrections/checklist appendix

[1] See also the Education Sector Overview 2021–2023↗ under the heading: 'Much uncertainty remains regarding research data' (page 4, last paragraph).

Table of contents

1 Introduction

Before you lies the guide Personal Data in Research 2025 (hereinafter 'guide'). This practical guide has been written for you, a researcher in higher education. It is designed to help you comply with data protection legislation, such as the General Data Protection Regulation (hereinafter 'GDPR') and the General Data Protection Regulation Implementation Act (hereinafter 'GDPRIA').

There is a need within the research community for clarity regarding the GDPR and its application. The Dutch Data Protection Authority (hereinafter 'DPA') also notes this in its Sector Overview for Education 2021–2023.[2] In this report, the DPA invites the sector to engage in dialogue regarding personal data in research. In the sector overview, the DPA refers to *'the need for clarity for researchers at (higher) education institutions on how to handle personal data in (scientific) research*'.

To provide this clarity, a working group has been set up by SURF's Privacy Expertise Centre with the aim of drafting this guide. This Personal Data in Research (PGO) working group consists of a multidisciplinary team bringing together expertise on the GDPR, data management and conducting research.

The PGO working group has opted for a guide to provide you, as a researcher, with *practical* guidance. The guide has been reviewed by SURF's privacy and security community, to which higher education institutions are affiliated. In informal consultations with the PGO working group, the AP has indicated its support for the working group's initiative and that the guide can make a positive contribution to addressing the uncertainty surrounding the handling of research data.

Scope

This guide applies to both:

- scientific research conducted by universities, and
- research focused on professional practice carried out by universities of applied sciences.

This covers both new datasets containing personal data (primary use) and the reuse of existing datasets (further or secondary use). In this guide, we define these terms as follows:

- Primary use is when, within the research, you collect personal data directly from the data subjects with a specific objective in mind.
- Secondary use is when you do not collect the personal data directly from the data subjects, or when the data was originally collected for a purpose or research project other than your current research project and you wish to use this data for further processing for research purposes. In this guide, we refer to this as *reuse*.[3]

[2] https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023

[3] Reusing research data that you have collected yourself in a particular study for another study also constitutes further or secondary use of personal data. In such cases, you are using personal data that was initially processed for a different purpose or research project. See onderzoektips.ugent.be

Special regime
In this guide, we assume that the research is being conducted at a university or university of applied sciences and falls under the special regime of the GDPR applicable to scientific research. The special regime means that:

- (sensitive) personal data[4] may be used for scientific research (compatible purpose);
- there are exceptions to the right to erasure if this prevents the research objective from being achieved
- and also that the right of access, rectification and the right to restriction of processing no longer apply, provided it can be guaranteed that the data can be used exclusively for scientific purposes.

In all cases, appropriate safeguards must be put in place to protect personal data.

Definition of scientific research (including practice-oriented research)
The GDPR does not provide a definition of scientific research. The term 'scientific research' under the GDPR must be interpreted broadly and also includes research funded from private sources.

For the purposes of this guide, we use the following definition of scientific research[5] (including practice-oriented research):

- Research in which personal data is processed.
- Relevant sector-specific standards for methodology and ethics apply, including the concepts of informed consent, accountability and oversight.
- The research is conducted with the aim of increasing collective knowledge and the well-being of society, rather than primarily serving one or more private interests.

[4] See commission.europa.eu what personal data is considered sensitive↗.

[5] See 20-01-06_opinion_research_en.pdf, p. 13↗.

Definition of personal data
This guide applies if you process *personal data* for your research, namely:

1. **all information:** data that has meaning in relation to a person, such as a name, telephone number, home address, information about health, political affiliation or IP address;
2. **about:** the information says something about someone;
3. **an identified or identifiable person:** being able to trace it directly or indirectly to an individual, or to identify a specific person;
4. **natural person:** data relating to a living person, for example, not relating to companies or someone who has died.

The concept of 'personal data' varies depending on the situation: information may constitute personal data for one person but not for another. Consider, for example, a vehicle registration number. Only if you have access to the RDW's vehicle registration database can you see under whose name a vehicle is registered.

Information may also not be traceable to an individual on its own, but may be traceable when combined with other information. It may also be the case that information is secured in such a way (for example, through masking or encryption) that the data can no longer be traced (easily). This is called pseudonymisation. In any case, the GDPR does not apply to anonymous data. If pseudonymisation has been carried out in such a way that it would require an unreasonable amount of effort (in terms of budget or technology) to trace the data back, then the data may no longer fall within the scope of the GDPR[6] . For more information on this, see step 2, section 2.4. Pseudonymisation and anonymisation.

There must also be *processing* of personal data. Anything that can be done with personal data counts as processing. This includes collecting, recording, organising, storing, updating or altering, retrieving, consulting, using, disclosing by transmission, disseminating, combining, anonymising, erasing or destroying.

Sensitive and special categories of personal data
The GDPR imposes stricter requirements on the processing of 'special categories of personal data'[7] , such as medical data or religious beliefs (see the glossary in Appendix 3). The adverse consequences are greater for research participants if this data is insufficiently protected. For the sake of convenience, we consistently refer to *'sensitive* data' in this guide, as there is also sensitive data (such as bank account numbers) that does not fall within the category of special categories of personal data, but which also requires extra protection.

⚠ Please note: processing special categories of personal data is prohibited unless an exception applies (see Article 9 of the GDPR and Article 24 of the UAVG).

[6] Guidelines on pseudonymisation: edpb_guidelines_202501_pseudonymisation_en.pdf ↗ Recital 26 of the GDPR sets out which factors are relevant in determining whether data should be considered anonymous.

[7] See Special categories of personal data ↗ | Dutch Data Protection Authority

⚠ Please note that the processing of (pseudonymised) citizen service numbers (BSN) is not permitted for scientific research within the context of universities and universities of applied sciences.

Criminal personal data
Criminal personal data is highly sensitive, but does not fall under the category of 'Special categories of personal data'. Special rules apply. Consult your privacy contact regarding the use of this type of data.

Purpose

The GDPR imposes an accountability obligation on institutions to demonstrate that they process personal data lawfully. For instance, the institution must be able to demonstrate that processing complies with the core principles of data protection. These are: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.

If you process personal data in your research, for example data from participants, it is your responsibility to comply with these principles and to demonstrate this compliance. In doing so, you protect the rights and freedoms of the research participants. Consider, for example, maintaining control over one's own data, and preventing discrimination, stigmatisation, exclusion, financial loss or physical harm.

There are also other reasons to comply with the GDPR:

- careful handling of data enhances the quality and reliability of your research and its results;
- careful handling of data maintains the trust of participants and the wider community in the research;
- breach of the GDPR can lead to reputational damage and negative media attention for your institution, faculty/academy and for yourself as a researcher;
- breaches of the GDPR may result in fines or claims for damages; and
- consortium partners, clients, funding bodies and/or publishers require compliance with the GDPR.

Applying the GDPR to research practice can be perceived as complex. The guidelines in this handbook help to alleviate this complexity, and applying them generally leads to more GDPR-compliant research and greater clarity in this regard.

Status and disclaimer

The guide has no formal legal status. It merely provides guidance and imposes no obligations. Institutions are, provided they have committed to doing so, bound by the most up-to-date versions of:
- the Code of Conduct on the Use of Personal Data in Scientific Research ↗ ; and
- the Dutch Code of Conduct on Scientific Integrity ↗ .

This guide is intended solely as a resource and an informative document. It is the responsibility of higher education institutions to process personal data in research lawfully and with due care in accordance with the GDPR, whether or not after seeking legal advice.

Guide

Following this introductory chapter, Chapter 2 provides a summary to help you handle personal data with care. The summary allows you to quickly see where in this guide you can find further information. Chapter 3 sets out the steps you need to follow to handle personal data with care throughout the research process. The appendices contain further information and resources.

This guide is reviewed periodically, at least once every three years or sooner if legal or other developments so require.

2 Summary for the researcher

Good preparation ensures a smooth start and progress of the research. It also means you know what to look out for if you need to make adjustments during the research. Steps 1 to 3 all fall within the preparatory phase. At the end of step 3, you can actually start the research. The summary below aligns with the approach based on Harvard's Data Lifecycle (see section 3).

Step 1 – Planning & Design

This is the preparatory phase in which you lay the foundations for the secure and responsible processing of personal data in your research. It is important in this phase that you choose the correct legal basis for working with personal data. You should also describe here how you will address various aspects of working with personal data (for example, the purpose of the research, which GDPR role applies, whether you will carry out a DPIA, and how you will inform participants).

Step 2 – Collection and Use

During this step in the preparation, you check the transparency towards the research participants. If you are working with consent in accordance with the GDPR (not ethical consent), you set out here how you will request that consent correctly and what you will do if someone withdraws their consent. You check that you are using secure means and you register the research with the processing register.

Step 3 – Storage & Management

In this phase, you will put the framework from steps 1 and 2 into practice, with an emphasis on access management and appropriate protection. You will also consider the possibility of working with anonymous or pseudonymous data. Furthermore, you will arrange the retention and destruction periods.

Step 4 – Analysis & Sharing

During this phase, you are actively engaged in your research. You continually check whether you are still working securely as circumstances change and whether you can already delete any personal data.

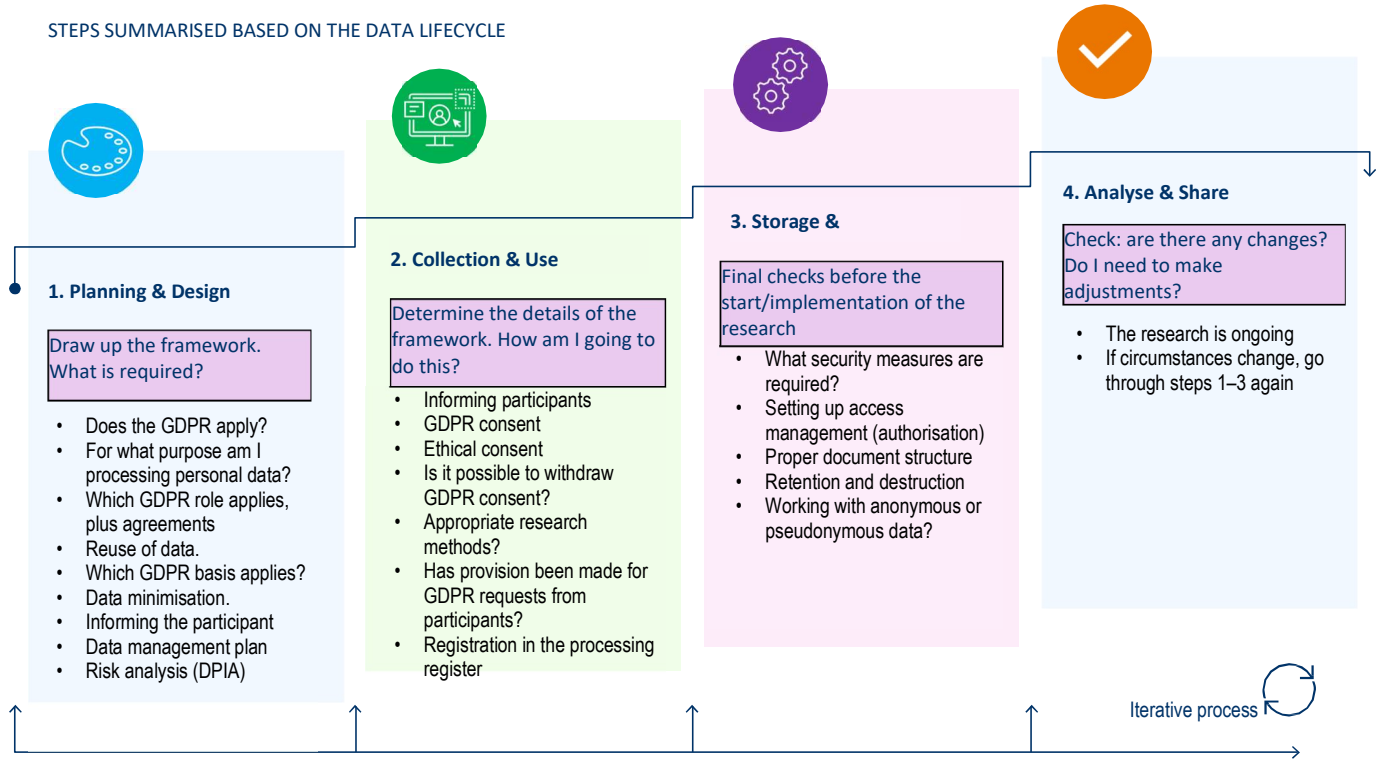
Step 5 – Evaluate and Archive

Step 5 is the final phase and focuses on archiving. Your research is complete and you will now begin to apply your retention and destruction periods. You must store any personal data that still needs to be retained in the correct manner and delete it where possible.

Step 6 – Publishing

In the final step, you move on to publishing your research. You ensure that no traceable personal data is published. If you wish to share the research dataset, you must ensure adequate anonymisation.

On the next page, you will find an overview of the points for steps 1 to 4.



Steps 1–4 deal specifically with working with personal data in research

Steps 5 and 6 cover completion; see the steps further on in the document (evaluation, archiving and publication).

See also the checklist in Appendix 5.

3 Steps for researchers

Data Lifecycle

This guide uses Harvard's Data Lifecycle for Research, illustrated in Figure 1.[8]

Figure 1: Harvard's Data Lifecycle.

[8] https://datamanagement.hms.harvard.edu/plan-design/biomedical-data-lifecycle ↗ See also Harvard Data Lifecycle – Information Security & Data Privacy ↗ (Plan, Create/collect, Store, Use, Share, Archive/Destroy).

In this chapter, you will find the questions for responsible data use for each step of the lifecycle, which you can use to get started, with or without the help or advice of your internal or external advisers. The *lifecycle* within your institution may differ, but the step-by-step plan in this guide has been drawn up in general terms, so that you can also apply it – whether or not in a modified form or order – if you follow a different *lifecycle*. Some steps have been combined. In the centre of the circle in Figure 1 is 'Store & Manage'. You must review this component at every step.

Step 1: Planning & Design

1.1 Does the GDPR apply to my research?

Processing of personal data

First, you must determine whether the GDPR applies to your research. In the introduction, you will find information to help you establish whether *personal data* is involved and whether *processing* is taking place.

The GDPR applies only to personal data (which can be traced back to a natural person), and therefore not to data that cannot be traced back to individual persons. We refer to this as anonymous data. If you conclude that you are working with anonymous data, you do not need to follow this guidance. This also applies if you pseudonymise data in such a way that it would require a disproportionate amount of effort to trace it back to individual persons. Note: the GDPR also applies to the pseudonymisation and anonymisation of personal data. These are also forms of processing personal data.

⚠ Please note: true anonymisation or sufficient pseudonymisation is very difficult and goes far beyond simply removing names. Always check with your organisation's data protection officer to ensure you are doing this correctly. For more information on this, see step 2, section 2.4. Pseudonymisation and anonymisation.

Be aware that during your research, you may collect personal data that you do not need for your research itself, simply because you are involving people (even if you are not conducting research on individuals). Consider, for example, recordings of interviews in which, although you do not collect personal information, the interviewee may be recognisable on the recording (through their voice or the context), and this constitutes personal data. In such cases, the GDPR also applies and you must take measures to handle this data with care. For ease of reading, the guide refers to 'research participants', but this term should be interpreted more broadly: it covers all individuals whose personal data you process for your research.

Within or outside the EEA?

The GDPR applies[9] if you are conducting research as part of an institution based in the European Economic Area (EEA), i.e. in an EU country or Norway, Liechtenstein and Iceland. This also applies if your research involves personal data of people from outside this area or if you are conducting

[9] See Ghent University, GDPR: when does this legislation apply to my research?↗

research from outside the EEA on individuals within the EEA. Under certain circumstances, the GDPR also applies if you collaborate with parties based outside the EEA, such as a consortium with non-European educational institutions. Discuss and investigate with these parties whether the GDPR applies. If you exchange data outside the EEA, check with your organisation's data protection officer whether a Data Transfer Impact Assessment (DTIA) may also be required. This may lead to additional measures being required in step 2.

Does the GDPR apply to your research? If so, answer the questions in sections 1.2 to 1.12.

1.2 Which GDPR role applies?

Research often involves multiple parties. To determine your rights and obligations, you must establish which GDPR role applies. The following two roles are possible:

- **Data controller.** A data controller determines, either independently or jointly with another party, the purposes and means of the data processing (the 'how' and the 'why'). This party or these parties are fully responsible and liable for compliance with the GDPR.
- **Data processor.** A data processor is the party that processes personal data on behalf of (or, in other words, on the instructions of) the data controller. This party may only process data on the written instructions of the data controller and may not determine any essential aspects of the processing. Nor may the processor process the personal data for its own purposes. This party operates on the basis of the controller's legal basis and has limited liability. For example, the hosting provider where you store your research data is a processor. See also the examples below.

Table 2 sets out a number of common scenarios.

Situation	**GDPR role Data controller**	**GDPR role Joint controller**	**GDPR role Processor**
Research conducted by a higher education institution	Higher education institution, for example when it draws up the research plan and liaises with participants.	You are a sole data controller if you pursue your own purpose and determine the means to achieve it. If, within a partnership, you determine the means jointly but each of the collaborating parties pursues its own objective, then you are also considered independent data controllers	A party that assists with the implementation of your research is likely to be a processor. Examples include transcription services, parties that make audio or video recordings, and (server) hosting providers (Google Drive, Research Drive, M365).
Partnership between multiple higher education institutions	Higher education institution (s)	Depends on the situation. In a joint research project, where parties jointly determine the purpose and means to a greater or lesser	If your institution merely carries out the instructions of the other institution, and your institution therefore has little or no

Situation	GDPR role Data controller	GDPR role Joint controller	GDPR role Processor
		extent, there may be joint controllers.	(research) freedom to determine for itself what it wishes to achieve with the personal data, there is a high likelihood that your institution is a processor.

Diagram 2: Roles in research

NB If the other party is the lead organisation or has received a grant for the research, this does not automatically mean that your institution is a processor. This is a possibility, but this must be determined in more detail based on the actual circumstances surrounding the data processing (who determines the 'how' and 'why').

1.3 Have I entered into the correct agreement(s) with these parties?

Once you have clarified the roles of yourself and the other parties, it is important to make arrangements with these parties. Consider how both parties handle personal data with due care and what responsibilities each party has in this regard, what should happen in the event of a data breach, a request for access or erasure, and also who will communicate with the research participants or the Dutch Data Protection Authority and how.

If you are *a joint controller*, you must enter into a joint controller agreement (JCA). In this agreement, you set out your respective rights and obligations. You must also inform the research participants of the contents of this arrangement. An indication that the JCA is the appropriate form of agreement is the existence of a consortium agreement.

If you share data with another party that is *itself a data controller*, you must enter into a data exchange agreement (a 'DEA')[10] . This often specifies where one party's obligations end and the other's begin. It also covers the (secure) manner in which personal data is shared. Each party remains individually responsible for compliance with the GDPR.

If you *work with a processor (the party you need to process certain personal data on your behalf) or* if *you are a processor yourself*, you should set out the arrangements in a data processing agreement.

[10] Other terms used in this context are 'Data Sharing Agreement' and 'Data Transfer Agreement'.

In Appendix 4, you will find a decision tree to help you determine the division of roles and the agreements to be concluded.

Your privacy contact person can help you determine the correct role and conclude the appropriate agreements.

1.4 Do I have the correct legal basis for processing personal data?

To process personal data in your research, you need a legal basis. The legal bases are set out in the GDPR. It is important to know which legal basis applies to your research before you start. In principle, there is no hierarchy among the legal bases.

The processing of special categories of personal data is, in principle, not permitted, although the GDPR does allow for exceptions. If you process special categories of personal data, you may need to rely on one of the grounds for exception under the GDPR and/or the UAVG in addition to one of the legal bases listed below.[11]

Carefully consider the available options and what best suits your research. Below, we explain the relevant legal bases (public interest, consent and legitimate interest).

Legal basis: Public interest
The introduction provides a definition of scientific research as used in this guide. If you are conducting scientific research (including practice-oriented research), this falls under the public interest task assigned to universities and universities of applied sciences by law (the Higher Education and Research Act, hereinafter 'WHW'). If we look at the requirements set out in the WHW, the research must meet certain conditions in order to successfully invoke this legal basis for processing.

In short:

- As a university, you conduct fundamental or applied research under the supervision of a professor. As a university of applied sciences, you generally conduct research focused on professional practice under the supervision of a lecturer.
- Your research serves a public interest/does not have a primarily private purpose.
- Your research complies with the relevant methodological and ethical standards of the sector and is conducted in accordance with good practice (ethical research).

In these cases, you do not need to seek consent for the processing of personal data in your research in relation to the GDPR, unless you are using special categories of personal data for your research. In that case, check with your privacy contact person to see whether it is necessary to consider whether (, if so, how) consent can be sought, and, if necessary, arrange this at the same time as the ethical approval. In any case, stricter protection requirements apply to the use of special categories of personal data. Additional requirements also apply to requesting consent.

The 'public interest' legal basis may therefore also apply when you use sensitive data. However, you will likely need to take additional security measures to protect the rights of your research participants, but you do not always need to seek consent. Please contact your organisation's

[11] For practical examples of the grounds for exemption, seeonderzoektips.ugent.be/nl/tips/00001839/↗

privacy contact person regarding the implementation of additional measures and the process of seeking consent.

If your research meets the conditions for the GDPR legal basis of 'public interest task', you may deviate from certain obligations regarding the rights of your research participants, insofar as these restrictions are necessary to achieve the intended research objective. Discuss this with your organisation's data protection officer.

Legal basis: Requesting consent in accordance with GDPR requirements

It may be the case that the applicable legal basis is 'consent'. In that case, you must ask the data subject for consent (in addition to any ethical approval relating to (voluntary) participation in the research). You must do this correctly.

For a successful reliance on consent under the GDPR, you must meet four conditions; the consent must be:

- freely,
- unambiguous,
- informed, and
- specific.[12]

Free consent means that you must not put a research participant under pressure or disadvantage them when they withhold consent. You must also inform the participant in good time about the processing(es) and the possibility of withdrawing consent. It can be difficult to obtain free consent from vulnerable groups of people or from people in a dependent position (such as students, clients or patients) who may feel pressured to consent due to a power imbalance. Withdrawing consent means that you must stop processing the personal data. You must then delete it. If you are processing sensitive personal data, an extra strict test applies and explicit consent is required. Consult your organisation's data protection officer on how to request consent correctly.

Legal basis: Legitimate interest

In other cases, you may rely on the legal basis of legitimate interest. Legitimate interest as a basis for processing personal data for research purposes is unlikely to arise frequently. In such cases, you must carry out a three-step test[13] :

1. there is a *legitimate* interest on the part of the controller or a third party (an interest that does not conflict with the law). You must be able to identify this interest; and
2. there is a necessity for the processing of the personal data in order to pursue the legitimate interest. You must substantiate this necessity; and
3. The fundamental rights and freedoms of the participants do not take precedence. You must therefore weigh up the interests of the organisation conducting the research against those of the individuals concerned. The more sensitive the data or the more vulnerable the participants are, the greater the weight given to their interests. Ensure that you involve the Data Protection Officer (DPO) in the balancing of interests and that you document this assessment.

Data subjects also have the right to object to the processing.

[12] See Dutch Data Protection Authority, Legal basis: consent ↗

[13] See Dutch Data Protection Authority, Legitimate Interest ↗

You cannot use the legitimate interest basis if you process sensitive data in your research or for tasks that your institution carries out in the public interest (research).

Explanation of ethical consent

In addition to consent as a basis for processing personal data, ethical consent is also important: consent to participate in the research. To avoid confusion between 'informed consent' as referred to in the GDPR, and the term 'informed consent' which is also used for ethical consent, we consistently use 'ethical consent' here to indicate the difference.

Ethical consent is a measure designed to safeguard the right to human dignity and the right to human integrity.

Although both forms of consent can be combined, ethical consent is not subject to the same conditions as consent as a legal basis under the GDPR. If necessary, check with your organisation's ethics committee to find out what you need to take into account.
For research involving human subjects that falls under the Medical Research Act (WMO), there may be additional requirements for ethical consent. See also the website of the Central Committee on Research Involving Human Subjects (ccmo.nl ↗).

If you use consent as the legal basis for processing personal data under the GDPR, it is advisable to do so in the same form, but ensure that the distinction is clear.

Unlike 'consent as a legal basis for processing personal data', this ethical consent is not intended to ensure compliance with the GDPR. You can document both forms of consent using the same form, but the difference must be clear (and one does not automatically lead to the other).

1.5 Conditions and examples of legal bases

When you process personal data, you must also check whether it passes the necessity test (unless the legal basis of 'consent' applies, in which case this test is not required).

In doing so, you must consider proportionality and effectiveness:
- Does the processing of data achieve the stated purpose, or is that not certain?
- Is the legitimate purpose proportionate to the fact that personal data must be processed for this purpose?

And you must consider subsidiarity:
- Is this the best way to achieve it: can the objective not be achieved in another, less intrusive manner (with less infringement of privacy)?

In Table 3 you will find conditions and examples of legal bases:

Task in the public interest	**Conditions**	**Examples**
The processing of personal data for the purposes of scientific research or research aimed at professional practice may be based on the 'task in the public interest'. This task is laid down in the WHW. Not all research automatically falls under this.	• Your research is carried out by or under the supervision of a **professor or senior lecturer.** • You can demonstrate that the research **contributes to the advancement of knowledge and addresses a social issue**. • Your research **meets the relevant methodological and ethical standards of the sector and complies with good practice** (is **ethical**, for example through consultation with an ethics committee). • You have **put appropriate safeguards in place** for your research **so that the rights of participants are adequately protected**. The latter applies all the more if sensitive data is processed. For the final condition, see the other steps in this guide.	√ Research into poverty reduction or equal opportunities, health or well-being, sustainable energy, safety or entrepreneurship. You may process sensitive data for this purpose. X If the research is determined and funded by a commercial organisation for its own purposes, and this party cannot rely on this basis, then where possible choose 'Consent' as the legal basis. See also the GDPR division of roles. X Institutional research (research using the organisation's own data as part of its day-to-day operations).
Consent	**Conditions**	**Examples**
The legal basis of consent is also a basis that can be used in research.	• Your research does not fall within the scope of the public interest. • Consent is given through a clear, active act, for example via a written statement. • Consent must be **freely** given.	√ Commercial research, i.e. research where the increase in knowledge is in the interests of a commercial organisation rather than society. √ Research involving the processing of sensitive data that does not fall within the remit of the public interest.[14]

[14] In some cases – subject to certain conditions – special categories of personal data may be processed without seeking consent (see, for example, Article 24 of the UAVG). Consult your organisation's privacy contact person regarding this.

	• The data subject must **be informed** about the processing and the withdrawal of consent. • Consent must be sought **for each instance** of personal data **processing.** • Consent must be an **active act.** • You must be able to **demonstrate** that you have obtained consent. • Consent can be **withdrawn** at any time, so this must be **communicated** and you must establish a **process** for this.	√ Sharing your research data with other (research) parties for reuse if the compatibility assessment is negative. X Research involving (highly) vulnerable groups of participants or people in a dependent position if this prevents them from giving free consent.
Legitimate interest	**Conditions**	**Examples**
Sometimes it is possible to use the legitimate interest of your institution or a third party as the legal basis for processing data for research purposes.	• You must assess whether this is the best way to conduct the research • Your research **does not** fall **within the scope of the public interest.** • You can **identify** a **legitimate interest** (which must not conflict with the law). • You can **substantiate** the **necessity** of processing the data in relation to the legitimate interest; • You carry out a **balancing of interests** and the **interests of the participants do not prevail** (depending on the vulnerability of this group); • You **do not** process **sensitive personal data**	√ Commercial research, i.e. research where the increase in knowledge is in the interest of a commercial organisation and not primarily for society. √ Research with limited impact on the rights and freedoms of research participants, for example, by using little or very general personal data ( ). √ Secondary use/reuse, provided that appropriate safeguards are in place. X Research involving sensitive data. X Research involving (highly) vulnerable groups of participants. Whether a group is vulnerable depends on your research. Examples include children, the elderly, migrants, patients, people with disabilities, people who lack legal capacity, etc.

Table 3. Conditions and examples of legal bases

Consult your privacy contact person if you are unsure about your legal basis, how to properly justify it, or whether you are processing sensitive data.

1.6 Do I have a purpose for processing the data?

Purposes

You may only collect and use personal data for a specific and clearly defined purpose, in this case for your research. Further processing of personal data is, in principle, prohibited once you have achieved the defined processing purpose and further processing of the personal data serves a different purpose that is incompatible with the purpose you defined in advance.

Tips on purpose limitation

- ❑ Describe your research objective as specifically as possible so that you can determine which personal data you need for which purpose, either for or within the research (for example, for communicating with participants).
- ❑ Check whether the personal data you are requesting is truly necessary to achieve this objective.
- ❑ If you wish *to reuse* personal data *for the purposes of scientific research*, this is deemed to be compatible with the original purpose and you may use this data and even share it with third parties (unless you have relied on the 'consent' basis, in which case you may only reuse the data if you specifically requested this when obtaining consent). Please note that you must notify the participants of this potential reuse in advance. The compatibility test (see next bullet point) can then be omitted. However, you must:
  - make arrangements with the recipients of the data (see 1.3);
  - secure the personal data appropriately. Consider, for example, applying pseudonymisation, restricting access to the data, using encryption, or using secure storage . Your privacy contact person can tell you more about what is considered appropriate in your situation.
- ❑ If you *wish to reuse* personal data *for a purpose other than scientific research*, you must check whether this is permitted in relation to the original purpose of the processing. This is known as the compatibility test (Article 6(4) of the GDPR). You may only reuse personal data for a different purpose if this:
  - is based on the consent of the research participant;
  - the rights and freedoms of persons other than this participant are not compromised; and
  - the purposes of the further processing are compatible with the purposes for which you initially collected the personal data.

  You must assess whether the reuse falls within the expectations of the research participants. The following factors may play a role in this:
  - the connection between the original purpose and the new purpose;
  - the context in which the data were collected;
  - the type and nature of the data (does it concern sensitive data?);
  - the potential consequences of the reuse (what are the consequences for the participant?);
  - the existence of adequate technical and organisational measures (such as pseudonymisation).

  Does this use fall outside the participants' reasonable expectations? If so, you cannot reuse the data. Bear in mind that anonymising data for reuse also constitutes the processing of personal data. You must be transparent about this in advance.

1.7 Am I only requesting the data necessary for my research?

Before starting your research, you must consider whether you need personal data to answer your research question or whether anonymous data will suffice. And if you do need personal data, think carefully about *which* personal data is necessary. Keep the data to a minimum. You should only use the personal data you need to achieve your objective. This is known as *data minimisation*. It simplifies management and reduces the impact of a security breach.

By applying data minimisation, research participants can be assured that no more (sensitive) data about them will be processed. Furthermore, the risks associated with incorrect processing – for example, in the event of a hack or when data is sent to the wrong recipient – are reduced. And that benefits both the research participants and your institution.

So always ask yourself: do I actually need this data from this person to answer my research question? And if so, how detailed does this data need to be (or could you, for example, work with less data, such as year of birth instead of date)?

An example of this is if you wish to communicate with your research participant exclusively by telephone and email. In that case, it is not necessary to request a home address. Or, if you are conducting research into employees' digital resilience, it is not necessary to ask about trade union membership.

Adequate, relevant, necessary

To comply with data minimisation, you must ensure that the personal data is adequate and relevant and limited to what is necessary. This means the following:

- **Adequate –** Sufficient to enable you to carry out your research properly.
  ⚠ *Please note: this means you must not collect too much data, but also not too little. If you have collected too little data, you may not be able to answer your research question properly or you may have to follow this up later.*
- **Relevant –** The personal data has a rational connection to your research; and,
- **Limited to what is necessary –** You do not collect or retain more than you need for your research. This means you must also consider a retention period. See step 2.3 for more on this.

Tips on data minimisation

- ❑ Check as soon as possible whether, and if so, where in your research you can pseudonymise or anonymise data.
- ❑ Do not request more data than you need. For example, ask for the year of birth only and not the full date of birth; ask for place of residence rather than an address; process only the four digits of a postcode; use audio rather than video, etc.
- ❑ Where possible, use multiple-choice questions and as few open-ended questions as possible. The risk of traceability and, for example, stigmatisation is greater with open-ended questions (as they are more unique).
- ❑ Carry out the data minimisation check at every stage of your research. You may have initially needed certain personal data, but it may no longer be relevant.
- ❑ Also consider whether it is necessary for you to know who completed which questionnaire. If this is not the case, immediately decouple the answers from the respondent. This can be done,

for example, by sending respondents a general link to a questionnaire rather than a personal link (the same link for every respondent).

You can include all this information in your data management plan or research protocol.

1.8 Can or do I want to reuse (part of) the data or make it available for reuse?

It is wise to consider, during the planning phase of your research, whether you can or wish to share the data you are currently using for your research with other (research) parties, or whether you might wish to use it yourself later for scientific research.

Tips on reuse

- ❑ Check which data you want or can share for other research (see step 1.8 and step 4).
- ❑ Check whether the data can be anonymised (see step 2.4).
  If anonymisation is not possible, do not share more than the data necessary for the purpose for which you are sharing the data (see step 1.7).
- ❑ Assess the legal basis for this further processing:
  - If consent has been given for your research, consent must also have been given for its reuse for compatible purposes (see 'Tips on purpose limitation', 1.6).
  - If the data were collected in the performance of a task carried out in the public interest, this new research must also fall within the scope of that task. This also applies if you provide the data to other parties.
- ❑ Check whether the sharing of this data is within the expectations of the research participants.
- ❑ Ensure appropriate security for this data, preferably by applying pseudonymisation, restricting access to the data, applying encryption, ensuring secure storage and making agreements with the recipients of the data (step 2.4).
- ❑ State in the data management plan and the register of processing activities that you intend to reuse the data or share it with third parties for reuse. See step 1.11 and Appendix 1).

If you receive or share anonymised data – that is, data that neither you nor the other party can trace back to specific individuals – then the GDPR does not apply to you or that party. For more information on this, see Step 2: Storage & Management.

Do you have questions about the reuse of personal data and the practical implications this has for your research? Please contact your institution's data protection officer.

1.9 Am I informing participants correctly?

Research participants have a right to information. As a researcher, it is your responsibility to inform participants in a proper, understandable and transparent manner. This is usually done in the information letter and/or the consent form. In Step 3, the guide discusses in detail the method of providing prior information and the other conditions.

⚠ It is important to note here that you must not start processing personal data until you have informed the research participants (unless exceptions apply).

1.10 Do I need to carry out a DPIA?

A *data protection impact assessment* ('DPIA') is a tool that allows you to determine the impact of your intended data processing and to incorporate (and implement) risk-mitigating measures.

You may need to carry out a DPIA before you start your research. You should carry out a DPIA if the processing of this data *is likely* to pose a high risk to the rights and freedoms of the research participants.

Consider, for example:

- the processing of sensitive personal data, whether or not on a large scale;
- when you process data relating to vulnerable groups, such as children, employees, patients, people living below the poverty line, or people in a dependent position (such as patients or clients), etc.;
- whether combined datasets are involved, where the processing may not meet the expectations of some of the participants;
- whether you use new technologies (automated decision-making/AI).

Consult your privacy contact person to determine whether a DPIA is required. If this is the case, you must not begin processing the personal data until the assessment has been completed.

1.11 Does my data management plan comply with the GDPR?

Drawing up a data management plan ('DMP') is an essential step in planning and designing research involving the processing of personal data. A DMP encourages you to think carefully in advance about how personal data will be handled throughout the entire research process. It is important to include GDPR aspects in this plan.

Describe how you handle personal data and how you comply with the principles of the GDPR, such as lawfulness, transparency and data minimisation. For the purposes of the GDPR, it is important that you address at least the following aspects in the DMP:

1. Purpose of the research and risks
   You will determine what personal data you collect, why it is necessary, and how you can minimise the amount of data. You should also specify how you will obtain consent or on what other legal basis you will collect this data. You will have carried out a DPIA where necessary.
2. Storage
   You will specify how you store personal data securely. Check within your institution which tools and infrastructure are available for this purpose and follow the internal agreements on storage. Consider local systems and secure cloud environments, such as SURF Research Drive. In addition, where necessary, describe the additional technical and organisational measures you are taking to adequately protect data. Ask your privacy contact person for help.
3. Sharing (authorisation and access security)

You describe which individuals have access to data at which stage of the research. You specify with whom you share the data and why. You explain how you facilitate secure collaboration and data exchange, for example through encryption or anonymised datasets.

4. Storage and destruction
   You specify what happens to data during and after the research. How and when is data deleted and/or anonymised for archiving?

The DMP not only provides guidance for yourself, but also helps to demonstrate that you are taking measures to comply with the GDPR. A DMP is often also required by funding bodies or clients. Make the DMP a living document and adapt it as necessary during your research.

Would you like to know more about drawing up a DMP? Please consult the information pages, guidelines and templates available through your institution or research organisation, or contact your institution's data steward. You will find a DMP template in Appendix 1.

1.12 Research with/by students

If research is carried out by or with students, you must pay particular attention to the legal basis. If research is carried out solely for educational purposes, for example, you will probably not be able to rely on the 'public interest' legal basis.

Points to consider:

- Choose the correct legal basis;
- Determine how you wish to manage access (will students have access to all data, or will you restrict this?);
- Is a non-disclosure agreement perhaps required?

As a researcher, always ensure that students receive extra supervision during the research and clarify the ultimate responsibility of the supervisor.

Step 2: Collection & Use

In this phase, you will proceed to collect personal data and process it for your research. For this phase, there are five key questions you must first consider to ensure you handle the rights and freedoms of your research participants with due care.

2.1 How do I inform research participants about the use of their personal data in a manner that complies with the GDPR?

You must always inform research participants in good time (in advance) about how you will handle their personal data during and after your research (unless an exception applies). If you use consent as a legal basis, you must also provide additional information in order to lawfully rely on the legal basis of consent.

Tips for informing research participants

❑ **Provide the correct information, depending on where you obtained the data**
When providing this information to research participants, the GDPR distinguishes between whether you obtained the personal data directly from the participant or via another source. Consider, for example, reuse where you have received data from another party. Depending on this, you must provide certain information.

Table 5 sets out what information you must provide.

Information that must be provided to the participant in advance when you have obtained the personal data from:	**the participant**	**another source**
The identity and contact details of the institution or organisation on whose behalf you are conducting the research, and if that institution is not established in the EEA, the identity and contact details of that institution's representative in the European Union (EU).	√	√
The contact details of the data protection officer (DPO) of the institution or organisation on whose behalf you are conducting the research	√	√
Purposes of the processing of personal data as recorded in the register of processing activities and the GDPR basis. Is the GDPR basis legitimate interest? If so, please also state which interest is being relied upon.	√	√
The (categories of) recipients of the personal data. I.e. the details of organisations (recipients) and/or a description of the type of organisations (categories of recipients) with which personal data is shared or to which access to the personal data is granted	√	√
If you intend to transfer the personal data outside the EEA or to an international organisation, the legal basis on which this will be done.	√	√
The categories of data processed.		√
Retention periods, or, if this is not possible, the criteria for determining the periods.	√	√
The right of access, erasure, rectification, restriction, objection and portability. Please note: in the case of scientific research, some of these rights do not apply. Furthermore, the right to data portability applies only where the legal basis is 'performance of a contract' or 'consent'.	√	√
Where processing is based on the GDPR legal basis of consent: the right to withdraw consent at any time.	√	√
The right to lodge a complaint with the Dutch Data Protection Authority (AP).	√	√
Whether data subjects are legally or contractually obliged to provide the personal data and what the (possible) consequences are if the data subject does not provide the data. NB This is not always relevant to scientific research.	√	
Whether automated decision-making, including profiling, is used, how decisions are reached, and the right to an explanation from a human.	√	√

Information that must be provided to the participant in advance when you have obtained the personal data from:	the participant	another source
If you have received the data from another organisation: the source from which the personal data originates. And, where applicable, whether the data originates from public sources.		√

Table 5. Information for participants

- ❑ **Know when you do not need to inform research participants**
  You do not need to provide participants with information if they have already received the same information in the past. As a researcher, you must be able to demonstrate this.

- ❑ **Personal data from another source: sometimes it is not necessary to inform participants**
  If you have obtained personal data from another source, you do not need to provide the above information if:

  - this is impossible or would require a disproportionate amount of effort; or
  - the collection or provision of the data is required by law; or
  - the personal data must remain confidential due to a legal duty of professional secrecy (see Article 14 of the GDPR).

  It remains important that you make an effort to provide the information somewhere, for example via a newsletter or an interest group, and to publish it on a website.

  In the case of reuse, you do not need to inform the participant if:

  - the data subject already has the information; or
  - providing the information would require a disproportionate amount of effort, particularly in the case of processing for the purposes of scientific or historical research. When reusing pseudonymised data, informing data subjects about the new processing of their data is often not feasible. If this is not feasible, you must record why not, so that you can justify this if the supervisory authority requests it; or
  - if informing them would mean that you can no longer achieve the purpose of processing the personal data or if it would seriously jeopardise that purpose.

- ❑ **Provide information in a clear and comprehensible manner (in writing and, upon request, also verbally)**
  Participants must fully understand the content, including the information about the processing of their personal data. Check whether:

  - Dutch or English is the right choice of language for your target group, or whether another language or languages would be more appropriate (sign language may also be an option);
  - the language level is appropriate for your target group in terms of age, particularly where minors are involved; for example, use a tool that helps you write at language level B1[15] and use images where possible;

[15] See tips at communities.surf.nl↗ , paktaal.nl/taalniveaus ↗ and accessibility.nl/kennisbank/tools/leesniveau-tool↗

- the choice of words is appropriate for your target audience, for example, if your research focuses on vulnerable groups, university professors or government officials.

It is advisable to provide information in a layered manner: you provide the necessary information at the right time and no more than that. In this way, you avoid becoming less transparent due to an overload of information and prevent the person concerned from losing sight of the essentials and the bigger picture. Providing information in layers combines the requirement for brevity with the need to provide all necessary information.

- ❑ **Provide information free of charge**
  You may not charge for providing information.

- ❑ **Align the content of the information letter, the consent form (if applicable) and the data management plan**
  The information you provide to the participant must align with the internal process. Therefore, ensure that the various documents do not differ from one another, as otherwise adjustments will be necessary that could affect the risk assessment and the required measures, or the DMP may need to be amended.

- ❑ **Provide information prior to data processing**
  You may not use personal data before you have provided information. If you obtain the personal data of the data subjects yourself, you must inform them at the time of collection of the personal data. If you obtain personal data from another source, you must provide the information to the data subject no later than one month after obtaining the personal data. This period may be shorter but must never exceed one month:
  - If you use the personal data to communicate with the data subject, you must inform the data subject no later than at the time of first contact;
  - If you wish to transfer the data to another party (recipient), you must inform the data subject no later than at the time of the transfer of the personal data;
  - In the event of subsequent changes to the processing (e.g. new recipients, new compatible purposes, transfer outside the EU, etc.), you must inform the data subject in advance and do so well in advance, so that the data subject has time to exercise any rights.

- ❑ **Provide specific information if you use consent as a basis and request consent in the correct manner**
  If you request consent for the processing of personal data, also state that consent can always be withdrawn and how. You must obtain consent from the parent/legal representative if a research participant is under 16 years of age.

  Consent must be requested for each instance of personal data processing. This means that you must also request consent for each study if you are using the data for different studies. In practice, it can be difficult to be very specific in advance. Be as specific as possible and, if necessary, use a phased consent process, whereby participants can give consent at different times over a certain period for a study that is specified at that time.

  In addition, there must be an active action such as signing or ticking a box, an opt-in (i.e. not an opt-out: ‘I will process your data unless you indicate that you do not want me to’).

Examples of methods for obtaining consent:

- Via a consent form signed digitally or on paper.
- Via an online questionnaire (where the data subject has been informed that completing the questionnaire is regarded as consent).
- Verbally. For example, by recording this on audio/video or in the presence of a witness.

An example of what should be included in a consent form can be found in Appendix 2.

2.2 Do I have a procedure in place if a research participant withdraws their consent?

Consent under the GDPR may be withdrawn at any time, and following withdrawal, personal data may no longer be processed (from that point onwards). You must then delete this data. Please note that this does not concern ethical consent.

Withdrawing consent is an absolute right. In principle, you must always comply with this, even if you suspect that doing so could jeopardise your research. You must not process the data any further from the moment consent is withdrawn. You cannot comply with a request to withdraw consent if the personal data has been anonymised. In that case, the data can no longer be traced back to an individual.

You have informed the research participants of this. It is then important to set up an internal process, or to link up with existing processes within your institution. In this way, you can respond (quickly) to the withdrawal of consent.

2.3 Do I store the consent forms in a secure place?

As a researcher, you must be able to demonstrate that you have obtained consent. You should therefore keep the consent forms in a safe place. In many cases, you can use an information letter and a separate consent form, referring to the information letter on the consent form. You must keep all consent forms, but you only need to archive the information letter once and not for each respondent individually, as these information letters are all identical.

You must store the consent forms in a secure location, for example within Research Drive. Access to these forms must be restricted to what is strictly necessary (just as access to key files for pseudonymisation). Not every researcher or other staff member needs access.

How long you need to retain such a form depends on how the data collection is organised. If personal data is anonymised during the research project, there are no (longer) any source files containing traceable data, and there is no longer a need to collect additional data from respondents, then the purpose of the collected consent forms may also have expired (always bear in mind the need to be able to demonstrate research integrity).

2.4 Am I using secure research tools?

When using (digital) research tools, it is important to check whether these tools are in line with your institution's policy. If there is no policy or if there is uncertainty about this, bear in mind that,

in any case, these tools must also comply with the GDPR (or that you make agreements on how any other party handles the research data).

Tips for the safe use of research tools

- ❑ Check whether your institution has a policy on the use of personal mobile phones, recordings or artificial intelligence. If so, adhere to this policy or follow your institution's procedure for deviations from policy.
- ❑ Check whether your institution (or department) has approved certain (research) tools. Bear in mind that you often have to go through a process to request new (research) tools within your organisation if you need them.
- ❑ Choose providers of research tools that (as far as you can ascertain) handle personal data appropriately. This means they must comply with the basic principles of the GDPR, depending in part on whether they are the data controller or data processor. Consult the website and read the privacy statement and the user agreement (which may include a data processing agreement) to form an opinion.
- ❑ Check whether the providers use personal data for their own purposes. This may be the case, for example for analytical purposes to improve their services. It may also be for direct marketing purposes or resale to third parties. Ask yourself whether you consider this desirable and/or appropriate, and whether it is GDPR-compliant. If not, negotiate that this data is not used for these purposes, or choose another party to work with.
- ❑ Set out arrangements regarding the handling of personal data in the appropriate agreement (see step 1.3).
- ❑ Always check whether (survey) tools are available within your own institution. Often, you are required to use them, and consideration has been given to issues such as:
  - how this party informs your research participants;
  - whether the completed surveys are adequately secured;
  - what happens in the event of a potential security incident or data breach;
  - which systems you use to store the data
  - whether personal data is stored within the EEA;
  - whether the data is shared with third parties;
  - whether the data can be pseudonymised or anonymised;
  - whether the data can be viewed (by the research participant) or deleted (for example, once the deadline for completing the surveys has passed).

In this stage of your research, also check whether your security measures are still adequate (see Step 2: Storage & Management).

2.5 Have I registered my research in the register of processing activities?

As part of its accountability obligations, your institution must maintain a register of processing activities. As a researcher, you must register the processing of personal data for your research in this register (or have it registered). In principle, you should carry out this registration for each new processing operation. The data management plan can assist with this; see step 1.11.

It is also important to keep the information relating to the registered processing activities up to date throughout the duration of your research.

Step 3: Storage & Management

3.1 What measures can I take to secure the data?

As a researcher, you must *appropriately* secure the personal data in your research at every stage of your research. This step recurs at every subsequent stage in the lifecycle. Always check the information security requirements set by your institution. What is appropriate depends on several factors. Consider:

- the scale of the data;
- the context of your research;
- the sensitivity of the data;
- who needs access to the data;
- whether you share this data with multiple parties;
- the state of the art in terms of security measures.

This guide does not provide an exhaustive list of measures. Please consult your organisation's privacy contact person. Never store data on your personal devices or private clouds without good reason. In any case, consider the following measures.

Measures

- ❑ **Restrict access**
  Restrict access to personal data to those who genuinely need it for your research (or research support). This applies to staff at your own institution as well as to partners and third parties who need to receive the data.
  Draw up an authorisation matrix for this purpose. Your organisation will usually have a template for this. Base this on roles rather than individuals.
- ❑ **Prevent unauthorised access**
  Ensure that you authenticate access to data. Secure access to personal data using multi-factor authentication (MFA). This is now a standard measure for information security. Where possible, use a Virtual Private Network (VPN) connection if you wish to access your data from outside your organisation. Your organisation often enforces this as well. A VPN connection helps protect you against your data being intercepted by a malicious party.
- ❑ **Technical security systems**
  Always install software updates, use a firewall and adhere to the other state-of-the-art security measures on your systems.
- ❑ **Make a backup**
  Ensure you back up your data regularly so that your research information is not lost if there are problems accessing your systems or if the system crashes. Use the backup facility provided by your organisation for this purpose, rather than, for example, Dropbox, and secure this backup with an additional password if necessary. So check what your organisation has in place for backups – in terms of location, frequency, etc. – and follow these procedures.
- ❑ **Share personal data securely**
  Use Research Drive↗ and/or SURFfilesender↗ if you wish to share sensitive files or research data. Do not use email to share data, as this carries a high risk of data breaches or unauthorised access.
- ❑ **Adjust your document structure**

When organising your documents, it is important that file and folder names do not contain information that can be directly traced back to individual persons. In section 2.2, you will find a number of specific ways to choose file and folder names.

- ❑ **Limit storage to the EEA**
  To maintain control over your research data, it is advisable to limit the transfer/storage outside the EEA as much as possible.
- ❑ **Keep a clean desk**
  Do not leave research information in plain sight of third parties (within and outside the institution). If you use physical documents, such as completed questionnaires, store them in a lockable cabinet (and ensure it is locked).
- ❑ **Restrict access to facilities/locations**
  Ensure that the areas where you store research information can be locked and are only accessible to authorised personnel (e.g. with a key or a personal or role-specific access card).
- ❑ **Do not store data for longer than necessary**
  Personal data must not be retained for longer than is necessary for the purpose of your research. In the context of reproducibility and promoting the reuse of data, you may wish to retain data for a longer period. This means you must consider retention periods that take these interests into account. You must also describe these carefully. Align these plans with any requirements for consent.
  In section 2.3, you will find a recommendation (Table 4) for retention periods by document type. Always check your own institution's retention and destruction policy.
- ❑ **Adhere to policy and undertake training**
  Institutions often have data protection policies, whether or not these are specifically tailored to research. Consult these and adhere to them. Also undertake (compulsory or optional) training in this area.
- ❑ **Report data breaches involving personal data**
  If you suspect a data breach involving your research data, for example because someone has (or has had) unauthorised access to personal data or because it has been accidentally deleted, report the (suspected) data breach immediately in accordance with the data breach procedure applicable within your institution.
- ❑ **Check whether you can anonymise or pseudonymise your data**. As this is a broad topic, it is discussed separately below.

3.2 Adjusting the document structure

A number of specific ways to choose file and folder names.

1. Avoid personal information:
   Do not use names, national insurance numbers (!), email addresses or other directly traceable data in file or folder names. Example:
   a. Not: "JanJansen_Interview01.docx"
   b. Do: "Respondent01_Interview.docx"
2. Use neutral codes:
   Use unique, non-traceable codes for your documents. Example: "R01_Transcript.docx", where "R01" refers to a respondent in your database.
3. Document your structure: create a separate document explaining the meaning of the codes used and the structure of your files and folders. Store this file securely and separately from the data.
4. Restrict access: ensure that only necessary individuals have access to the documentation explaining the codes, such as a coding key.

5. Check file names prior to data publication: in the context of Open Science and FAIR data, you may wish to publish your dataset once the research is complete. Check the file and folder names of the items before publishing, to ensure they do not contain any traceable information.

   Thinking carefully about your file structure helps you work more efficiently and effectively during your research. At the same time, it helps to limit the consequences of a potential data breach.

   Do you have questions about organising your file names and folder structure? Please contact the data steward or another research support staff member at your institution.

3.3 Retention periods for your research data

Recommendations for retention periods by document type. Always check your own institution's retention and destruction policy.

Document	Example	Recommended retention period	Explanation
Consent forms	Signed consent form (may also be combined with an ethical consent form).	At least for as long as the personal data is used or shared, or is still required. Please check your organisation's policy for this.	Mandatory to be able to demonstrate consent for as long as personal data is processed. Only applicable if you operate on the basis of the 'consent' legal ground
Recordings (audio/video)	Interviews or focus groups	As short a period as possible; for example, destroy after transcription or analysis (if the data is no longer required)	Limit the storage of sensitive personal data by processing it quickly and pseudonymising it where possible.
Transcripts/ questionnaires	Written transcripts of interviews or completed questionnaires	Retention period depends on the purpose. ~~Preferably a maximum of 10 years.~~	Take into account your institution's policy, the National Code of Conduct for Scientific Integrity and the funding body. Different retention periods may apply in the medical field.
Metadata/analysis files	Coded data for analysis	May be retained for longer (e.g. 10+	Anonymised datasets are often required for

Document	Example	Recommended retention period	Explanation
		years), provided it is anonymised.	longer periods for reuse and replication research. It is preferable to delete the dataset and retain the syntax for reproducibility.
Other documents	Project documentation	Retention period as prescribed by institutional policy.	Check institutional requirements and other relevant regulations.

Table 4: Retention period guidelines by document type.

Do you have questions about the retention periods for your research data? Please contact the data steward or another research support staff member at your institution.

3.4 Pseudonymisation and anonymisation

Many people find it difficult to distinguish between pseudonymisation and anonymisation. To do this properly, you need to determine whether the process is irreversible or not. Put simply:

Pseudonymisation is usually reversible[16] - With the security measure of pseudonymisation, personal data cannot be directly linked to an individual without additional information (a key). The key is stored separately and securely. The GDPR still applies. If you do not need directly traceable personal data, ensure pseudonymisation is used as standard. Make a conscious decision as to whether you need to be able to trace the data back to the individual (for example, if a high risk of breast cancer is identified in a participant)

Anonymisation is irreversible - The complete anonymisation of personal data means that individuals can no longer be identified, even with additional information. This is irreversible. The GDPR then no longer applies. You are then referring to data and no longer to personal data. Bear in mind that for the temporary holding of personal data intended for anonymisation, a legal basis for processing and adequate protection are still required.

⚠ True anonymisation is very difficult. An anonymous dataset may lose that anonymity, particularly in view of advancing technology. The GDPR then applies (again). Always seek assistance from your privacy contact person.

In summary:

[16] The EDPB guidelines: edpb_guidelines_202501_pseudonymisation_en.pdf↗.

Pseudonymisation is different from anonymisation. After all, pseudonymised personal data can be combined with the key or with other datasets, allowing individuals to still be identified. This means that the GDPR still applies to pseudonymised data. Under certain conditions, pseudonymisation is sometimes preferable to anonymisation.

An effective method of anonymisation ensures that it is impossible for any party to:

1. Singling out an individual;
2. Link different records to an individual ('linkability');
3. Deduce information about an individual ('inference').

Data is only anonymous if it is 'reasonably' impossible to identify individuals, taking into account constraints in terms of cost and time, as well as current technology and future technological developments.[17] In other words: if identification is impracticable in practice because traceability would require an excessive effort in terms of time, manpower or resources.

The above leaves some room for discussion as to what is meant by 'reasonably'. The guidance therefore does not specify when data is or is not, in concrete terms, anonymous. However, you will find practical tips below on what you can do to anonymise or pseudonymise data.

It is preferable to anonymise personal data wherever possible.

If anonymisation is not possible or would unduly affect the usability of the personal data, you may consider pseudonymising the data. Bear in mind, too, that a third party cannot simply reverse the pseudonymisation (without a key).

When considering pseudonymisation, you must always take the following factors into account:

- the state of the art (scalable, resistant to attacks) and the costs of implementing any measures;
- the nature, scope, context and purpose(s) of your processing. This influences the type of pseudonymisation; and
- the risks that your processing poses to the rights and freedoms of the research participants.

Not all pseudonymisation techniques are equally effective, and they may not have the same implementation costs or requirements. In such cases, you must choose a pseudonymisation technique by identifying the optimal approach for data protection by design (privacy by design) and security.

[17] Recital 26 of the GDPR.

Do you have questions about pseudonymising or anonymising your research data? Please contact your institution's data protection officer.

Steps for anonymisation

- ❑ Remove directly identifiable data (name, date of birth, postcode, etc.).
- ❑ Remove unique identifiers from the dataset.
- ❑ Apply aggregation:
    - Combine data into broader categories, such as age groups ("20–29 years") rather than exact ages.
    - Add small changes to data values without affecting the research results.
    - Introduce noise.[18]
- ❑ Check traceability.
- ❑ Test whether the dataset really cannot be traced back to individuals, even when combined with other datasets. Various tools are available for this purpose.

Key considerations:

- Often, the smaller the number of participants, the more difficult it is to anonymise the dataset.
- In practice, pseudonymisation is more common than anonymisation. Ask yourself whether individuals really cannot be identified after going through the various steps. Research into specific study populations, for example participants with characteristics that are un ly common (this could also be a participant with an uncommon occupation) or patient groups with rare conditions, is difficult to anonymise.
- Anonymisation may limit the usability of your research data. Re-evaluate which measures are appropriate for each research project or research question.
- Document your approach.
- Describe how you carry out anonymisation in your DMP.
- If anonymisation is not possible or significantly affects the usability of the personal data, you may consider pseudonymising the data.

Steps for pseudonymisation:

- ❑ Replace identifying data: substitute directly traceable information (such as names, addresses or email addresses) with a unique code, such as a number or pseudonym. Other common methods of pseudonymisation include:
    - hashing;
    - encryption;
    - tokenisation.
- ❑ Separate data and key: store the pseudonymised data and the key in two different environments. Ensure that the key is stored in a secure environment, such as an encrypted database.

[18] For more information on these types of techniques, see:

- Privacy Design Strategies (The Blue Book)↗ by Jaap-Henk Hoepman.
- The anonymisation protocol↗ by Radboud University.
- The EDPB guidelines: edpb_guidelines_202501_pseudonymisation_en.pdf↗.
- Ghent University provides concrete examples of pseudonymisation↗ .

- ❑ Restrict access: ensure that only a limited number of people have access to both the data and the key.
- ❑ Document your approach: describe your pseudonymisation approach in the DMP.

Step 4: Analysis & Sharing

In the earlier stages of the research, you considered the careful design and collection of personal data. You may already have shared data with other parties and made agreements regarding this.

In this phase of the research, it is important that you continue to handle this data securely. Please refer to the questions and tips in sections 4.1 to 4.4.

4.1 How can I continue to handle personal data securely when changes occur?

As your research progresses, you may find that you need more data or that the context of your research changes.

If changes occur, always check whether the measures are still adequate.

Tips

- ❑ As soon as more (internal) staff members become involved in your research, carefully assess whether access to personal data is necessary, or whether access to only part of the personal data or even anonymised data will suffice. Ensure that access to this data is properly organised and, if necessary, adjust this in the authorisation matrix.
- ❑ If an employee no longer needs access to personal data, restrict access to this data.
- ❑ If you involve new parties in your research, ensure you make the appropriate arrangements with them via the relevant agreements (step 1.3).
- ❑ If you require more data for your research and this involves more or different personal data:
  - carefully assess whether the data meets the data minimisation requirement;
  - record the change in the processing register and DMP;
  - amend the information letter/consent form accordingly where necessary;
  - check whether the impact on research participants has changed and whether you need to update a previously carried out DPIA or carry out a DPIA (if you haven't already);
  - consider whether the agreements entered into need to be amended (so that they are accurate and so that you can assess whether the arrangements made, including security measures, are still adequate).

4.2 Can I already delete personal data?

Under the GDPR, you must delete personal data if you no longer need it. Check whether you can already delete personal data at this stage without compromising the purpose and integrity of your research.

For example, you can delete personal data if:

- the data has been processed;
- you have made recordings or collected other personal data, you may be able to delete this data after processing. For example, you can delete the original recordings once you have made transcripts of interview recordings, provided this does not otherwise pose any problems for demonstrating the integrity of the research.

- the personal data is not necessary for your research. This applies, for example, to personal data that research participants have provided without being asked, or which you subsequently assess as irrelevant.

Tips for secure deletion

- ❑ Include in your information letter/consent form how you handle the storage/deletion of personal data.
- ❑ Ensure that you delete data in such a way that it is irretrievable. You may be able to use software, or your internal service desk may be able to help you do this securely. Also check the digital recycle bins/deleted items if necessary.
- ❑ Destroy paper documents in a manner appropriate to your institution (for example, using shredders or special bins that are collected and destroyed by a certified company).
- ❑ Document the process: specify in your DMP which data you will delete, when you will do so and how you will carry this out. This will also help you respond correctly to any future requests for access.

It may be necessary to retain data for a longer period, for example for ethical approval or to replicate results upon publication or in follow-up research. Record this assessment (for example when determining retention periods) and consider whether you can store the data in pseudonymised or encrypted form.

Questions about the early deletion of personal data? Please contact your institution's data steward or privacy contact person.

4.3 Can I anonymise or pseudonymise the data in my research?

If it is not yet possible to delete the personal data – for example, because you need it – check whether you can anonymise the data at this stage. If that is not possible either, consider the options for pseudonymisation. See step 2.4.

In your research/paper itself, you should publish anonymised data, unless traceable data is unavoidable. In that case, you must take this into account as early as step 1, Planning & Design, and in your information letter/consent form to the research participants.

4.4 Are the security measures I have put in place still adequate?

It may be that your research has changed or that more staff or parties are involved in your research. Developments in the state of the art are also ongoing. Check whether the security measures you have taken (in earlier steps of your research) are still sufficiently appropriate. See

step 2. Management & Storage.

Any doubts? Then consult your internal contact person (data steward, security officer, CISO, etc.).

Step 5: Evaluation & Archiving

At this stage of the research, the processing of personal data has been completed. You must ensure that you:

- retain what needs to be retained;
- delete what can be deleted or cleared;
- transfer the results to the records management department.

Tips

- Your institution probably has a policy on retention and destruction periods. You must follow this policy. If there is no policy, look at examples from similar institutions or check with your organisation's legal advisor.
- Check whether you can further minimise (personal) data, bearing in mind two archiving objectives:
  1) Select and organise the data needed to validate your findings. Data that is important for verifying the research must be retained.
  2) Select and organise the data that may be valuable for further research by you, your team or fellow researchers.
- Discuss the conclusion of the project within the team and with collaboration partners.
- Remove copies of data from secondary locations (e.g. the platform used to collect data, laptop, SURFdrive, etc.).
- Review how you manage access to project folders and similar files. Consider, for example, revoking access where possible once the project has ended, for instance for external parties or researchers who no longer require access to the data themselves after completion.
- If you do not intend to use the data for future projects, consider removing it from your work environment after archiving.
- If you are still working with the data, consider tidying up your working directory.
- Delete all temporary working files (e.g. data that can easily be regenerated using archived scripts).
- Remove duplicate or outdated versions (e.g. final_v1.csv, final_v2.csv, etc.).

Step 6: Publishing

If you wish to use direct quotes in a publication of your research, it is advisable to check this with the person who made the quote beforehand.

Publication options:

1. Anonymised publication in a public repository[19] .

[19] See also the information on FAIR data↗ (Wikipedia) and publishing according to the principle 'As open as possible and as closed as necessary'.

2. Publication with access restrictions in which personal data has been made non-traceable or masked (always check which procedure applies and whether this is consistent with the consent given and the agreements made – consult your privacy team).
3. Only metadata and materials used to conduct the research (such as questionnaires, codebooks, scripts, etc.).

⚠ Please note: if you wish to make the research data set used publicly available, ensure that the set is truly fully anonymised.

Appendix 1 – Data Management Plan

- Standard DMP for research - DCC-PO (NL and ENG)

Appendix 2 – Consent form

Check with your privacy contact person whether your organisation has a template for requesting consent and withdrawing consent.

See Legal basis for consent↗ (Dutch Data Protection Authority) for an explanation of this legal basis and how to request consent.

⚠ Please note that you should not simply reuse a consent form later on. Always check whether the form you wish to use is actually appropriate for the situation.

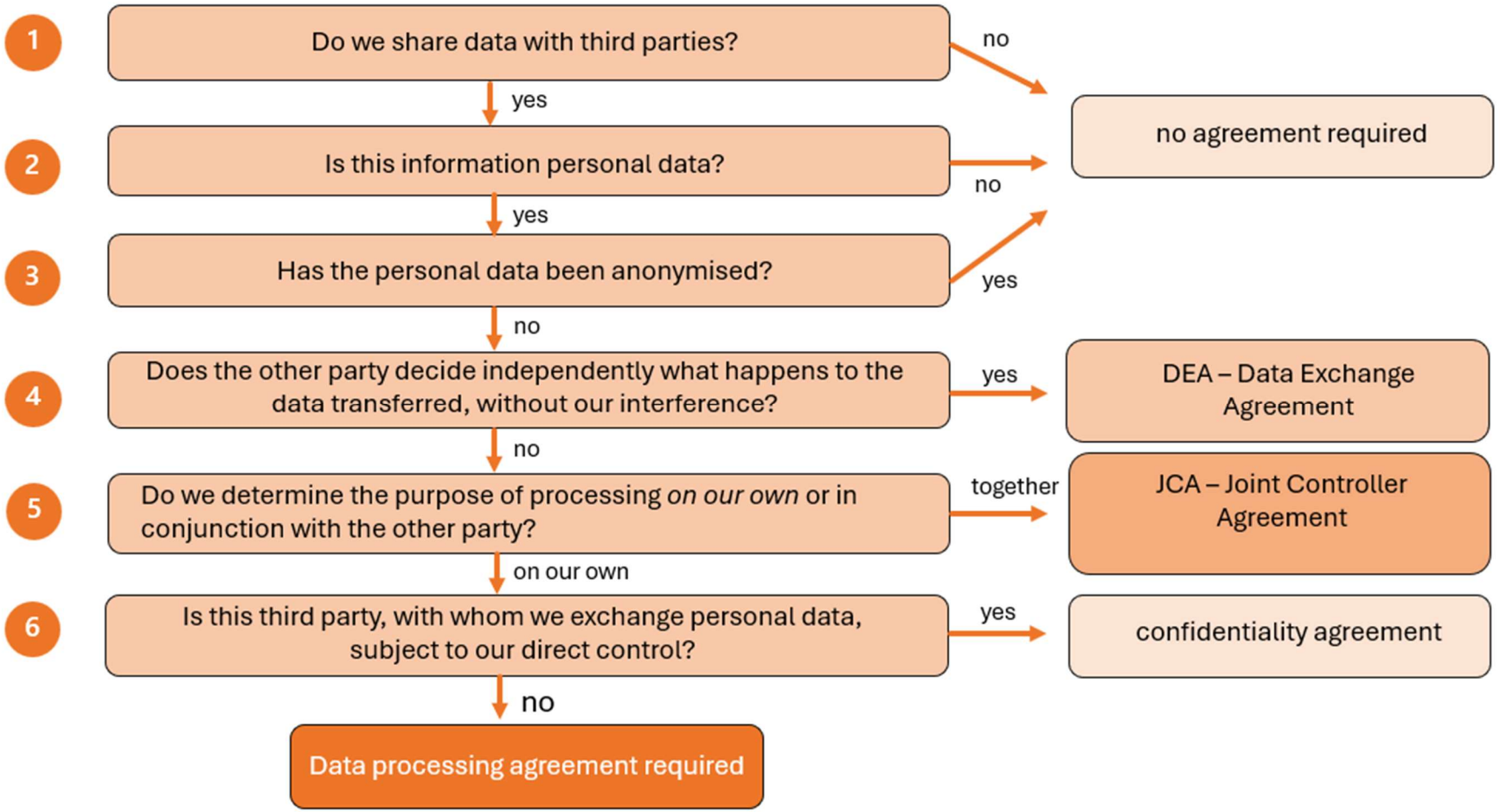
Appendix 3 - Glossary

See the AP's privacy glossary for a clear explanation of various privacy terms. The following terms are provided for further clarification:

Term	Explanation
EEA	The European Economic Area (EEA) comprises all EU countries plus Liechtenstein, Norway and Iceland.
Personal data	Personal data refers to information that either relates directly to a person or can be indirectly traced back to that person, in particular by means of an identifier such as a name, an identification number or location data. For example, by combining multiple pieces of personal data.
Special (categories of) personal data	Special categories of personal data are data that are so sensitive that they can have a significant impact on a person if an organisation processes them. For example, data relating to a person's health or political preferences. For this reason, special categories of personal data receive extra protection under the GDPR (such as data revealing a person's racial or ethnic origin, political opinions, data concerning a person's health, or sexual behaviour). In this document, special categories of personal data fall under the term 'sensitive data' because there is also sensitive data that does not fall within the category of special categories of personal data, but which also requires extra protection. ⚠ Please note: the processing of special categories of personal data is prohibited unless an exception applies. Ask your privacy contact person what you should do. ⚠ Criminal records are not covered by this definition.
Metadata	Information that provides details about other data, such as creation date, author, subject, size, etc.
Research participants	All individuals whose personal data you process for your research (even if the research is not about those participants themselves).
Primary use of personal data	Primary use is when, within the research, you collect personal data directly from the data subjects with a specific objective in mind.

Term	Explanation
Secondary use of personal data	Secondary use occurs when you do not collect personal data from an (existing) dataset directly from the data subjects, or when the data was originally collected for a purpose or research project other than your current research project. In this guide, we refer to this as 'reuse'.
Scientific research (in the context of this guide)	• Research in which personal data is processed. • Relevant sectoral standards for methodology and ethics apply, including the concepts of informed consent, accountability and oversight. • The research is conducted with the aim of increasing collective knowledge and the well-being of society, rather than primarily serving one or more private interests.

Appendix 4 – Decision tree for allocation of roles and agreement to be concluded



Appendix 5 – Checklist for the researcher

The checklist is consistent with the approach based on Harvard's Data Lifecycle (see Chapters 2 and 3).

Check	Steps	Lifecycle step	Guidance
❍	I have checked whether the GDPR applies to my research.	Step 1 Planning & Design	Page 12
❍	I have set out agreements on data use with other parties in the appropriate contracts.	Step 1 Planning & Design	Page 14
❍	I have considered the reuse of data from my research and taken measures to facilitate this.	Step 1 Planning & Design	Page 22
❍	I have assessed whether I needed to carry out a DPIA and have taken measures to protect data appropriately.	Step 1 Planning & Design	Page 23
❍	I have drawn up a data management plan (DMP) in which I have explained my data protection choices.	Step 1 Planning & Design	Page 23
❍	I inform participants in a timely and appropriate manner. The content of my information letter is consistent with the DMP and the processing register.	Step 2 Collection & Use	Page 24
❍	I have organised my processes in such a way that I can comply with participants' GDPR requests.	Step 2 Collection & Use	Page 28
❍	I have registered my research in the processing register.	Step 2 Collection & Use	Page 29
❍	At every stage of my research, I check whether the measures taken are still appropriate.	All steps	Page 30
❍	I have taken the appropriate protective measures, anonymised or pseudonymised data where possible, determined the retention periods, and ensured that data is stored in the correct location for long-term storage.	Step 3 Collect & Create	Pages 33/34
❍	I have checked that I am still working securely and, where possible, have deleted, anonymised or pseudonymised data, or complied with retention periods and ensured the correct location for long-term storage.	Step 4 Analysis & Sharing	Pages 37/38
❍	At every stage of my research, I check whether the measures taken are still appropriate.	All steps	Pages 30, 33 and 37