TILBURG UNIVERSITY

Thematic Privacy & Personal Data Protection Policy

Scientific Research

The Use of Personal Data

Version 1.2 - May 2023

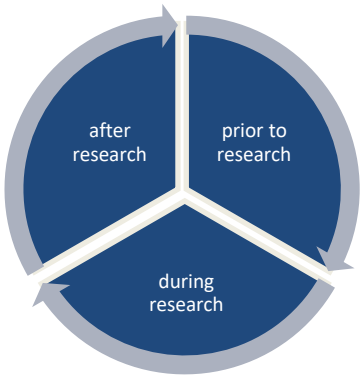
Reader's Guide

This Thematic Privacy & Personal Data Protection Policy - Scientific Research is part of the Privacy & Personal Data Protection Policy and describes, for scientific research purposes, how Tilburg University implements the General Data Protection Regulation (GDPR) regarding the protection of personal data.

The directives set forth in this Policy apply only if personal data (data that can now or in the future be traced back to a natural person) is used in a scientific research project. Research normally involves the collection of more data than just personal data. However, this Policy deals primarily with legal aspects related to personal data.

If no personal data are processed or if they are already fully anonymized when obtained (and therefore never traceable to any person) then this directive does not apply. **Please Note!** The anonymization of personal data does constitute processing to which the directives apply.

For readability, we have divided this Policy into three phases, based on the different stages of doing research: prior to, during, and after the research.



All information related to European legislation (GDPR) and the protection of personal data is included on the Privacy and Security portal. [1] This portal also contains practical elaborations and examples.

This Policy includes references to other policies; these documents are **in bold**. Directives that apply are shown in blue blocks to make them easy to find:

Subject	

This Policy includes many definitions; these terms are conveniently listed in the definition list (Appendix 3). Throughout the document, definitions are explained in the green blocks:

Concept	

Each School/Division within TiU has appointed so-called Data Representatives.[2] They are the first point of contact for employees in case of questions about the protection of personal data. For questions about data management, data storage, and data archiving that may or may not involve processing personal data, researchers can also contact the Research Data Office (RDO). For more detail, please refer to the **Research Data Management Regulations**.

This Policy provides general points of reference to researchers. However, the lawful use of personal data in scientific research depends on the facts and circumstances of each case. Therefore, a researcher must weigh up on a case-by-case basis whether the processing complies with this Policy, TiU's general **Privacy & Personal Data Protection Policy** and applicable legislation, and remains responsible for doing so.

[1] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security
[2] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/careful-handling-personal-data/questions

Since 2017, UNL (Universities of the Netherlands, formerly VSNU) has been developing a new version of its Code of Conduct on the Use of Personal Data in Scientific Research, which may of course affect this Thematic Policy. When a new version of this Code of Conduct is finally adopted, this Policy will be evaluated and brought into line with the Code of Conduct. Also when additional regulations are issued by the European Union (for example, in the form of recommendations of the European Data Protection Board) that may affect the content of this Policy, such a review will take place.
Furthermore, practice will have to show which research disciplines will require further elaboration of this Policy.

In line with the Privacy & Personal Data Protection Policy, this Policy will be reviewed every two years and revised as necessary, unless earlier revision is necessary based on changed legislation and regulations or changed policy recommendations.

When this Policy refers to he, it is understood to mean he/she or gender-neutral.

Contents

1. Introduction

This chapter describes when this directive does or does not apply. Next, various terms are briefly explained and the difference between pseudonymization and anonymization is made clear. Finally, this chapter contains an overview detailing who within the university is responsible for what.

1.1. Application

This directive applies only if personal data are processed in scientific research. If no personal data are processed then this directive does not apply. If personal data are collected in the context of scientific research but are anonymized within a short period of time, then we are still talking about processing personal data. To determine whether personal data are processed or not, the starting point is always the data collected during data collection.

This Policy applies to all processing of personal data that takes place in the context of scientific research under the responsibility of Tilburg University and applies to everyone working under the responsibility of Tilburg University. This includes all Tilburg University personnel, including personnel not on payroll, student assistants, temporary or hired staff and interns, (external) PhD researchers, and students who contribute to research. Therefore, it concerns all processing of personal data carried out by researchers in the context of scientific research.[3]

1.2. Terms

Personal data	Personal data are any information about an identified or identifiable natural person[4] (in the terms of the GDPR: the data subject). An "identifiable" person is considered a natural person who can be directly or indirectly identified.

When data can be traced back to individuals, we speak of personal data. These can be both directly traceable personal data, such as name or email address, and indirectly traceable personal data, such as a license plate number or a combination of initials and zip code and house number. However, what can be personal data is also context-specific; the combination of several not directly traceable data (for example, rare medical condition, place of residence, and age group) can cause an individual to be traceable nonetheless, making the relevant data to be considered personal data. For example, there was a study in which the researcher in question used a model they developed to correctly re-identify 99.98% of Americans in a random "incomplete" dataset based on 15 demographic attributes.[5]

In scientific research, a lot of work is done with respondents. Tilburg University (TiU) attaches great importance to the careful processing of personal data in the context of scientific research

[3] In this policy, "scientific research" means "scientific research within the meaning of the Higher Education and Research Act.

[4] A "natural person" means only living persons. This means, therefore, that deceased persons do not fall within the scope of the GDPR. However, data about deceased persons can in theory also contain information about living persons (for example: the information that someone died of a hereditary disease is also information about his/her children). Therefore, do not necessarily assume that data about deceased persons do not fall within the scope of the GDPR.

[5] Rocher, Hendrickx & De Montoye 2019, "Estimating the success of re-identifications in incomplete datasets using generative models," *Nature Communications*, <https://www.nature.com/articles/s41467-019-10933-3/>.

because misuse of data can cause great harm to these respondents. A good balance is sought between privacy, security, and functionality.

Processing	For the purposes of this Policy, Processing means performing an action with one or more personal data in whole or in part by automated means or included in a file or intended to be included in it.

The GDPR understands the term processing to mean any operation or set of operations involving personal data, whether automated or not, such as the collection, recording, structuring, storage, alteration, analysis, retrieval, consultation, use, provision (forwarding), dissemination, making available, combination, blocking or destruction of data. In other words, all the operations you can perform with personal data. A processing of personal data can be either non-automated, such as in a paper file or archive, or automated, such as in a digital file or application/system (including in mailboxes and on computers or other data carriers such as USB sticks). However, not all processing falls within the scope of the GDPR: the legislation only applies to fully or partially automated processing, as well as processing of personal data contained in a file or intended to be contained in a file. A file is a structured set of personal data accessible according to certain criteria. To illustrate: a paper archive structured on the basis of names is a file; a folder containing an unstructured set of papers containing personal data is not a file.

When we refer to processing for the purposes of this Policy, we mean processing of personal data that falls within the scope of the GDPR.

Data Subject	In this Policy, data subject means all persons involved in scientific research, including (but not limited to) respondents.

The GDPR refers to data subject or data subject. In scientific research, this refers to all persons involved in the research. The data subject in scientific research will in most cases be a respondent (also called a test subject or participant). However, because other persons may also be included and in order to remain in line with the terminology of the GDPR, we use the term data subject in this Policy.

Anonymization	For anonymization, personal data are processed in such a way that they can no longer be used to identify a person and are, therefore, no longer personal data. This processing is, by definition, irreversible.
Pseudonymization	For pseudonymization, identifying data are separated from non-identifying data and replaced with artificial information.

Anonymization and pseudonymization are terms that are regularly used interchangeably, but there is an essential difference between the two. In pseudonymization, identifying data is separated from non-identifying data and replaced with artificial information. However, a key file is created, which records which data have been replaced with the artificial information. With pseudonymization, the data can thus be reconnected with this key, making it possible to trace back to natural persons. Anonymization, on the other hand, revolves around processing that is no longer reversible: once personal data have been stripped of identifying data, it is no longer possible to reconnect them to individuals later.

An example of pseudonymization is replacing the data of a data subject in a study with a unique respondent number. For example: the medical data are then linked to this respondent number instead of, for example, name, address, and place of residence. This makes it invisible to outsiders who the person is to whom the medical data belong. Only the person who can link the respondent number to the person (e.g., researcher) is able to link the medical data. Sufficient (organizational

and technical) measures must then be taken so that unauthorized persons cannot link these files. Because the data are still traceable in the case of pseudonymization, the GDPR and thus this directive applies.

An example of anonymization is permanently removing a data subject's identifying data. For anonymous data, the GDPR does not apply. However, keep in mind that, with anonymous data, there is no longer any possibility of identification or tracing back to individuals. However, anonymization in itself is processing of personal data and is, therefore, still subject to the GDPR. If data can still be traced back to a person, anonymization is not applied.

Many different pieces of data may be collected during a research study. Data minimization means that only data that are necessary to answer the research question are collected and will actually be used for that purpose. An example would be a workplace satisfaction survey, asking questions about workplace atmosphere and satisfaction with facilities. The researchers could also ask questions about diet, smoking, and drinking habits, but in the context of data minimization, this is not allowed. The survey does not focus on the lifestyle of employees, and therefore, these data are not needed to answer the research question.

Data minimization	Data minimization means that when collecting and processing personal data, no more data must be collected than is necessary to achieve the purpose for which it will be used.

Data minimization is valuable for a simple reason: what you do not own, you cannot lose or process incorrectly. Thanks to data minimization, a data subject is assured that no more privacy-sensitive data than necessary about him or her are floating around an organization. That alone ensures more privacy. After all, an organization does not know more about the data subject than it needs for its purpose. It also reduces the chance of incorrect processing. Consider access by an unauthorized person or even theft by hackers. Data that an organization does not own cannot end up on the street or seen by the wrong people.

1.3. Responsibility

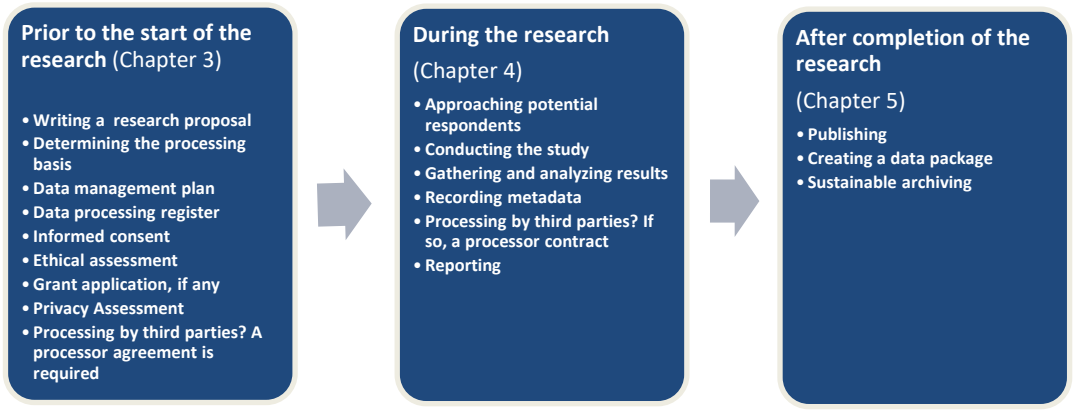
A research study is conducted under the direction of a researcher. He is responsible for compliance with this Policy and must ensure that everyone who participates in the research under his responsibility (e.g., (external) PhD researchers, student assistants, and students) complies with this policy on personal data protection. For research, there are different forms of responsibility:

Researcher	Using the facilities offered by Tilburg University, the researcher is responsible for: • compliance with the university's **Privacy & Personal Data Protection Policy** (including this Thematic Policy) and, thereby, the GDPR as well as the **Research Data Management Regulations;** • proper data management and data storage in accordance with the principles in the **Research Data Management Regulations;** • drafting a Data Management Plan prior to new research in accordance with the **School's Data Management Policy;** • ensuring that PhD researchers and students (performing work under the responsibility of the researcher) comply with the Regulations and Policies as stated above.
Dean	The Dean of the School concerned is responsible for:

	• the implementation of the **Privacy & Personal Data Protection Policy** regarding scientific research within the School (possibly using School policies); • informing academic staff about this Policy; • overseeing compliance with these policies and report to the Executive Board.
Executive Board	The Executive Board is responsible for: • establishing a general university policy framework as set forth in the **Privacy & Personal Data Protection Policy**; • providing flanking knowledge, advice, and guidance on processing personal data; • providing adequate infrastructure for data storage and management; • conducting and supervising audits, respectively.
Joint responsibility	If, on behalf of TiU, a researcher exchanges personal data with, provides personal data to, or receives personal data from another organization, proper contractual agreements must be made. For more information, see Section 3.5.

1.4. Phases of research

The aspects of scientific research that are relevant to personal data can be represented in three phases: prior to, during, and after completion of the research. These three phases have their own concerns when it comes to personal data protection that the researcher must take into account. Chapter 2 deals with general directives; subsequent chapters adhere to these phases of research.



2. General Directives

The directives mentioned in this chapter are general directives that do not apply specifically to any of the phases of scientific research and involve:

- Use of datasets (**Section 2.1**).
- Lawfulness - Processing Basis (**Section 2.2**)
- Lawfulness - Processing Basis for special personal data (**Section 2.3**)
- Purpose limitation (**Section 2.4**)
- Material requirements (**Section 2.5)**

2.1. Use of datasets

Scientific research often involves the use of paper or digital datasets that include personal data. These may include:

- Creating a new dataset (Section 1.5.1)
- Use of existing datasets (secondary use) (Section 1.5.2)

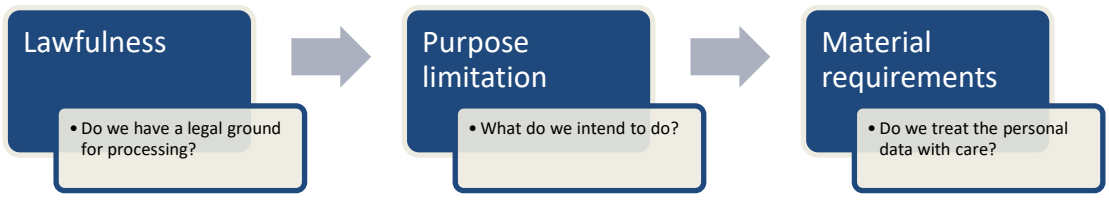
2.1.1. Creating a new dataset

Appendix 1 provides some examples of types of datasets in which personal data are processed, indicating specific directives for the following types of research:

- Video and audio recordings
- Interviews
- Observations
- Experiments in Labs with respondents (including virtual reality labs)
- Eye tracking
- ECG/EEG/MRI
- Wearables

The above list is not exhaustive; other examples not mentioned are obviously also covered by this Policy. TiU considers the data collected in such studies to be personal data. This policy choice is made because patterns from such studies may well be traceable to individuals in the future.

If personal data are processed in scientific research, the so-called lawfulness and purpose limitation must first be established. After this, the so-called material requirements must be observed to ensure that personal data are handled with care.



2.1.1.1. Collecting data directly from data subjects

In scientific research, you can create a new dataset by collecting data from data subjects. A dataset can take the form of a file of quantitative data, but it also includes a collection of qualitative data such as video and audio recordings, interview transcripts, eye-tracking recording, etc. These data subjects may be self-recruited such as through a call for participation or from a human subject

pool. When the research with the data subjects is conducted in such a way that the research data cannot be directly or indirectly traced back to individuals, we consider the research data to be anonymous data. This may be applicable in some cases for research taking place in university labs or through participant panels such as M-Turk, Prolific, CentERData, etc. However, this is highly dependent on the design of the research. Please note that nevertheless, the necessary agreements on responsibilities (such as control over the data, security, incident reporting, etc.) must still be in place. Please contact your Data Representative for more information on this.

Data subjects	For data subjects (mostly respondents), it is important that they participate voluntarily and that they are well informed in advance about the research, among other things, with regard to personal data protection. This is ensured by means of the consent form (also called informed consent) (Sections 2.5.3 and 3.1). If special personal data are processed, additional requirements apply (Section 2.3).
Data minimization	The researcher may only collect personal data necessary for the purpose of the scientific research (as little as possible) but ensures that sufficient data are collected to answer the research question. See **Chapter 6 of the Privacy & Personal Data Protection Policy**.
Security	If personal data are used in research they must be processed in an adequately secure manner. Measures such as pseudonymization and/or anonymization must also be applied as early as possible. **Chapter 9 of the Privacy & Personal Data Protection Policy**.
Information requirement	Data subjects have the right to information and must be properly informed. See Section 2.5.6 for Data Subject's Rights and **Section 10.3 of the Privacy & Personal Data Protection Policy.**
Registration	Research must be recorded in the data processing register (Section 3.2)

2.1.1.2. Dataset based on public or closed sources

In addition to collecting data from data subjects, a new dataset can also be created from public or closed sources. By this we mean specifically the collection of already known data that are not already part of a dataset. For the use of already existing datasets, we refer to the secondary use of datasets in **Section 2.1.2**.

For compiling a new dataset based on public or closed sources, the following applies:

Data subjects	For data subjects, it is important that they are well informed in advance about the research, among other things with regard to personal data protection. Preferably they are asked for their consent and informed immediately, unless an exceptional situation applies. See Sections 2.2 and 2.3.

Data minimization	The researcher may only collect personal data necessary for the purpose of the scientific research (as little as possible) but ensures that sufficient data are collected to answer the research question. See **Chapter 6 of the Privacy & Personal Data Protection Policy**.
Security	If personal data are used in research they must be processed in an adequately secure manner. Measures such as pseudonymization and/or anonymization must also be applied as early as possible. **Chapter 9 of the Privacy & Personal Data Protection Policy**.
Information requirement	Data subjects have the right to information and must be properly informed. See Section 2.5.6 for data subject rights and **Section 10.3 of the Privacy & Personal Data Protection Policy.**
Registration	Research must be recorded in the data processing register (Section 3.2)

A common technique in this context is the collection of data via Web scraping from (semi) public sources. If a researcher wants to scrape forums, social media, or other (semi) public websites, there may be copyright and terms of use of the public source.

In addition, the researcher must also consider the context in which the public information is placed. Public information may be used for scientific research if the purpose for which it was initially disclosed is an extension of what is being researched, so that data subjects could reasonably surmise that their data could be used for such research. This also expressly applies to special personal data that have been clearly disclosed by the data subject himself.

Use of web scraping	For scientific research, the researcher may, subject to conditions, process personal data by web-scraping if they are public and have been collected for a similar purpose. This also applies to special personal data clearly disclosed by the data subjects themselves. Please note that there may be copyright and terms of use of the public resource. For more detail, see the Copyright Information Point on the Intranet.[6] If you have any questions about this complex issue, please contact your Data Representative.

Some examples for clarification in the context of web scraping:

- *If a researcher uses blogs from AirBnB (in which travelers indicate their experiences) that are publicly available to ascertain whether tourists are ethnocentric. When writing the blogs, authors could not have suspected how their texts would be used and might not have given consent if asked. The researcher is then not allowed to use this information must and must then seek explicit consent from the authors of the blogs.*
- *If a researcher uses a public blog on Facebook in which someone writes about personal experiences with cancer with the goal of informing peers and loved ones. In this case, the researcher is allowed to use this information if he uses it to compare patient experiences.*

[6] https://www.tilburguniversity.edu/cip?check_logged_in=1

- *If a researcher uses a blog on a private forum that is not public (but to which the researcher has access with the purpose of the research), it may not be used for scientific research (unless researcher has specific permission (informed consent) from the data subjects).*

2.1.2. Use of existing datasets (secondary use).

In scientific research, it frequently occurs that datasets created for another study or even another purpose are reused in a new study. This is called secondary use, for which the GDPR has included specific regulations (Article 5, paragraph 1, under b). The use of an already existing dataset is permitted under the GDPR due to the importance of scientific research under conditions (Article 89) such as appropriate safeguards, technical and organizational measures, pseudonymization, etc.

When reusing a pre-existing dataset, only anonymized or pseudonymized data will be used whenever possible, with the researcher not receiving the interconnected file in the case of pseudonymized data.

If special personal data are involved (Art 9, paragraph 2, under j of the GDPR), an additional criterion applies in scientific research: their use is only permitted if necessary, proportionate, and appropriate measures are taken.

Finally, based on Article 14, paragraph 5, under b of the GDPR, data subjects have the right to be directly informed about the processing if the personal data were received from the data subjects themselves, unless this requires disproportionate effort. In the latter case, the data subjects must be informed by other means (e.g., by means of the public publication of a privacy statement).

Of course, it is also possible to create a new dataset for scientific research by collecting data from participants and using existing datasets. In this situation, the directives in Section 2.1.1.2 apply to the collection of new data and the directives in this Section apply to secondary data.

2.1.2.1. Non-public datasets

A non-public dataset is a dataset to which access must first be obtained before the data can be accessed. For example, the metadata of such a dataset has been made public. In a repository, such as DataverseNL, a researcher can choose not to publish the data publicly. If you want to use this dataset, contact the researcher and make arrangements. There may also be restrictions on datasets not initially collected for scientific purposes, for example, financial data from a commercial company.

Anonymization or pseudonymization	When using pre-existing datasets, personal data must be anonymized as much as possible. Once the primary dataset is anonymized, this directive no longer applies, nor does the data processing register need to be updated. If anonymization is not possible, then personal data must be pseudonymized as much as possible. The GDPR and this directive apply to this. See further explanation below.

Data minimization	The researcher may only use personal data necessary for the purpose of the scientific research (as little as possible) but ensures that sufficient data are used to answer the research question.
Security	If personal data is used in research it must be processed in an adequately secure manner. See **Chapter 9 of the Privacy & Personal Data Protection Policy.**
Information requirement	Data subjects have the right to information and must be properly informed. When re-using existing datasets, direct information will often be impossible or require too much effort; in those cases, data subjects must be informed in another way. See Section 2.5.6 for rights of data subjects.
Registration	Research must be recorded in the data processing register (Section 3.2).

2.1.2.2. Public datasets

Scientific research often makes use of public datasets (licensed or not) that do not contain easily traceable personal data. Examples are the CBS datasets or the European Social Survey and World Value Survey (WVS). Dataverse datasets stored as "open" are also included.

These datasets do contain personal data, but these are usually anonymized[7] or pseudonymized (for which Tilburg University does not have the key to link the datasets and thus (for Tilburg University) cannot be traced back to individuals). In a few cases, these datasets do contain personal data that have been made public on the basis of legal regulations and of which the data subject can expect that these data are used for scientific research, for example salaries of CEOs of listed companies. Often when these datasets are used (when the license is concluded), the researcher does have to declare a number of things, for example, that the data will not be used commercially. We consider these datasets as not falling under the scope of the GDPR.

A point of attention here is that if two public datasets are combined, there may well be (in the future) traceable personal data.

Use of public datasets	When public datasets are used, anonymized or pseudonymized personal data (without a connection file) are used in principle and are thus not traceable. The researcher must ensure that the requirements set forth in the license or at the time of downloading are met and that personal data are not traceable unless they have been made public on the basis of a legal regulation and the data subject can expect that these data are used for scientific research Please note: If the public dataset contains personal data or the data is Traceable through combination of datasets, then the research must comply with all requirements as included in this Policy. The Data Representative can assist in determining whether this is necessary.

[7] Anonymized datasets do not contain personal data and, therefore, are not covered by this directive.

2.2. Lawfulness - Processing basis

Any processing of personal data must be lawful, that is, there must be a legal processing basis and purpose for the processing. The **Privacy & Personal Data Protection Policy explains** the six legal processing bases in detail.

For scientific research, the processing bases depend on how the researcher compiles a dataset:

- Setting up a new dataset directly from data subjects.
- Setting up a new dataset not through data subjects (e.g., web scraping).
- Use of existing dataset (secondary use).

The processing bases are set out below for the different ways of compiling a dataset. The bases that are possible in scientific research are in order of priority:

Consent	Consent is the primary basis in scientific research. It is important to distinguish this consent as a legal basis in the GDPR from ethical consent (as a safeguard). For ethical reasons, you may need consent from participants to participate in a particular study (this may be legally required or ethically recommended). While both can be combined, ethical consent is not necessarily subject to the same conditions as consent as a legal basis in the GDPR. These conditions from the GDPR are: 1. Data subject must be properly (clearly) informed in advance of the processing for which he is giving consent. 2. Consent must be given actively. That is, no use of a pre-filled check box. 3. Consent must be provable after the fact; 4. Is consent given by means of a statement that also covers other matters? Then the request for consent must be presented in understandable and easily accessible form and in clear language such that it can be clearly distinguished from the other matters. Consider including a separate checkbox on a form; 5. Consent can be withdrawn by the data subject at any time, and this can be as simple as giving it. Example: processing personal data for prospective students who have given consent to approach them for university activities. See more detail Sections 2.5.3. and 3.1.
Public interest	This legal basis can only be used when it can be demonstrated that there is an urgent social need for the processing of certain personal data and asking permission is not possible. This means that there must be an explicit gain of knowledge in the interest of society. However, this is not applicable by default to most research. For example, this may be the case for research on poverty alleviation. Thus, the use of the legal basis public interest requires a social need, a gain of knowledge for society, and an explicit task in the public interest assigned to the institution.

Legitimate interest	Only if processing based on consent or public interest does not succeed can the basis of legitimate interest be considered. When the processing of personal data takes place on the basis of legitimate interest, the researcher (assuming that the research serves a legitimate purpose, and the processing of the personal data is necessary) must weigh up the interests. This balancing of interests must include the following issues: a. the consequences for the data subject; b. whether (additional) safeguards are in place; c. the seriousness of the interference; and d. whether the data subject can more or less expect the processing. The researcher must document this consideration in the data processing register portion of the integrated application form for the GDPR, ethical review, and data management.

It is necessary for the research to properly safeguard the interests of data subjects in terms of research design and management/security of personal data. For this, see the requirements under the various points of the research life cycle.

Note that if special personal data are also processed, Section 2.3 instead of Section 2.2 applies. This is subject to stricter rules and fewer possible bases.

Processing basis new dataset directly from data subject	The processing basis is the data subject's consent. To properly inform the data subject, informed consent must be sought (Sections 2.5.3 and 3.1).
Processing basis new dataset not via data subject - non-public data	The processing basis is generally the data subject's consent. However, in exceptional situations, one of the following processing bases may also apply: • Necessary for a task of public interest • Necessary for legitimate interest Whether and if such an exception applies, this must be properly documented and justified by the researcher in the data processing register component of the integrated application form for GDPR, ethical review, and data management. If necessary, the Data Representative can advise in this regard. An information requirement also applies: o if the researcher has contact information of the data subject: inform personally if this does not require disproportionate effort,[8] otherwise inform publicly; o if the researcher does not have contact information: inform publicly. *Example:*

[8] Disproportionate effort could apply, for example, if the databases are very large and many data subjects need to be approached. If this exception is chosen, this must be recorded by the researcher (motivated).

	• *Certain forms of economics research may have a processing basis for a task of public interest.*
Processing basis new dataset not via data subject - public data	The processing basis in scientific research for which a new dataset is established whereby public research data is collected without obtaining it directly from data subjects is: public interest or legitimate interest The research data in this case are collected from information disclosed by the data subject himself. The public information may be used for scientific research if the purpose for which it was initially disclosed is an extension of what is being researched, so that data subjects could reasonably surmise that their data could be used for such research. An information requirement also applies: ○ if the researcher has contact information of data subject: inform personally if this does not require disproportionate effort,[9] otherwise inform publicly; ○ if researcher does not have contact information: inform publicly. If the original purpose is not an extension of what is being researched, it is only possible to process the data with the consent of the data subject. *Example: setting up new dataset using web scraping. See also Section 2.1.1.2.*

For secondary use of an already collected dataset, the researcher must consider whether permission to reuse the data for a future study has already been granted, and the researcher must also consider whether the new study falls within the same research area as the initial study or in a different research area. Two scenarios can then be distinguished to determine which processing basis may apply:

i. Permission has already been granted for reuse for future research in the research area in which the new research is taking place
ii. There is no permission for reuse for future research in the research area in which the new research is taking place.

Processing basis secondary: Consent for reuse	The processing basis is consent, but the researcher need not seek new consent. However, an information requirement applies: ○ if the researcher has the data subject's contact information: inform personally if this does not require disproportionate effort;[10] ○ if the researcher does not have contact information: inform publicly.

[9] Disproportionate effort could apply, for example, if the databases are very large and require many data subjects to be approached. If this exception is chosen, this must be recorded by the researcher (motivated).
[10] Disproportionate effort could apply, for example, if the databases are very large and require many data subjects to be approached. If this exception is chosen, this must be recorded by the researcher (motivated).

	Note: When consent is given, a data subject may always withdraw it; if this happens, the data of this data subject may no longer be used for follow-up research unless the exceptions for scientific research apply. See Section 2.5.5 for directives on withdrawing consent. *Example: a researcher uses data from a previous study for a follow-up study within the same research area. This previous study is based on consent and the data subjects have agreed to have their data used in future studies.*
Secondary processing basis: no consent for reuse	Because consent for reuse for the study area of the new study was not requested when the dataset was initially prepared, it must still be requested if reasonably possible: ○ if the researcher has the data subject's contact information: seek personal consent ○ if the researcher does not have contact information: processing basis public interest or legitimate interest (see also the block of processing bases at the beginning of this section). However, in connection with the right to be informed, data subjects must be publicly informed. The above also applies if the dataset was not initially created for scientific research. *Example: a researcher uses data from a previous study for a follow-up study within another research area. This previous research took place in research area marketing and the data subject has been asked permission for reuse but only within the marketing research area. The new research takes place within a law research area. If it is possible (disposal of contact data), then the researcher must still ask permission. If this is not possible, another processing basis such as legitimate interest may apply, in which case the researcher must carefully weigh the interests of the research against the privacy interests of the data subject.* NOTE: On ethical grounds, if the data subject was asked about the dataset when it was initially created but did not provide consent for reuse of the data, it may not be reused on any other basis unless consent is obtained after all.

2.3. Lawfulness - Basis for processing special personal data

Under the GDPR, special personal data may only be processed under strict conditions. For scientific research, an exemption from the ban on processing special personal data applies under conditions. See **Section 4.3 of the Privacy & Personal Data Protection Policy**.

The table below shows which personal data are designated as special or have another special status under the GDPR.

Special personal data	Special personal data are data revealing: • Racial and ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership As well as: • Genetic data • Biometric data for identification purposes • Data concerning health (medical data) • Data concerning a persons sex life or sexual orientation. This data may only be processed in accordance with what is provided in this section. Personal data of a criminal nature may also be processed only under strict conditions. This is subject to the same regime as special personal data. Note: If special personal data is processed, then there are additional security requirements. See **Chapter 9 of Privacy & Personal Data Protection Policy**.
BSN	The Citizen Service Number (*BSN*) may never be processed for scientific research. However, it is possible that in some situations the *BSN* may be required for *UBD* (amounts paid to third parties). The *BSN* is then only used for the financial process and may not be included in the research data.
Id.	A copy ID may only be viewed, but not stored unless storage is necessary for scientific research, photograph and *BSN* number are masked, and it is marked on the copy that it was issued for the purpose of research. **Tip**: Preferably write down only necessary information instead of a copy of an ID.

The following table outlines the rules for the use of special personal data within scientific research.

Use of special personal data	Special personal data may be processed in scientific research if there is explicit consent. Specifically for scientific research, an exception applies, which only applies if: 1. requesting consent proves impossible or requires a disproportionate effort, 2. the processing is necessary for the purposes of the research, and 3. the research serves a public interest. There must also be safeguards in place such that the privacy of the data subject is not disproportionately affected. An elaboration for the various types of datasets is given below.

New dataset with special personal data - received directly from data subject	Consent required (informed consent): data subject must give explicit consent to the processing of the special personal data on the informed consent form.
New dataset - web scraping or public data	Obtaining consent is impossible or takes disproportionate effort, therefore: • only on the lawfulness basis of public interest (thus legitimate interest cannot provide a valid basis in this case); • publicly inform through privacy statement (Section 2.5.7).
Reuse Dataset (secondary use) with special personal data	At the initial data collection, consent was given for special personal data and consent for reuse of data in same/determined research area(s): ○ No new consent required if within designated research area. At initial data collection, no consent was given for special personal data or reuse (for research area new research) ○ Request consent for special personal data unless the exception from the "use of special personal data" block applies (researcher must document reasoned application of exception). Note that the information requirement always applies.

2.4. Purpose limitation

The second requirement is that there must be purpose limitation: there must be a well-defined, explicitly defined purpose for data processing (for more detail, see **Chapter 5 of the Privacy & Personal Data Protection Policy**).

Purpose limitation new dataset	The purpose of processing personal data is to conduct scientific research as referred to in the Higher Education and Research Act and the Dutch Code of Conduct for Research Integrity on [specify purpose of research].
Purpose limitation - secondary use dataset	For scientific research using an existing dataset containing personal data, the purpose is considered compatible with the original purpose for which dataset was collected if the data was collected on the basis of legitimate interest, an agreement, or public interest If the data was collected on the basis of consent or a legal requirement, further processing outside the areas covered by the original consent or legal provision is not possible. Further processing requires new consent or a new legal basis. The purpose of the new processing of personal data is to conduct scientific research as referred to in the Higher Education and Research Act and the Dutch Code of Conduct for Research Integrity on [specify purpose of research].

2.5. Material requirements

2.5.1. Research Data Management Regulations

For the purpose of proper data management and data storage, the **Research Data Management Regulations** were drafted and implemented within TiU.

Research Data Management Regulations	All scientific research is subject to the **Research Data Management Regulations** for the purpose of ensuring adequate data management and data storage.

2.5.2. Ethics Review Boards

Personal data protection directives are minimum requirements if personal data are involved in scientific research. The School's Ethics Review Board[11] may impose additional, more stringent requirements.

Ethics Review Board	The Ethics Review Board may impose additional (more stringent) requirements to what is described in this personal data protection document.

2.5.3. Informed consent

In scientific research, it is important that the data subject is properly informed about the content of the research (on the basis of scientific ethics) and can make the decision to voluntarily participate in the research on the basis of that information. If the basis for processing is consent, use is made of the so-called informed consent form in which the data subject is informed and his consent to participate is demonstrably given.

For more detail, please refer to Section 3.1 which explains when this is or is not necessary.

2.5.4. International research

It regularly happens that Tilburg University researchers collaborate with other universities or conduct research on international populations. This affects the GDPR's scope of application. The GDPR and thus this directive applies to:

International collaborations	• Scientific research involving a Tilburg University researcher. Because the researcher is affiliated with Tilburg University, Tilburg University is involved in the research and, therefore, (co-)responsible for processing. Because Tilburg University is an EU-based institution, the GDPR, therefore, applies even if the research does not involve personal data of EU residents. Please note that in the case of international collaborations, personal data may be transferred to countries outside the European Union.

[11] https://www.tilburguniversity.edu/research/ethics-review-boards

	This is subject to specific directives, for which we refer to the **Privacy & Personal Data Protection Policy.**

2.5.5. Withdrawal of consent

If the processing of personal data is based on consent, then the data subject has the right to withdraw this consent (in addition to the other rights listed below in Section 2.5.6).

Withdrawing this consent must be as easy for data subjects as giving this consent. This means that if it is by means of a form, withdrawal can also be done by means of a form.

If a data subject withdraws his consent, this means the following:

Withdrawal of consent prior to the research	The data subject does not participate in the study, and all his data must be deleted.
During the research	The main rule here is that the data of the person withdrawing consent must be removed from the research database unless this threatens to make the achievement of the purpose of the research impossible or seriously jeopardizes it. In that case, the research data must be completely anonymized so that it is no longer traceable to the person in question. If an entire cohort withdraws consent then the researcher must consult with the Ethics Review Board and the Data Protection Officer. For verifiability of research, however, it is often necessary in the context of research ethics that data can be traced. In the case of anonymization, this is no longer possible. Withdrawal must, therefore, be recorded so that the absence of certain data can be explained (for the purpose of the audit trail).
After the research	After the research is published and thus completed: • Any withdrawal of consent from data subjects must be processed in the dataset intended for future reuse: the research data of those who have withdrawn consent cannot be used for future research. The researcher must ensure that this does not happen; and • The research data, to the extent it has not already been done and is possible, must be completely anonymized so that it is no longer traceable to the individual in question.

2.5.6. Rights of data subjects

The data subject has a number of rights prior to, during, and after the research. For more information, please refer to **Chapter 10 of the Privacy & Personal Data Protection Policy**. A brief summary of the rights that data subjects have:

Right	Data subjects have the right to
Right to be informed	be informed about which personal data are being processed.

Right	Data subjects have the right to
Right of access	be allowed to inspect, at any time, the personal data collected relating to their person.
Right of rectification	to demand that incorrect personal data be rectified at any time.
Right to restriction of processing	limit the processing of their personal data, for example, pending the outcome of an objection. Restriction means that personal data will be marked and may not be processed or shared during this period.
Right of erasure	make a request to erase the data of participation including the answers given by the data subject.
Right to object	indicate that they do not (or no longer) want their data to be processed.

For the aforementioned general rights of data subject, scientific research has certain exceptions in the GDPR regarding:

- Access
- Erasure
- Rectification
- Restriction of processing

A request for access, erasure, restriction of processing, or rectification of personal data does not have to be honored if this could seriously threaten scientific research and if the necessary provisions (for example, security in the form of authorization) have been taken to ensure that personal data can only be used for scientific research. It is of course allowed.
For example, consider research for which erasing or modifying the data will have the implication that the results can no longer be used or generalized.

Furthermore, it is important that Ethics Review Boards can implement guidelines that are stricter than those contained in the law and can require that data subjects be informed of all data stored in the service of research (not just personal data).

Rights of data subjects	Data subjects have the rights of data subjects as set forth in the GDPR (see **Privacy & Personal Data Protection Policy Chapter 10**). The following details apply to scientific research: • Access, rectification, restriction of processing, and erasure do not apply if this could seriously threaten scientific research. Data subjects cannot invoke this. Researcher are allowed cooperate in this, by the way. • The preceding exception applies only if the necessary arrangements have been made to ensure that the personal data can only be used for scientific research. If unclear, consult the School's Ethics Review Board. Please note that if the processing basis is consent, the data subject always has the right to withdraw his Consent. See more detail in Section 2.9. Please note that to invoke rights, data subject must use the standard data subject rights forms.

Responsible for rights to erasure, rectification, and restriction of processing	• First, the researcher shall coordinate with the Ethics Review Board when invoking the rights of erasure, rectification, and restriction of processing. • The researcher informs the Data Protection Officer of the request of the right and decision on it for the purpose of central registration.

2.5.7. Right to be informed

Data subjects whose personal data are processed have the right to be properly informed in advance. Data subjects are usually informed by means of an information letter. This includes information about the purpose of the research, what is expected of the data subject, and where to go with any questions. Subsequently, the data subject is given an informed consent form in which the most important information is listed.

Right to be informed	Data subjects must be clearly and properly informed in advance about the use of personal data processed as part of research. This must be done by: • informed consent (for details see Section 3.1) • privacy statement on website • if reusing existing dataset: by means of information (if the researcher has contact information it must be sent personally and otherwise publicly announced (Internet)).

3. Prior to the Research

This chapter describes the elements of careful handling of data that are important prior to any research in which personal data are processed and the way Tilburg University ensures careful handling of data in this phase of the research. In doing so, this chapter covers the following topics: processing basis for processing personal data in research; informed consent; preparing a Data Management Plan (DMP) prior to the research; conducting the pre-Data Protection Impact Assessment (pre-DPIA); reviewing the DMP; the Data Protection Impact Assessment (DPIA); providing the necessary information for the data processing register; and obtaining informed consent. This chapter also addresses the implications if research data are received from third parties or shared with third parties.

3.1. (Informed) consent

One of the legal processing bases for scientific research is consent. However, in exceptional cases, other processing bases may apply (Section 2.2).
If special personal data are processed in scientific research, explicit consent must be given.

But even if consent is not required based on the GDPR, Tilburg University chooses, for ethical reasons, to seek informed consent from data subjects for new datasets and when reusing existing datasets if reasonably possible.
The chart below shows how consent can be given for the processing of personal data and/or special personal data for the various situations.

This consent must preferably be combined with the informed consent needed from an ethical point of view so as not to overburden the data subject with the various forms. When informed consent is needed follows from Sections 2.2 and 2.3.

Regarding informed consent, the following directives apply.

Informed consent form	For each scientific research in which informed consent is applicable, an informed consent form must be available, which includes the content of the research, duration, possible consequences, risks, and the data subject's rights. The informed consent must (to meet the requirements of consent under the GDPR) include at a minimum: • consent regarding the processing of personal data within this study; • consent for reuse for future scientific research in the same research area; • consent for reuse for future scientific research in other research areas; • description of how the data subject may withdraw consent; • The data subjects' rights, with reference to the privacy statement on the Tilburg University website. In case special personal data are processed in the research, the following must be included:

	• explicit consent for processing of special personal data. Giving informed consent requires an active act that is reproducible. Best practices include signing a separate form or including a tick box in a questionnaire, but an audio recording in which informed consent is explicitly given is also possible.
Statutory representative	If a person is unable to give consent himself (e.g., mental or other type of disability, after death, or other reason), the informed consent form must be authorized by that person's statutory representative.
Minors	If a research involves minors, the following rules apply: • younger than 16: consent of data subject (if possible) and parent/guardian; • from 16 years of age: consent of data subject. It is possible that different (stricter) agreements have been made within Schools. Please note that if personal data of minors is processed then there are additional security requirements for this data. See **Chapter 9 Privacy & Personal Data Protection Policy**.

Requirements	• The data subject must be given sufficient time to read and complete the informed consent form. Preferably, this form must be sent to the data subject in advance so that he can familiarize himself with it.
	• Completed and authorized informed consent forms must be kept securely within the established retention period (Section 5.2):
	  ○ in a locked cupboard/archive,
	  ○ in a (digital) folder accessible only to researcher(s),
	  ○ not linked to the other data collected in the research.

3.2. Drafting a Data Management Plan and data processing register.

A Data Management Plan (DMP) must be drafted prior to the start of the scientific research based on the **Research Data Management Regulations**. Furthermore, within the framework of accountability in the GDPR, the researcher must record the research in the data processing register and conduct a pre-DPIA (for the latter, see Section 3.3). Among other things, the researcher records what data he will collect during a research project, how he stores or manages this data during the project, and what happens to the data after the project ends. The integrated application form for the GDPR, ethical review, and data management is used for this purpose.

3.3. Data Protection Impact Assessment (DPIA).

In some cases, processing personal data poses a high risk to data subjects. In such cases, the GDPR requires that a Data Protection Impact Assessment (DPIA) be carried out to ensure that the protection of the data subjects' privacy is properly safeguarded. The DPIA identifies the risks of data processing in a timely manner by determining what personal data are being processed, what TiU does with them, what the consequences are, and what measures are taken to mitigate the risks.

As indicated above, the researcher must conduct a pre-DPIA. For this purpose, the researcher completes the pre-DPIA form that is part of the integrated application form for the GDPR, ethical review, and data management. Based on the completed pre-DPIA form, the Data Representative can decide whether a DPIA is necessary. A DPIA is usually not required for scientific research. For more detail regarding when a DPIA is required, please refer to the **Privacy & Personal Data Protection Policy Section 11.2**.

Data Management Plan -Data processing register	For each scientific study, the researcher must draw up a Data Management Plan which defines which (personal) data will be processed. Insofar as personal data are processed in the research, this Data Management Plan is included in the university's data processing register. For the format, please refer to the integrated application form for the GDPR, ethical review, and data management.
Pre-DPIA	For any scientific research involving the processing of personal data, a pre-DPIA (questionnaire) must be completed to determine whether conducting a DPIA is necessary. This questionnaire is included in the integrated application form for the GDPR, ethical review, and data management.
Data Protection Impact Assessment (DPIA)	In some situations, it is necessary to conduct a Data Protection Impact Assessment (DPIA). Whether this is necessary results from the Pre-DPIA questionnaire and is decided by the Data Representative. The researcher is responsible for conducting the DPIA if necessary. A procedure is available for this purpose.
Assistance with drafting	The School Data Representative assists in completing the pre-DPIA, DPIA, and data processing register.
Review DPIA	The Data Protection Officer reviews the DPIA, and it is approved by the School's Dean or Vice-Dean for research.
Review Data Management Plan and review by Ethics Review Board.	Further agreements have been made in each School regarding the review of the Data Management Plan (DMP) (by an academic and/or Ethics Review Board) and its storage.

3.4. Privacy statement

Based on the right to be informed, Tilburg University publishes a privacy statement on its website, in which TiU informs about the use of personal data in scientific research. Informing in this way is necessary because not all research can be done with informed consent (e.g., public database, re-use of existing database, or web scraping), and it must be transparent how TiU handles personal data in these types of data as well. It is also possible that certain studies are not included in this list (privacy statement) because of confidentiality or sensitivity of the study (e.g. if we conduct research on an indicator for the presence of hemp farms).

Privacy statement	The privacy statement on scientific research and the list of current scientific research that uses personal data is compiled from the information in the data processing register. This requires no action by the researcher.

	The Ethics Review Board may decide to mark a study as confidential, which means that information about the study in question may not be disclosed in the privacy statement.

3.5. Agreement and processor agreement

It is a legal requirement that, when a researcher exchanges personal data with, provides personal data to, or receives personal data from another organization on behalf of TiU, proper contractual agreements are made. What kind of agreement must be made depends on TiU's role and the role of the other party (controller, processor). For more information, we refer to the **Privacy & Personal Data Protection Policy Chapter 11.4** and the Internet page with models and procedures**.** If a study involves collaboration with other (external) research institutes or parties, a research agreement must be entered into in which arrangements are made for the division of responsibilities etc.; model agreements are available for this purpose.

Situation	Mandatory agreement
TiU is controller and third party is processor	Processor agreement in accordance with established model. See procedure and explanation for more information. Example: storing or processing personal data in application running in the cloud (e.g. Qualtrics)
TiU is a processor for other party responsible for processing	Processor agreement in accordance with established model. Example: commissioned research where the client determines the purpose and means for the research and TiU collects and analyzes the personal data.
TiU is jointly responsible for processing with others or both parties are independently responsible for processing	Arrangements in the research agreement or in separate agreement on division of responsibilities. Consider: • Who regulates the data subjects' rights (access, rectification, etc.), who informs about the processing (privacy statement) and possibly a recourse scheme? • What are parties allowed to do with the data, and does confidentiality apply, for example? Example: commissioned research where the client works with TiU to determine the purpose and means for the research or research where another controller shares data with TiU as an independent controller.
Deviating from model processor agreement	For risk reasons, it is preferable to enter into the standard model agreement. Nevertheless, it may be necessary to deviate.[12] If the researcher wishes to deviate from the standard model he must coordinate with the School's Data Representative. The Data Representative may seek advice from the Privacy & Security Working Group. The processor agreement must be authorized by a signatory, which is usually the Dean, School's Managing Director, or Executive Board.
Responsible for the realization and content of agreement	The researcher must consult the Data Representative and Information Manager prior to entering into the agreement. The

[12] A detailed explanation has been written to accompany the model agreement. This includes which aspects you can deviate from, and the risks involved.

	Data Representative supports this process and may seek advice from the Central Privacy Officer and/or Legal Affairs.
Registration/audit trail	The processor agreement (including motivation in case of deviation) must be archived centrally. For more detail, see **procedure Processor Agreement**.

If third parties with whom personal data is shared are involved during the research, for example for data analysis, collection, or storage, a processor agreement will also need to be entered into with these parties. For further explanation, see **Section 4.4** of this Policy.

4. During the research

This part of the Policy describes the elements of careful handling of data that are important during any research in which personal data are processed and the way in which Tilburg University ensures careful handling of data, especially in this phase of the research. This chapter discusses the handling of contact details of respondents; the rights of participants during the research; the use of programs for collecting, storing, and analyzing data; sharing data, securing of data; and reporting the results.

4.1. Contact details of (potential) respondents

A researcher at Tilburg University who collects and stores contact data in the context of scientific research must, according to the GDPR, store these securely for which limited access is guaranteed. The researcher is responsible for separately storing the file with contact data. The contact data that can be linked to the dataset must be removed as soon as possible (within 6 months unless longer is necessary) by the researcher, as long as this does not conflict with interests of the scientific research.

Storage and access to personal data	Files containing contact information must be accessible only to necessary persons: the principal researchers and manager involved. These files may only be stored in locations approved by Tilburg University. These locations will be communicated through the advice for data storage during the research.

4.2. Change in personal data collected

A researcher may decide during the course of the research that additional personal data is necessary or, conversely, less data is needed. The following directives apply for this:

Change personal data	If there are any changes in the personal data collected during the research, the researcher must: • change the Data Management Plan by means of an amendment and submit it to the Ethics Review Board so that the data processing register is also updated.

4.3. Access and security of personal data

Within Tilburg University, as few people as possible are given access to datasets (digital or physical) concerning research in which personal data have been processed. This access is usually limited to the researchers involved and their managers. We also refer to **Chapter 9 of the Privacy & Personal Data Protection Policy** and the **Information Security Policy.**

Access to personal data files	Access is allowed only to the researchers involved (including student researchers) and the manager (in connection with backup). This must include determining who has access rights to what data (no more than necessary). This access must be logged at least for high-risk processing. In cases where the processing presents a high risk to data subjects, confidentiality agreements must be made with anyone who has access.

Access to archived research data	Access to datasets (digital and physical) containing personal data is permitted only to researchers, the Head of Department, and the administrator of the digital or physical dataset.

Datasets (digital and physical) containing personal data must be stored securely and must be accessible only to those for whom it is necessary in the context of the research.

Secure storage of personal data - digital	Datasets containing personal data must be stored securely. That is: • pseudonymized which means that the connection or communication file is stored separately; • at a TiU-approved data storage location; • only in an encrypted form on a storage medium (laptop, USB); • in case the processing poses a high risk to data subjects, the dataset must always be stored encrypted. • in the absence of the researchers in the workplace, computers and the workspace must be locked.
Secure storage of personal data - physical	Documents containing personal data must be stored securely in a locked cupboard or archive. When absent, cupboards or archives must be locked and inaccessible to unauthorized persons.

4.4. Use of programs to collect, store, analyze, and share data

Data collection during the research can take place in various ways: online, face-to-face, with a paper questionnaire, observations, video footage, etc. The GDPR has implications for these ways of data collection, for the use of existing or new data, for the tools used in data collection, and for any security concerns arising from the GDPR during the research.

When using applications/programs from external suppliers, a processor agreement must be entered into to make proper arrangements about responsibilities, security, etc. For more explanation on this, please refer to Section 3.5 of this Policy and **Section 11.5 of the Privacy & Personal Data Protection Policy.**

Collecting data	If external applications are used to collect personal data: • Preferably use applications already contracted by TiU. These applications have been determined to meet all requirements of the GDPR and have a processor agreement in place. • If the researcher wants to use another application then he must take the initiative to enter into a processor agreement (see Section 3.5).
Storing data	Digital: • See **Research Data Management Regulations** for additional guidance. • All (raw) data must be stored pseudonymized in TiU-approved locations. • If researcher wants to use another (cloud) service: ○ preferably use already contracted applications. These applications have been determined to meet all requirements of the GDPR and have a processor agreement in place.

	○ If the researcher wants to use another application then he must take the initiative to enter into a processor agreement (see Section 3.5). Physical: All personal data must be stored in a locked cupboard or archive. If stored on external location/or by an external administrator then a processor agreement must be concluded with them.
Analyzing data	If, for analyzing data, applications such as SPSS are used: • Preferably use already contracted applications. These applications have been determined to meet all requirements of the GDPR and have a processor agreement in place. • If researcher wants to use another application then he must take the initiative to enter into a processor agreement (see Section 3.5).
Sharing data	• Sharing data with colleagues for co-analysis or peer review of the analysis must only be done if conducted in a secure manner, for example by using encryption (via Secure File Transfer: procedure on intranet). • For use of cloud services, refer to storing data above. • Sharing of data through a cloud service or other programs outside of TiU's control is permitted only if a processor agreement is in place with the relevant party.
Anonymization or pseudonymization	If personal data are no longer necessary (or have to be kept based on the **VSNU Code of Conduct** only for verifiability purposes), but the data cannot yet be deleted, the personal data must be anonymized or pseudonymized at the earliest possible stage.

4.5. Writing and publishing an article

When writing the article, the researcher must avoid including any traceable personal data in the article. There are times when the researcher wants to quote from the research. This is possible if it can be done anonymously. Citations resulting from web scraping may be traceable (easily searchable on the Internet) and, therefore, not anonymous. Preferably, these are paraphrased. A point of attention is the possibility that a combination of data may be traceable to individuals. For example, consider singling out a manager of a large hospital in the Eindhoven region in the age category 45 to 55.

If permission has been requested and obtained, citations may of course be published by name.

Personal data in an article	The researcher must ensure that no traceable personal information is included in the article by: • anonymizing/pseudonymizing research results • On citation: ○ Anonymizing; ○ In case quote was obtained via web scraping: paraphrasing. ○ In case permission has been requested and obtained: publication including name permitted.

Data sharing for review purposes

During the publication process, data may need to be shared with peer reviewers. It goes without saying that personal data must be protected as much as possible.

If datasets are shared without traceable personal data, then this Policy does not apply.

Sharing data with peer reviewers	If personal data is to be shared with peer reviewers:
	• If possible, anonymize or pseudonymize (whereby the key is not sent to the reviewer) (Section 4.3).
	• If this is not possible: agreements have been made with publishers to take technical and organizational measures to protect personal data and to conclude agreements on confidentiality and security obligations with so-called subcontractors (to which we include peer reviewers). However, the researcher is advised that when delivering the dataset:
	  ○ to send it encrypted (see also Section 4.4);
	  ○ to point out that the dataset must be removed by the peer reviewer after it is no longer needed (i.e., in fact, after conducting the peer review).
	• If a raw dataset is required: provide free of traceable personal data.
	• Agree (contractually) that the dataset will be destroyed after the review procedure.

4.6. Rights of data subjects during the research

Data subjects may also invoke a number of rights during the research, see **Section 2.5.6**.

5. After the Research

This chapter of the policy describes the elements of careful handling of data that are important at the conclusion of any research in which personal data are processed and the way in which Tilburg University ensures careful handling of data precisely at this stage of the research. In doing so, this chapter deals successively with retention periods, data packaging, and the data subjects' rights.

5.1. Retention periods

The data collected must be kept carefully and deleted if no longer necessary. The following rules apply to this

Retention period	• The retention period for research data is at least 10 years from the date of the last publication. For medical data, an exception applies in some cases. See also **Research Data Management Regulations.** • The directly traceable personal data (mainly contact details and informed consent) may be kept separately as long as necessary, but no more than 10 years after the date of last publication.[13] Again, an exception applies to medical data in some cases. Please contact the Data Representative in this regard. • There may be national discipline-specific agreements that deviate from these standards. If applicable these are described in the scientific research directives of the respective discipline. • If research did not result in a publication, the maximum retention period of traceable personal data (such as contact information and informed consent) is 10 years after the research is completed. After the maximum retention period for traceable personal data (informed consent), it must be destroyed in a secure manner, under the responsibility of the manager.

5.2. Storage of data

It is important that data be stored carefully after completion of the research in line with the **Research Data Management Regulations**. The following directives apply for this purpose:

Raw data	After completion of a study, the raw data must be carefully stored. This can be done on TiU's servers or those of others if a processor agreement is in place.
Data package	All research data (with the exception of traceable personal data) must be included in a data package according to the university's **Research Data Management Regulations**. The data package (including analysis files and other relevant data) is provided with the full metadata is stored in a Trusted Digital Repository (TDR), such as TiU Dataverse.

[13] For scientific research, it is important that accountability can be provided in the context of scientific ethics. For this, it is important that it is clear which data subjects (respondents) were involved. In connection with the minimum retention period for scientific research, the maximum retention period for informed consent forms is related to this.

If a researcher wants to use another TDR and personal data are present in the dataset, these personal data must be pseudonymized, and a processor agreement must be concluded with the provider of the TDR.

5.3. Rights of data subjects after completion of research

Data subjects may also invoke a number of rights after the research, see **Section 2.5.6**.

Appendix 1: Types of datasets

Audio and video recordings

Audio and video recordings are frequently used in scientific research. Sometimes it will be possible to anonymize these recordings, for example by blurring faces, or filming only hands, but this is highly dependent on the purpose of the research.
Recordings may be used for presentations or publications (for example, in education), and it is important that the data subject is properly informed and gives consent.

Informing data subjects and obtaining consent	• The data subject is clearly informed in advance of making recording through informed consent. • The data subject is properly informed in advance of any use of recordings for presentations and publications and gives specific consent for this.
Use audio or video data	In the case of audio or video recordings in scientific research, it is important that the researcher collects only personal data necessary for the purpose of the scientific research but collects enough personal data to answer the research question. Recording of study results is done if possible (for the purpose of the research) to comply with the directive below. • Do not mention of names (or "masking" them later) • Do not film faces if not necessary (e.g., only hand movements). However, in connection with integrity directives, it is important that the data is verifiable, e.g., who participated in the research. This can be done by pseudonymizing, in the form of communication/connection file and the informed consent forms. **Please note** that if voice of data subject is recognizable then this is never anonymized but pseudonymized; it is after all traceable to person.

Interviews and observations, and experiments in labs

Reports of interviews and observations are often made by researchers. Some studies involve experiments with human subjects in labs. Sometimes this involves measuring special personal data such as blood pressure to see if there is stress.

It is important here to avoid the inclusion of directly traceable personal data (e.g., names) as much as possible.

Informing data subjects and obtaining consent	The data subject is clearly informed in advance of the purpose and method of scientific research through informed consent. If advance information is not desirable because of the purpose of the study (e.g., ethnic discrimination research), then information in informed consent may be general. However, when debriefing the study, this information must be provided (retrospectively).

Administrative handling	It happens that lab participants or respondents are paid for participating in a study. In this case, personal data is processed for the payment (justification financial administration). This is a form of processing of personal data, and therefore, this process must be recorded in the data processing register (not broken down by research) by F&C.
Registration directives	In the case of interviews and observations in scientific research, it is important that the recording (elaboration) of these complies with the directive below: • Do not mention names or other personally identifiable information when recording the interview and observations or lab results. However, in connection with integrity directives, it is important that the data is verifiable, e.g., who participated in the study. This can be done by pseudonymizing, in the form of communication/connection file and the informed consent forms. Please note that additional security requirements apply when processing special personal data. See **Chapter 9 of the Privacy & Personal Data Protection Policy** and **Section 4.2** on special personal data in scientific research.

Eye tracking

Some scientific studies (such as how individuals look at Web sites) use eye tracking to track eye movements. Depending on how this eye tracking is recorded, there may be an increased privacy risk for data subject. This is the case if an iris scan is involved because an iris scan is used as a means of identification (and thus the risk of identity fraud is high for the data subject).

Informing data subjects and obtaining consent	The data subject is clearly informed in advance of the manner and purpose of the study through informed consent.
Eye tracking	In the case of eye tracking in scientific research, it is important that: • only eye movement is tracked, here the iris must not be photographed or scanned due to increased privacy risk of the data subject.

Medical screening (MRI/EEC/ECG)

Some scientific research uses medical screening such as MRIs, EEGs, and ECGs. These are special personal data. The following directives apply to this:

Informing data subjects and obtaining consent	Subject is clearly informed in advance of the manner and purpose of the study through informed consent.
Medical screening EEG, ECG, MRI, etc.	In case of use of medical data, special personal data are processed of which it is important that recording (elaboration) of this complies with the directive below: • Do not mention names or other personally identifiable information when recording the MRI/ EEG or ECG.

	However, in connection with integrity directives, it is important that it is verifiable by means of the data who participated in the study. This can be done by pseudonymizing, in the form of communication/connection file and the informed consent forms. Please note that additional security requirements apply when processing special personal data. See **Chapter 9 of the Privacy & Personal Data Protection Policy** and **Section 2.4** on special personal data in scientific research.

Wearables

If so-called wearables (e.g., Fitbit) are used in a scientific study, the following directives apply.

Informing data subjects and obtaining consent	Subject is clearly informed in advance of the manner and purpose of the study through informed consent.
Wearables	In the case of the use of wearables in scientific research, it is important that the recording (elaboration) of this complies with the directive below: • Do not mention names or other traceable personal data when recording wearables results. However, in connection with integrity directives, it is important that it is verifiable who participated in the study. This can be done by pseudonymizing, in the form of communication/connection file and the informed consent forms. Please note that additional security requirements apply when processing special personal data. See **Chapter 9 of the Privacy & Personal Data Protection Policy** and **Section 4.2** on special personal data in scientific research.

Appendix 2: Responsibilities (RASCI) for scientific research projects

Task	Sub	Deliverable	Accountable	Responsible	Supportive	Consulted	Informed
Monitoring upcoming law and legislation		See general RASCI in Privacy & Personal Data Protection Policy					
Definition of Data Protection Strategy		See general RASCI in Privacy & Personal Data Protection Policy					
Definition TiU Data Protection Regulations		See general RASCI in Privacy & Personal Data Protection Policy					
Definition TiU Research Data Management Regulations.		TiU Research Data Management Regulation	Executive Board	• Data Protection Task Force • Director LIS • Research Data Office	• Data Protection Officer • CISO and ITSO	• Research & Impact Portfolio Holders' meeting • Scientific/Ethics Review Board • Data Representative	• Researchers • Research Support Teams
Execution pre-DPIA		Pre-DPIA	Dean	Researcher	• Data Representative • Data Steward	Scientific/Ethics Review Board	Data Protection Officer
Execution DPIA		Data Protection Impact Assessment	Dean	• Researcher • Data Representative	• Central Privacy Officer • CISO/ISO/ITSO	Data Protection Officer	
Close Agreement with regard to Personal Data Protection	Processor Agreement	Standard model	Dean	Researcher	Data Steward	Data Representative	• Central Privacy Officer • Data Protection Officer
		Adjusted standard model or supplier version	Dean	Researcher	• Legal Affairs • Data Steward	• Data Representative • Central Privacy Officer • Legal Affairs (only mandatory in case of authorization by the Executive Board).	Data Protection Officer

Task	Sub	Deliverable	Accountable	Responsible	Supportive	Consulted	Informed
						Security standards: • Chief Information Security Officer • Information Security Officer • Information Technology Security Officer	
	Other agreements	Data sharing agreement, Joint controller agreement, Standard Contractual Clauses, other	Dean	Researcher	• Legal Affairs • Data Steward	• Data Representative • Central Privacy Officer if necessary • Legal Affairs (only mandatory in case of authorization by the Executive Board). Security standards: • Chief Information Security Officer • Information Security Officer • Information Technology Security Officer	Data Protection Officer
Register Data processing for research project		Record of Processing Activities	Dean	Researcher		Data Representative	• Data Protection Officer • Central Privacy Officer

Task	Sub	Deliverable	Accountable	Responsible	Supportive	Consulted	Informed
Advice regarding Data Protection research		Advice	Data Representative	Data Representative	• Central Privacy Officer • Data Protection Officer • Research Data Office • Data Steward		
Internal Report of Research data breaches or incidents		See general RASCI in Privacy & Personal Data Protection Policy					
Analyze data breaches and report (if necessary) to Supervisory Authority (AP)		See general RASCI in Privacy & Personal Data Protection Policy					
Raise Awareness		Awareness - knowledge data protection	Dean	• Data Representative • Central Privacy Officer	• Data Protection Officer • Legal Affairs • Research Data Office		
Organize Research Data Protection Training and Education		Training and awareness	Dean	Director of Library & IT Services Director University Services	• Research Data Office • Data Representative • Central Privacy Officer • Data Protection Officer • Legal Affairs		
Monitoring - checks on compliance to law and legislation for research projects		See general RASCI in Privacy & Personal Data Protection Policy					

Appendix 3: Definitions.

Concept	Definition
Anonymizing / anonymous data	Data that does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a way that the data subject is not or no longer identifiable (e.g., for statistical or research purposes).
Data subject	An identified or identifiable natural person to whom personal data relates.
Special personal data or special categories of personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and genetic data, biometric data for the purpose of uniquely identifying an individual, or data concerning health, or data relating to an individual's sexual behavior or sexual orientation.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person that enables or confirms unambiguous identification of that natural person, such as facial images, or fingerprint data
Data leak (i.e., "Personal data breach")	A breach of security that accidentally or unlawfully results in the destruction, loss, alteration, or unauthorized disclosure of or unauthorized access to transmitted, stored, or otherwise processed data.
Third party	Any other person, other than data subject, controller, processor, or any person authorized under the direct authority of the controller or process, authorized to process the personal data.
Data Protection Impact Assessment (DPIA) or Privacy Impact Assessment (PIA).	An assessment of the impact of the intended processing activities on the protection of personal data that helps identify privacy risks and provides guidance on how to reduce the risks to an acceptable level.
Traceable personal data	Any personal data that leads to an identifiable person. This can be unique personal data (such as for example *BSN* number) but also a combination of personal data (for example name in combination with an address).
Identification document	Legal identity documents (passport, Dutch identity card, ID card or passport from an EEA country, or a Dutch aliens' document). At TiU, employees and students can also identify themselves with a driver's license and the TiU card with a passport photo.
Informed consent	Consent form that clearly informs the subject about, among other things, the content of the scientific research, their rights.
Personal data	Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is someone who can be identified, directly or indirectly, primarily by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more elements characteristic of that natural person's physical, physiological, genetic, psychological, economic, cultural, or social identity.
Pseudonymization	Processing personal data in such a way that the personal data can no longer be linked to a specific data subject without the use of additional data, provided that such additional data are kept separately, and technical and organizational measures are taken to ensure that the personal data are not linked to an identified or identifiable natural person

Right to restriction of processing	The right to restriction means that the personal data may not be processed (temporarily) and may not be modified. The fact that the processing of personal data is restricted must be clearly indicated in the file by the controller so that it is also clear to recipients of the personal data. When the restriction is lifted again, the data subject must be informed of this. (Article 18 of the GDPR)
Right to object	A data subject may exercise this right to object (which is not comparable to an objection under the Dutch General Administrative Law Act (*Awb*) to the processing of personal data concerning him for reasons relating to his specific situation, if the requirements set forth in the Regulation are met. If a data subject objects, the controller ceases processing unless compelling legitimate grounds dictate otherwise. (Article 21 of the GDPR)
Right to data portability/transferability	This right means that a data subject must be able to obtain data from a data controller in a structured, commonly used, and machine-readable form and has the right to transfer or have the data transferred directly to another data controller without hindrance unless this adversely affects the rights and freedoms of others. A data subject has the right to portability as far as data provided by himself are concerned. (Article 20 of the GDPR)
Right to data erasure/to be forgotten	The controller is obliged to erase personal data of the data subject without unreasonable delay, amongst others, if personal data are no longer necessary for the purposes for which they were collected or otherwise processed; the data subject withdraws his consent and there is no other legal basis for processing; the data subject objects to the processing; the personal data have been unlawfully processed. (Article 17 of the GDPR)
Right to be informed	A data subject must be informed of the fact that processing of his personal data is taking place or will take place and what the purposes of this are. The GDPR indicates what information must be provided in any case, for example, information about the period, the rights of the data subject, the source of data, and the legal basis for the processing. If the purpose of the processing changes, information about this must also be provided. (Articles 13-14 of the GDPR)
Right of access	Data subjects have the right to know whether their relevant personal data are processed by the controller. The GDPR lists the information to which the right of access applies. The controller must provide data subjects with a copy of the personal data being processed. (Article 15 of the GDPR)
Right to rectification	Data subject has the right to rectification of inaccurate personal data concerning him or the right to provide a supplementary statement when processing is carried out on the basis of incomplete data. The rectification must take place immediately. The controller is obliged to notify any recipient to whom personal data have been provided of any rectification unless this is impossible or requires disproportionate effort. (Article 16 of the GDPR).
Respondent	Is a natural person contributing to the research. Is therefore also a data subject within the meaning of the GDPR.
Consent (from the data subject).	Any freely given, specific, informed, and unambiguous expression of the data subject's wishes whereby the data subject signifies, by means of a statement or an unambiguous affirmative action, his consent to the processing of personal data relating to him. (Article 4 under 11 of the GDPR)
Processor	A natural or legal person, public authority, an agency, or other body who/that processes personal data on behalf of the controller.
Processor agreement	The agreement between a controller and processor in which agreements are made regarding the processing of personal data to ensure data protection of data subjects. (Article 28(3) of the GDPR)

Processing	An operation or set of operations involving personal data or a set of personal data, whether or not performed by automated procedures, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction of data
Processing Basis	A basis for processing as listed exhaustively in Article 6 of the GDPR (for example: consent or legal obligation).
Data processing register	The register of the processing activities referred to in Article 30 GDPR in which some data are recorded for accountability purposes.
Controller	A natural or legal person, public authority, agency, or other body who/that, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State (Dutch) law, it may determine who the controller is or according to what criteria he is to be designated.
Web scraping	A computer technique in which software is used to extract a possibly analyze information from web pages. Usually the software attempts to explore a portion of the world wide web using the code-based Hypertext Transfer Protocol (HTTP), or by simulating browsing behavior with a web browser.