Thematic Privacy & Protection Personal Data Policy

Scientific Research—The Use of Personal Data

Readers' Guide

This thematic policy on scientific research is part of the Privacy and Protection of Personal Data Policy and describes, for scientific research purposes, the way in which Tilburg University implements the General Data Protection Regulation (GDPR) with regard to the protection of Personal Data.

The guidelines as included in this Policy only apply if a scientific study uses Personal Data (data that can be traced back to a natural person now or in the future).
If no Personal Data are processed or if they were already completely Anonymized at the time of their acquisition (and can therefore never be traced back to the person), this guideline does not apply. **Caution**! Anonymizing Personal Data is, however, a Processing Operation to which the guideline applies.

For the sake of readability, we have divided this policy into three phases based on the different phases of research:

All information relating to European legislation (GDPR) and the Protection of Personal Data can be found on a Tilburg University website[1], including Frequently Asked Questions. Practical elaborations and examples can also be found on this website.

The Policy includes references to other policy documents. These are marked as "**referrals**." The applicable guidelines are set out in blocks to make them easy to find:

Subject	Rules and guidelines with which Research must comply in the area of the Protection of Personal Data

Many definitions are included in this policy (see **Appendix 2**). The terms that can be found in the definition list are underlined.

Research normally involves collecting more data than just Personal Data. However, this Policy focuses mainly on the legal aspects relating to Personal Data.

Each School/Division within Tilburg University has appointed so-called Data Representatives[2]. They are the first point of contact for employees in the event of questions about the Protection of Personal Data. For questions about data management, data storage, and data archiving for

[1] https://www.tilburguniversity.edu/intranet/support-facilities/legal/legalprotection/privacy/
[2] https://www.tilburguniversity.edu/intranet/support-facilities/legal/legalprotection/privacy/contact/

which Personal Data may or may not be processed, the researcher can contact the Research Data Office (RDO). For more details, please refer to the **Research Data Management Regulations**.

This Policy contains general points of reference for researchers. However, the lawful use of Personal Data in scientific research **depends on the facts and circumstances per case**. The researcher must, therefore, consider, on a case by case basis, whether the processing complies with this Policy, the general Tilburg University Privacy and Protection of Personal Data Policy, and the applicable legislation and remains responsible for this.

At the time this Policy was drawn up, the VSNU's new Code of Conduct for the use of personal data in scientific research was still being developed, which is why the new version was not included in the formulation of this Policy. Once the Code of Conduct has been definitively adopted, this Policy will be evaluated and brought into line with the Code of Conduct. In addition, the European Union is expected to issue additional regulations (e.g., in the form of WP29 opinions) that may have an impact on the content of this guideline.
Moreover, practice will have to show which research disciplines will require further interpretation of this Policy.

The policy will, therefore, be reviewed and revised annually at least, unless earlier revision is necessary on the basis of amended legislation and regulations or changed policy positions.

When *he* is referred to in this policy, it is understood to mean he/she or gender-neutral.

Contents

1. Introduction 6

2. General Guidelines 8

2.1. Use of Data Sets 8

2.1.1. Setting up a new data set with Respondents 9

2.1.2. Use of pre-existing data sets (Secondary use) 9

2.1.3. Use of public data sets 10

2.1.4. Data set based on Web Scraping 11

2.2. Lawfulness—Processing Basis 12

2.3. Lawfulness— Processing Basis Special Personal Data 14

2.4. Purpose Limitation 15

2.5. Research Data Management Regulations 16

2.6. Ethics Review Boards 16

2.7. Informed Consent 16

2.8. International Research Projects 16

2.9. Withdrawal of Consent 17

2.10. Rights of Respondent 18

2.10.1. Right to Be Informed 19

3. Prior to the Research 19

3.1. Informed Consent- consent for Processing of Personal Data 19

3.2. Drawing up a Data Management Plan 22

4. During the Research 24

4.1. Contact Details of Respondents or Potential Respondents 24

4.2. Changes in the Personal Data Collected 24

4.3. Access and Security of Personal Data 25

4.4. Use of programs to collect, store, analyze, and share data 25

4.5. Contract and Processing Agreement 27

4.6. Writing and Publishing an Article 28

4.7. Rights of the Respondents during the Research 28

5. After the Research 29

5.1. Storage Period 29

5.2. Data Storage 29

5.3. Rights of the Respondents after the Research 30

Appendix 1: Types of Data Sets
Appendix 2: Responsibilities (rasci)
Appendix 3: Definitions

Flow chart for researcher – in progress

Flowcharts

To be developed

1. Introduction

This guideline shall **apply only if Personal Data are processed in the course of scientific research**. If no Personal Data are processed, this guideline does not apply.

An item of Personal Data is

---

any information that can identify a natural person or information that can be traced back to that person now or in the future.

This definition of Personal Data is based on the GDPR and is very broad.

There is a difference with Pseudonymizing and Anonymizing. In the case of Pseudonymization, identifying data are separated from non-identifying data and replaced with artificial identifiers. An example of Pseudonymization is the replacement of a Respondent's data in a medical survey by a unique respondent number. The medical data will then be linked to this respondent number instead of name, address, and place of residence. As a result, outsiders cannot see who the person is to whom the medical data belong. Only the person who can make the link between the respondent number and the name (e.g., the researcher) is able to link the medical data. However, sufficient (organizational and technical) measures must be taken so that unauthorized persons cannot link these files. In the case of Pseudonymization, the GDPR, and hence this guideline, is applicable.

For Anonymous data, the GDPR is no longer applicable. Please note that with Anonymous data there is no longer any possibility for identification or tracing back to persons. Anonymization is a processing operation and still falls under the GDPR. If data can still be traced back to a person, there is no Anonymization.

If data can be traced back to persons, then we speak of Personal Data. This can, therefore, be either directly traceable Personal Data (such as a name, e-mail) or indirectly traceable Personal Data (for example, license number or a combination of initials and zip code and house number).

In scientific research a lot of work is done with Respondents. Tilburg University attaches great importance to the careful Processing of Personal Data in the context of scientific research because the misuse of data can cause great damage to Respondents, employees, students, and Tilburg University. A good balance is sought between privacy, security, and functionality.

This Policy applies to all Processing of Personal Data that takes place within the framework of scientific research under the responsibility of Tilburg University and applies to everyone working under the responsibility of Tilburg University.

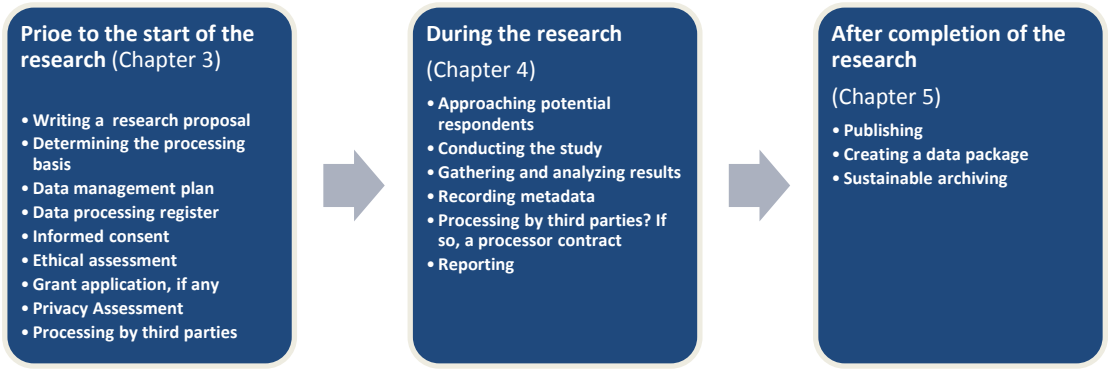
Processing is understood to mean the processing of Personal Data, whether or not automated, such as collecting, recording, structuring, storing, modifying, analyzing, retrieving, consulting,

using, providing (forwarding), distributing, making available, combining, shielding, or erasing data. In other words, everything you do with Personal Data.

It concerns Processing of Personal Data in a paper file or archive, digital file, or in an application/system (including in mailboxes and on computers or other data carriers such as USB sticks) and the Policy applies **to all Personnel (also Personnel Not on Payroll) including student assistants, temporary or hired staff, interns, (external) PhD candidates, and students who contribute to the research**. Therefore, this concerns all the Processing of Personal Data carried out by researchers in the context of scientific research.

The GDPR talks about the Data Subject; in scientific research this mainly concerns Respondents (also referred to as human subjects or participants). The term Respondents will, therefore, be used from now on.

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 points for attention when it comes to the protection of Personal Data for the researcher to take into account.



A research shall be conducted under the direction of a researcher. He is responsible for compliance with this Policy and for ensuring that everyone who cooperates in the research under his responsibility (e.g., (external) PhD candidates, student assistants, and students) adheres to this Policy on the protection of Personal Data.

Responsible	There are various forms of responsibility for research:
	• when using of the facilities offered by Tilburg University, the **researcher** himself is responsible for:
	  ○ compliance with the university's **Privacy & Protection of Personal Data Policy** (including this Thematic Policy) and, therefore, the GDPR and the **Research Data Management Regulations**;
	  ○ ensuring good data management and data storage in accordance with the principles in the **Research Data Management Regulations**;
	  ○ drawing up a Data Management Plan prior to a new research in accordance with the School's data management policy; and
	  ○ Ensuring that PhD candidates and students (who work under the responsibility of the researcher) comply with the Regulations and the Policy as mentioned above.
	• The **Dean** of the School in question is responsible for:

- the implementation of the **Privacy & Protection of Personal Data Policy** with regard to scientific research within the School (possibly on the basis of the School policy);
- informing the scientific staff about this Policy; and
- supervising compliance with this Policy and accounting for this to the Executive Board.

- The **Executive Board** is responsible for:
  - drawing up a general university policy framework as laid down in the **Privacy & Protection of Personal Data Policy**,
  - offering flanking knowledge, advice, and guidance with Processing Personal Data;
  - providing an adequate infrastructure for data storage and management; and
  - conducting audits or supervising audits, respectively.

2. General Guidelines

The guidelines mentioned in this Chapter are general guidelines that do not apply specifically to one of the phases of scientific research and concern the following subjects.

- Use of Data Sets (**Section 2.1**)
- Lawfulness—Processing Basis (**Section 2.2**)
- Lawfulness— Special Personal Data (**Section 2.3**)
- Purpose Limitation (**Section 2.4**)
- Research Data Management Regulations (**Section 2.5**)
- Ethics Review Board (**Section 2.6**)
- Informed Consent (**Section 2.7**)
- International Research Projects (**Section 2.8**)
- Withdrawal of Consent (**Section 2.9**)
- Rights of Respondents (**Section 2.10).**

2.1. Use of Data Sets

Prior to the start of a research project, the researcher concerned shall decide whether to collect data himself or whether to use existing data sets or a combination of these. This process takes place at the same time as the application for the ethical assessment (if applicable).

In scientific research, paper or digital data sets are often used that also contain Traceable Personal Data. This may concern:

- setting up a new data set with Respondents (**Section 2.1.1**)
- reuse of data sets already collected (secondary use) (**Section 2.1.2**)

In addition, there are specific guidelines for the use of public data sets and in the case of Web Scraping with which Personal Data are collected.

- use of public data sets (**Section 2.1.3**)
- data set based on Web Scraping (**Section 2.1.4**).

2.1.1. Setting up a new data set with Respondents

In a scientific study, you can create a new data set by collecting data from Respondents or by combining two existing (public or otherwise) data sets. A data set can be in the form of a file, but other forms such as video and audio recordings, interviews, score forms, eye tracking, etc. also fall under this definition. These Respondents can be recruited by the researcher himself, for example, by means of a call for participation or from a human subject pool.

Respondents	For Respondents, it is important that they voluntarily participate and that they are **well informed in advance** about the research with regard to, among other things, the Protection of Personal Data. This must be done by means of an Informed Consent Form (**Sections 2.7 and 3.1**). If the Processing Basis requires consent or if Special Personal Data are processed, additional requirements apply. (**Section 2.3**)
Data minimization	If Traceable Personal Data are necessary for scientific research: • The researcher may **only collect Personal Data that are necessary for the purpose of the scientific research (as little as possible)** but ensures that sufficient data are collected to answer the research questions. See **Privacy & Personal Data Protection Policy, Chapter 6.**
Security	If Personal Data are used for research, these need to be Processed in such a way that they are adequately secured. **Privacy & Personal Data Protection Policy, Chapter 9**
Information requirement	Respondents have the Right to Be Informed and should be well informed. See **Section 2.10** for the Data Subject's Rights and the **Privacy & Personal Data Protection Policy, Section 10.3.**
Registration	Research needs to be recorded in the Data Processing Register. (**Section 3.2**)

2.1.2. Use of pre-existing data sets (Secondary use)

During scientific research, it regularly happens that data collected for another research is reused in a new research. This is referred to as secondary use, for which the GDPR has included specific regulations (Article 5(1), under b). The use of an already existing data set is permitted on the basis of the GDPR because of the importance of scientific research under conditions (Article 89) such as appropriate safeguards, technical and organizational measures, Pseudonymization, et cetera.
If existing data sets are reused, only Anonymized or Pseudonymized data will be shared where possible, with the researcher not receiving the interconnected file in the case of Pseudonymized data.

In the case of Special Personal Data (Article 9(2) subsection j, GDPR) an additional test applies in the case of Scientific Research: it is only permitted if necessary, proportionate, and appropriate measures are taken.

Finally, pursuant to Article 14(5b) of the GDPR, the Data Subject has the right to be directly informed about the Processing if the Personal Data was not received from the Data Subject,

unless this requires a disproportionate effort. In the latter case, the Data Subject must be either informed himself or publicly (by means of a Privacy Statement).

Anonymize or Pseudonymize	When using existing data sets, Personal Data should be Anonymized as much as possible. If the primary data set is Anonymized, this guideline no longer applies, and the Data Processing Register does not need to be updated either. If Anonymization is not possible, Personal Data must be Pseudonymized as much as possible. The GDPR and this guideline are applicable to this. See a further explanation below.
Data minimization	If Traceable Personal Data are necessary for scientific research: • the researcher may **only collect Personal Data that are necessary for the purpose of the scientific research (as little as possible)** but ensures that sufficient data are collected to answer the research questions.
Security	If Personal Data are used for research, these need to be Processed in such a way that they are adequately secured. See **Privacy & Personal Data Protection Policy, Chapter 9.**
Information requirement	Respondents have the Right to Be Informed and should be well informed. See **Section 2.10** for the Data Subject's Rights.
Registration	Research needs to be recorded in the Data Processing Register (**Section 3.2**).

2.1.3. Use of public data sets

In scientific research, public data sets, in which not easily traceable Personal Data are included, are often used. A distinction can be made between:

- public data sets that can be downloaded, such as data from Statistics Netherlands (CBS), the European Social Survey, and the World Value Survey (WVS). These data sets contain Personal Data, but these are Anonymized[3] or Pseudonymized (in which case Tilburg University does not have the key for linking the data sets) and, therefore, (by Tilburg University) cannot be traced back to persons. Therefore, these data sets without traceable Personal Data do not fall under the GDPR. Often, when using these data sets (when concluding a license) you will have to declare a number of things, for example, that you are not using them commercially.
- Public databases that can be used by means of a license.

Please note that if two public data sets are combined, there may be traceable Personal Data (in the future).

Use public data sets	When public data sets are used, Anonymized or Pseudonymized Personal Data (without an interconnecting file) will, **in principle**, be used that can, therefore, not be traced back. The researcher must guarantee that the requirements set out in the license or when downloading are met and that the Personal Data are not Traceable.

[3] Anonymized datasets do not contain Personal Data and are, therefore, not subject to this guideline.

	Please note: If the public data set or the combination of these sets contain Personal Data that are Traceable, the research must meet all requirements as set out in this Policy. The Data Representative can assist in determining whether this is necessary.

2.1.4. Data set based on Web Scraping

In addition to public data sets, Web Scraping from public or semipublic sources is regularly used. If a researcher wants to scrape forums, social media, or other public or semipublic websites, copyright and conditions of use of the public source may apply.

Use of Web Scraping	For scientific research, a researcher may use **Web Scraping** to process Personal Data under certain conditions if they are **public** and have been collected for a similar purpose. This also applies to Special Personal Data that have clearly been disclosed publicly by the Data Subject himself. **Please note**: copyright and terms of use of the public source may apply. For more details, see the **Copyright Information Point** on the Intranet.

In addition, the researcher must also take into account the context in which the public information is placed. The public information may be used for scientific research if it was written for this purpose. This also expressly applies to Special Personal Data that have been clearly disclosed publicly by the Respondent himself. Here are a number of examples for clarification:

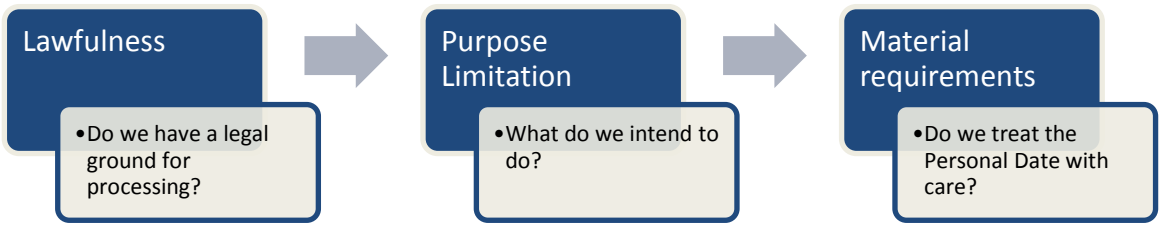
- *If a researcher uses Airbnb blogs (in which travelers display their experiences) that are public to determine whether tourists are ethnocentric. When writing the blogs, the authors could not have suspected how their texts would be used and they might not have given consent if requested. This information may not be used and the researcher must request explicit consent from the authors of the blogs.*
- *When a researcher uses a public blog on Facebook in which someone writes about personal experiences with cancer with the aim of informing fellow sufferers and relatives. In this case, the researcher may use this information if he uses it to compare patient experiences.*
- *If a researcher makes use of a blog on a closed forum that is not public (but for which the researcher receives access for the purpose of the research), it may not be used for scientific research (unless the researcher has specific consent (Informed Consent) from the Data Subject.*

Appendix 1 contains a number of examples of types of data sets in which Personal Data are processed for which specific guidelines are given for the various types of research, such as

- video and audio recordings,
- interviews,
- observations,
- experiments in labs (including virtual reality labs),
- eye tracking,
- ECG/EEG/MRI
- Wearables
- ….

The list above is not exhaustive: other examples that are not mentioned are, of course, also covered by this Policy.
Tilburg University considers the information collected in such researches to be Personal Data. This policy choice is made because patterns from such studies may be traceable to Persons in the future.

If Personal Data are processed in a scientific study, the so-called Lawfulness and Purpose Limitation must first be established. In the following, the so-called Material requirements must be observed in order to ensure that Personal Data is handled with care.



2.2. Lawfulness—Processing Basis

Any processing of Personal Data must be lawful, i.e., there must be a legal Processing Basis and purpose for the processing. The six legal Processing Bases have been explained in detail in the **Privacy & Personal Data Protection Policy**.

The following Processing Bases apply to scientific research, which depend on how the researcher composes a data set.

- setting up a new data set directly from Respondents,
- setting up a new data set not via Respondents (e.g., Web Scraping),
- using an existing data set.

Please note: 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 DATA SET DIRECTLY FROM RESPONDENTS	In general, the Processing Basis is the **Data Subject's consents**. In **exceptional situations**, however, one of the Processing Bases below may also apply: • **necessary for the performance of a task of public interest**, • **necessary for a legitimate interest**: in doing so, a balance must be struck between the interest of scientific research and the Respondent's interest in terms of privacy. For more information about the various Processing Bases, please refer to the **Privacy & Personal Data Processing Policy, Section 4.2**. Whether and if such an exception applies, this should be well documented and motivated by the researcher and recorded in the research questionnaire. If necessary, the Data Representative can render advice on this.

	It is essential that the Respondent's interests are properly safeguarded during the research in terms of the design of the research and the management/security of Personal Data. For this, see the requirements at the various points of the research life cycle. *Example:* • *Certain forms of medical research for the benefit of public health may be based on the Processing Basis task of public interest.*
Processing Basis NEW DATA SET not VIA Data Subject – public data	The Processing Basis for scientific research involving the creation of a new data set in which research data are collected without being available directly from Respondents is **legitimate interest**. In this case, the research data are collected on the basis of information disclosed publicly by the Respondent himself. *Example: setting up a new data set using Web Scraping. See also **Section 2.1.4**.*

In the case of secondary use of data sets already collected, a distinction should be made in a number of scenarios to determine which Processing Basis may apply:

- Initial data collection is based on **Consent**:
  i. Consent for reuse for future research & new research will be granted in the area of research for which consent was granted.
  ii. Consent for reuse in future research & new research takes place in **another research area**
  iii. **no Consent for reuse** for future research.
- Initial data collection **is not** based on Consent but on **another Processing Basis**.

Processing Basis SECONDARY: Consent reuse for the SAME area of research	Processing Basis is **Consent** but the researcher does **not** have to ask for **new Consent**. There is, however, a duty to provide information: ○ Disposes of the contact details of the Data Subject: personal information if this does not require a disproportionate effort[4]. ○ Does not dispose of the contact details: inform publicly **Please note**: When Consent is given, a Respondent may always withdraw it: if this happens, then the Respondent's data may no longer be used for follow-up research in so far as this can be traced back. See **Section 2.9** for guidelines on withdrawal of Consent. *Example: a researcher uses the data of an earlier research for a follow-up research within the same research area. This earlier research is based on Consent and the Respondent has agreed that his data are used in future research*.
Processing Basis SECONDARY: Consent reuse for ANOTHER area of research	The Processing Basis is **Consent**. Because no Consent has been requested for this research area in the primary research, Consent should be requested if this is reasonably possible:

[4] Disproportionate effort could, for example, be applicable in the case of very large databases for which many Respondents need to be approached. If this exception is chosen, it must be recorded by the researcher (stating the reasons).

	○ Disposes of the contact details of the Data Subject: ask for personal Consent ○ Does not dispose of the contact details: Processing Basis is legitimate interest: inform publicly based on the Right to Be Informed. *Example: a researcher uses the data of an earlier research for a follow-up research within another research area. This earlier research took place in the research area of marketing and the Respondent was asked for Consent for reuse but only within the field of marketing. The new research will take place within the research area of law.*
SECONDARY: no consent for reuse	In principle, the Processing basis is Consent but could in exceptional cases also be one of the other bases mentioned above (e.g., legitimate interest). The researcher must still request **Consent** for the reuse of this data if this is possible. *Example: A researcher uses the data of an earlier research for a follow-up research. In this earlier research, no Consent was requested for reuse. If possible (disposal of contact details), the researcher must still request Consent. 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. He must record this assessment in the research questionnaire.*
SECONDARY: primary data set NOT based on CONSENT	In this case, the Processing Basis for the reuse of data could be legitimate interest, in which case the researcher has to weigh up the interest of the scientific research against the privacy interest of the Respondent. He must record this assessment in the research questionnaire.

2.3. Lawfulness— Processing Basis Special Personal Data

According to the GDPR, Special Personal Data may only be processed under strict conditions. Scientific research is exempted from the prohibition of processing Special Personal Data, under certain conditions. See the **Privacy & Personal Data Protection Policy, Section 4.3.**

Special Personal Data	Special Personal Data are: • Racial or ethnic origin • Political views • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data for identification purposes • Health data (medical data) • Data relating to sexual behavior or sexual orientation This data may only be Processed in accordance with **Section 2.3**. **Please note**: If Special Personal Data are processed, there are additional security requirements. See **Chapter 9 of the Privacy & Personal Data Protection Policy**.
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 involves a disproportionate effort**, 2. processing is **necessary for research purposes**; and 3. the **research** serves **a public interest**. **Safeguards** must also be provided **in such a way that the private life of the Data Subject is not disproportionately harmed**. For the various types of data sets, an elaboration is given below
NEW data set with Special Personal Data – received DIRECTLY FROM THE RESPONDENT (not by means of Web Scraping or public data)	**Consent is mandatory** (Informed Consent): the Respondent must give his explicit Consent on the Informed Consent Form to the Processing of the Special Personal Data.
NEW data set – WEB SCRAPING OR PUBLIC DATA	Getting Consent is impossible or involves a disproportionate effort: • Inform publicly by means of Privacy Statement (**Section 2.10.1**).
REUSE DATA SET (SECONDARY USE) with Special Personal Data	**Consent given for Special Personal Data at initial research and Consent given for re-use of this data in the same/defined area or areas of research:** ○ No new Consent required if used within specified research area. However, informing the Data Subject is required. **In case NO Consent for use or reuse of Special Personal Data was given for the initial research (for research area of new research)** ○ Ask for permission for Special Personal Data unless the aforementioned exception applies (researcher must record the application of the exception, stating the reasons) **Initial Research PUBLIC data:** no specific Consent in connection with publication data **Please note**: the Information requirement is always applicable.

2.4. Purpose Limitation

The second requirement is that there must be Purpose limitation: there must be a specific, clearly defined purpose (for more details, see of the **Privacy & Personal Data Protection Policy, Chapter 5**).

Purpose Limitation new data set	The purpose of the Processing of Personal Data: Performing scientific research as referred to in the Dutch Higher Education and Research Act and the Netherlands Code of Conduct for Scientific Practice (complete with THE PURPOSE OF THE RESEARCH).

Purpose Limitation – secondary use data set	• Scientific research using an existing data set containing Personal Data is always considered compatible with the original purpose for which the data set was collected. • The purpose of the new processing of Personal Data is: Performing scientific research as referred to in the Higher Education and Research Act and the Netherlands Code of Conduct for Scientific Practice (complete with THE PURPOSE OF THE RESEARCH)

2.5. Research Data Management Regulations

For the purpose of good data management and data storage, the **Research Data Management Regulations** were drawn up and implemented within Tilburg University.

Research Data Management Regulations	The **Research Data Management Regulations** apply to all scientific research involving the processing of Personal Data for securing adequate data management and data storage.

2.6. Ethics Review Boards

The guidelines on the Protection of Personal Data are minimum requirements in the case of Personal Data in scientific research. The Ethics Review Boards within the Schools may impose additional, more stringent requirements.

Ethics Review Board	The Ethics Review Board may impose additional and more stringent requirements to what has been described in this document regarding the Protection of Personal Data.

2.7. Informed Consent

In the case of scientific research it is important that the Respondent voluntarily cooperates in the research and is well informed about the content of the research (based on scientific ethics). If possible, this is done by using the so-called Informed Consent Form in which the Respondent is informed and gives his Consent for participation.

If the Processing Basis is Consent or there is Processing of Special Personal Data, the Respondent must give his Consent for this. This Consent must be demonstrable and can be combined with the Informed Consent Form. This is not necessary: it can also be done separately.

For more details, we refer to **Section 3.1** in which it is explained when this is necessary or not.

2.8. International Research Projects

Tilburg University researchers regularly collaborate with other universities or conduct research into international populations. This affects the GDPR's scope of application. The GDPR and thus this guideline apply to the following:

International Collaborations	• **Scientific research involving a researcher from Tilburg University.** After all, the researcher is responsible or co-responsible, which means that the GDPR applies even if the research does not concern EU citizens' Personal Data. **Please note** that international collaboration may involve transfers to countries outside the European Union. This is subject to specific guidelines for which we refer to the **Privacy & Personal Data Protection Policy**.

2.9. Withdrawal of Consent

If the Processing of Personal Data is based on Consent, the Data Subject will be entitled to withdraw the Consent (in addition to the other rights referred to in **Section 2.10** below). No exception applies to scientific research either.

Withdrawing the Consent should be as simple for Respondents as giving the Consent. This means that if this was done by means of a form, this can also be done by means of a form.

If a Respondent withdraws his Consent, this means the following:

Withdrawal consent prior to the research	The Respondent does not participate in the research and all his data must be erased.
During the research	The main rule here is that the data of the person withdrawing his consent must be removed from the research database UNLESS, this threatens to make it impossible to achieve the objective of the research or seriously jeopardize it. In that case, the research data must be completely Anonymized so that it can no longer be traced back to the person in question. If a full cohort withdraws its Consent, the researcher must consult with the Ethics Review Board and the Data Protection Officer. In order for research to be verifiable, it is often necessary in the context of scientific ethics for data to be traceable. Anonymization makes this no longer possible, but the substantiation of this (and therefore verifiability) can take place by recording the withdrawal of the Consent (audit trail).
After the research	If the research has been published and thus completed: • If this has not been done yet, the research data must be completely Anonymized so that it can no longer be traced back to the person in question; and • If the withdrawal of the Consent has consequences for the future reuse of the data set, the research data of the persons who have withdrawn their Consent may NOT be used for future research. The researcher must guarantee that this does not happen.

2.10. Rights of Respondent

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

Right	Respondents have the right to
Right to be informed	be informed about which Personal Data are being processed.
Right of access	have access, at all times, to the Personal Data collected in relation to their person.
Right to rectification	at all times, demand that incorrect Personal Data be rectified.
Right to restriction	restrict 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 edited or shared during this period.
Right to erasure	make a request to erase the data of the participation including the answers given by the Respondent.
Right to object	indicate that they do not or no longer want their data to be processed.

The aforementioned general rights of the Data Subject are subject to certain exceptions in the GDPR relating to scientific research regarding:

- Access
- Erasure
- Rectification
- Restriction

Access, erasure, restriction, or rectification of Personal Data need not be honored if this could seriously threaten the scientific research and if the necessary measures (for example, security in the form of authorization) have been taken to guarantee that Personal Data can only be used for scientific research. Of course, you are allowed to remove the Personal Data.
Think, for example, of research in which the erasure or modification of the data means that the results can no longer be used or generalized.

It is also important for Ethics Review Boards to be able to apply guidelines that are stricter than those set out in the law and to demand that Respondents be informed of all data that is stored for the purpose of the research (not only the Personal Data).

Right of Respondents	Respondents have the Rights of the Data Subjects as referred to in the GDPR (see **Privacy & Personal Data Protection Policy, Chapter 10**). The following details shall apply to scientific research: • Access, Rectification, Restriction and Erasure are not applicable if they may pose a serious threat to scientific research. Respondents cannot rely on this. However, researchers are allowed to cooperate in this matter. • The before mentioned exception only applies if the necessary provisions have been made to guarantee that the Personal Data can only be used for scientific research purposes.

	If it is unclear, the School's Ethics Review Board should be consulted. Please note: if the Processing Basis is Consent, the Respondent will always be entitled to **withdraw** his **Consent**. See **Section 2.9** for more details. **Please note** that the Respondent must use the **standard forms** on Data Subject's rights in order to invoke his rights.
Responsible for rights to erasure, rectification, and restriction	• The researcher, first of all, discusses the invocation of the Rights of Erasure, Rectification, and Restriction with the Ethics Review Board. • The researcher shall inform the Data Protection Officer of the invocation of the right and the decision thereon for the purpose of central registration.

2.10.1. Right to Be Informed

Data Subjects whose Personal Data are processed have the right to be well informed in advance.

Right to be informed	Respondents must be clearly and well informed in advance of the use of Personal Data processed in the context of research. This must be done by means of: • Informed consent (see **Section 3.1** for details) • Privacy Statement on the website • In case of reuse of an existing data set: by information (if a researcher has contact details, these should be sent personally and otherwise be announced publicly (internet)).

3. PRIOR TO THE RESEARCH

This Chapter describes the elements of careful handling of data that are important prior to each research in which Personal Data are processed and the way in which Tilburg University guarantees the careful handling of data at this stage of the research. This Chapter deals successively with the Processing Basis for processing of personal data in research; the Informed Consent; the drawing up of a Data Management Plan (DMP) prior to the research, including carrying out the pre-Data Protection Impact Assessment (pre-DPIA) as part of the DMP; validating the DMP, the Data Protection Impact Assessment (DPIA), the Data Processing Register; and obtaining Informed Consent.

3.1. Informed Consent- consent for Processing of Personal Data

One of the legal Processing Bases for scientific research is the CONSENT of the Respondent. In exceptional cases, however, other Processing Bases may also apply (**Section 2.2**).
If Special Personal Data are processed in the course of scientific research, explicit Consent must be given.

However, even if no Consent is required on the basis of the GDPR, Tilburg University chooses, for ethical reasons, to request Informed Consent from Respondents for new data sets and, if this is reasonably possible, for the reuse of existing data sets.

The overview below includes how Consent can be given for the processing of Personal Data and/or Special Personal Data in the various situations.

This Consent should preferably be combined with the Informed Consent required from an ethical point of view in order not to overburden the Respondent with the various forms. The overview below includes the various situations in which this Consent is granted in the context of the GDPR.

Type of data set	Processing Basis	Special Personal Data	Informed Consent?
New data set – Collect Respondents' data yourself	**Consent**	**no**	**Yes**, Informed Consent for all Respondents regarding: ○ Processing Personal data ○ Consent for future reuse ○ indicate possibility of withdrawing Consent **Tip**: describe the research area as broadly as possible for possible reuse in the future.
	Consent	**Yes**	See previous and including: ○ Explicit Consent for the Processing of Special personal data
	Other grounds	**no**	**Yes**, Informed Consent for all Respondents on the basis of scientific ethics. No Consent for the use of Personal Data.
	Other grounds	**Yes**	See previous and including: ○ Explicit Consent for the Processing of Special Personal Data
New data set – NOT DIRECTLY FROM THE RESPONDENTS	Legitimate interest	**No**	**No**, only public information via privacy statement (Section 3.2).
	Legitimate interest	**Yes**	**Yes**, requesting Informed Consent with explicit consent for processing Special Personal Data unless this is impossible or requires a disproportionate effort. Always public information (Privacy Statement).
Reuse existing data set	Initial research consent for research area and reuse	**No/Yes**	**No**, but inform in person if this is reasonably possible, otherwise inform publicly (Privacy Statement) (Section 3.2).
	Initial research consent for reuse **other research area** **or** **Initial research no consent for reuse**	**No/Yes**	**Contact details** available: Informed Consent regarding: ○ Processing Personal Data ○ if applicable: explicit consent for the Processing of Special Personal Data ○ Consent for future reuse ○ indicate possibility of withdrawing Consent **No contact details available**: inform publicly (Privacy Statement) (Section 3.2).

			Please note: for Special Personal Data, additional requirements apply to the exception of no explicit Consent, see **Section 2.3**.
	Initial research NO consent	**No/Yes**	**Contact details** available: Informed Consent regarding: ○ Processing Personal Data ○ if applicable: explicit consent for the Processing of Special Personal Data ○ Consent for future reuse ○ indicate possibility of withdrawing Consent **No contact details available**: inform publicly (Privacy Statement). **Please note**: for Special Personal Data, additional requirements apply to the exception of no explicit Consent, see **Section 2.3**.

Regarding Informed Consent the following guidelines apply.

Informed Consent Form	For every scientific research to which Informed Consent applies in the diagram above, a so-called Informed Consent Form must be present which includes, amongst other things, the content of the research, duration, possible consequences, risks, and rights of the Respondent. If the **Processing Basis** is **CONSENT**, then informed consent must minimally contain the following information: • Consent for the Processing of Personal Data • Description of how the Respondent can withdraw his Consent. • Preferably, Consent for reuse for future scientific research. • The Data Subject's rights with a referral to the Privacy Statement on the Tilburg University website. If Special Personal Data are processed during the research, the following must be included: • Explicit Consent for the Processing of Personal Data. The Respondent must authorize the Informed Consent (by means of a signature, digitally, or on an audio recording) so that his Consent is reproducible. The Informed Consent can be obtained by means of a separate form or can also be included in a questionnaire in which, in case of consent (for Processing Personal Data and/or Special Personal Data), the Respondent must click on a tick box (explicit action).
Statutory representative	If a person is not able to give the Consent himself (e.g., mental or other disability, after death, or for any other reason), the Informed Consent Form must be authorized by this person's legal representative.
Minors	If minors are involved in a research, the following rules shall apply: • under 16 years: Consent of the Respondent (if possible) and parent/guardian • Over 16 years and under 18 years: Consent of the Respondent.

	It is possible that within Schools different (more stringent) agreements have been made. **Please note**: if Personal Data of minors are processed, there are additional security requirements for these data. See **Chapter 9 of the Privacy & Personal Data Processing Policy**.

Requirements	• The Respondent must be given sufficient time to read and fill out the Informed Consent Form. Preferably, this form should be sent to the Respondent in advance so that the Respondent can be made aware of it.
	• Completed and authorized Informed Consent Forms must be kept safely within the specified storage period (see **Chapter 5.2**):
	  ○ in a locked cupboard/archive,
	  ○ in a (digital) folder only accessible to researcher(s)
	  ○ not linked to the other data collected in the research.

3.2. Drawing up a Data Management Plan

A Data Management Plan (DMP) should be drawn up on the basis of the **Research Data Management Regulations** before scientific research starts. In it, the researcher records, among other things, which data he will collect during a research project, how he will store or manage this data during the project, what will happen to the data after the project has ended, and also the Accountability requirements, namely the Data Protection Impact Assessment and Data Processing Register, are guaranteed.

Data Protection Impact Assessment (DPIA)

In some cases, the Processing of Personal Data involves a high risk for the Data Subject. In order to deal with this properly, the Data Protection Impact Assessment (DPIA) must be carried out, on the basis of the GDPR, to ensure that the privacy risks of the Respondents are properly safeguarded.
A DPIA is usually not necessary for scientific research. For more details on when a DPIA is mandatory, please refer to the **Privacy & of Personal Data Protection Policy, Section 11.2**.

For each scientific research in which Personal Data is processed, a pre-DPIA (questionnaire) must be completed in order to determine whether carrying out a DPIA is necessary. This short questionnaire is included (integrated) in the Data Management Plan and is, as far as possible, combined with the questionnaire for the ethical review.

The purpose of the DPIA is to identify the risks of Data Processing in good time. What Personal Data are processed? What does Tilburg University do with it? What are the consequences and how do we deal with these?

If a DPIA is necessary, the Data Representative (who then consults the Data Protection Officer) should be contacted. The questionnaire for carrying out a pre-DPIA is included in the Data Management Plan.

Data Management Register

On the basis of the GDPR, all Processing of Personal Data must be recorded in the university's Data Processing Register in the context of Accountability. For scientific research, the Data

Processing Register is completed based on the information included in the Data Management Plan (and, if possible, combined with the ethical review questionnaire). The Privacy Statement on the website is updated on the basis of the Data Processing Register.

Data Management Plan – Data Processing Register	For each scientific study, **the researcher must draw up a Data Management Plan** in which it is laid down which (Personal) data will be processed. This Data Management Plan is included in the university's Data Processing Register to the extent that it contains Personal Data. For the format of the Data Management Plan, please refer to the **Research Data Management Regulations**.
Pre-DPIA	For each scientific study, a pre-DPIA (questionnaire) must be completed in order to determine whether carrying out a DPIA is necessary. This questionnaire is included (integrated) in the Data Management Plan and, if possible, combined with the questionnaire intended for the Ethics Review Board.
Date Protection Impact Assessment (DPIA)	In some situations it may be necessary to carry out a Data Protection Impact Assessment (DPIA). Whether this is necessary is a result of the pre-DPIA questionnaire. The researcher shall be responsible for carrying out the DPIA if this is necessary. A **procedure** is available for this. He is supported in this by the School's Data Representative [5].
Review DPIA	The Data Protection Officer reviews the DPIA.
Review Data Management Plan by the Ethics Review Board	In each School, further agreements have been made about the reviewing of the Data Management Plan (DMP) (by a scientific committee and/or Ethics Review Board) and its storage.

A researcher may not simply process all Personal Data. A number of specific details are set out below:

Data Minimization – Necessary data	The researcher may **only collect Personal Data that are necessary for the purpose of the scientific research**, but guarantees that sufficient data are collected to be able to answer the questions posed by the research.
BSN	The **citizen service number** (BSN) may **never** be processed for scientific research purposes.
Identity Document	A copy of the Identity Document may only be viewed but may not be retained unless its retention is necessary for the scientific research and the photo and BSN number are masked, and, on the copy, it is marked that it was issued for research purposes. **Tip**: It is best to write down only the necessary data instead of making a copy of the ID.
Assistance in drawing up	The School's Data Representative offers assistance with the completion of the pre-DPIA, the DPIA and the Data Processing Register.

[5] https://www.tilburguniversity.edu/intranet/support-facilities/legal/legalprotection/privacy/contact/

Privacy Statement

Based on the right to Information, Tilburg University publishes a Privacy Statement on the website, in which Tilburg University offers information about the use of Personal Data in scientific research. Offering information in this way is necessary because it is not possible to work with Informed Consent for all research projects (e.g., a public database, the reuse of an existing database, or Web Scraping), and it must also be transparent as to how Tilburg University deals with Personal Data, particularly with these forms of data. In addition, certain research projects may not be included in this list for reasons of confidentiality or sensitivity of the research (e.g., when doing research into an indicator for the presence of hemp farms).

Privacy Statement	The Privacy Statement regarding scientific research and the list of current scientific research projects, in which Personal Data is used, is compiled on the basis of the information from the Data Processing Register. This does not require any action by the researcher. The Ethics Review Board may decide to mark a research as confidential, as a result of which the information about the research in question may not be disclosed in the Privacy Statement.

4. DURING THE RESEARCH

This part of the Policy describes the elements of careful handling of data that are important during every research in which Personal Data are processed, and the way in which Tilburg University guarantees the careful handling of data, particularly during this phase of the research. This Chapter deals successively with the handling of contact details of Respondents, the rights of participants during the research, the use of programs to collect, store, and analyze data, the sharing of data, the security of data, and the reporting of results.

4.1. Contact Details of Respondents or Potential Respondents

According to the GDPR, a researcher from Tilburg University who collects and stores contact details for the purpose of scientific research should store them in a secure manner that guarantees limited access. The researcher is responsible for storing the contact data file separately. The contact details that can be linked to the data set should be removed by the researcher as soon as possible (within 6 months unless longer is necessary), as long as this does not conflict with the interests of the scientific research.

Storage and access to contact details	Contact Details files should only be accessible to necessary persons: the principal researcher and supervisor involved.

4.2. Changes in the Personal Data Collected

A researcher may decide, in the course of the research, that additional Personal Data are necessary. The following guidelines apply:

Changes Personal Data	If during the research changes occur in the Personal Data that are collected, the researcher should

	• adapt the Data Management Plan by means of an amendment 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 granted access to the data sets (digital or physical) for research in which Personal Data has been processed. Such access is usually limited to the researcher concerned, and his supervisor. 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 only allowed for the researchers involved (including student researchers) and the supervisor (in relation to backup).
Access to archives	Access to data sets (digital and physical) containing Personal Data is only permitted for researchers, the head of Department, and the manager of the digital or physical data set.

Data sets (digital and physical) containing Personal Data must be stored safely and are only accessible to those for whom this is necessary in the context of the research.

Secure storage Personal Data – digitally	Personal Data sets must be stored securely. That is to say: • Pseudonymized, which means that the interconnecting or communication file on the university network drive (M/O drive), • on the secure environment of a Tilburg University server, • in a contracted cloud service such as SURFdrive, • only in an encoded or encrypted form on a storage medium (laptop, USB). In the absence of the researcher at the workplace, computers and the workspace must be locked.
Secure storage Personal Data – physically	Documents containing Personal Data must be stored securely in a locked cupboard or archive. In case of absence, the cabinets or archives should be locked and not accessible to unauthorized persons.

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

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

When using applications/programs from external suppliers, a Processing Agreement must be concluded in order to make proper agreements about responsibilities, security, etc. For more information, please refer to the **Privacy and Personal Data Processing Policy in Chapter 11.4.**

Collecting data	If external applications are used for the collection of Personal Data: • See the **Research Data Management Regulations** for additional guidelines.

	• Preferably use applications specified in the list of Tilburg University approved applications. For these applications, it has been established that they meet all the requirements of the GDPR and that a Processing Agreement has been concluded. • If the researcher wishes to use an application that is not on this list, he must conclude a Processing Agreement (see below).

Storing data	**Digitally**:
	• See the **Research Data Management Regulations** for additional guidelines.
	• All (raw) data must be Pseudonymized and stored on the Tilburg University servers or SURFdrive where the interconnecting or communication file is stored on the university network drive.
	• If a researcher wants to make use of another (cloud) service:
	  ○ Preferably use applications specified **in the list of Tilburg University approved applications**. For these applications, it has been established that they meet all the requirements of the GDPR and that a Processing Agreement has been concluded.
	  ○ If the researcher wishes to use an application that is not on this list, he must conclude a Processing Agreement (see below).
	
	Physically:
	All Personal Data must be physically stored in a locked cupboard or archive. If stored at a remote location or by an external administrator, a Processing Agreement must be concluded for this.

Analyzing data	If, for analyzing data, applications such as SPSS are used: • Preferably use applications specified in **the list of Tilburg University approved applications**. For these applications, it has been established that they meet all the requirements of the GDPR and that a Processing Agreement has been concluded. • If the researcher wishes to use an application that is not on this list, he must conclude a **Processing Agreement** (see below).
Sharing data	• Sharing data with colleagues for co-analysis or peer review of the analysis is only allowed if this is done in a secure way, for example, by using encryption (via Secure File Transfer: **procedure** on the intranet). • To use cloud services, we refer to storing data above. • Sharing of data via a cloud service or other programs outside Tilburg University's control is only permitted if a Processing Agreement has been concluded with the party in question.
Anonymizing or Pseudonymizing	If Personal Data are no longer necessary (or only have to be kept for reasons of verifiability on the basis of the VSNU Code of Conduct), but the data cannot yet be deleted, the Personal Data must be Anonymized or Pseudonymized at the earliest possible stage.

4.5. Contract and Processing Agreement

It is a legal obligation that when a researcher, on behalf of the Tilburg University, exchanges, provides, or receives Personal Data with another organization, sound contractual agreements are made about this. What kind of agreement should be made depends on the role of Tilburg University and the role of the other party (Controller, Processor). For more information, please refer to the **Privacy & Personal Data Protection Policy, Chapter 11.4**.
If a study involves collaboration with other (external) research institutes or parties, a research agreement must be concluded in which agreements are made about the division of responsibilities, et cetera. **Model agreements** are available for this purpose.

Situation	Mandatory agreement
Tilburg University is Controller and third party is Processor	Processing Agreement in accordance with an established model. See **procedure** and explanation for more information. Example: Storage or processing of Personal Data in an application running in the cloud (e.g., Qualtrics)
Tilburg University is Processor for another Controller	Processing Agreement in accordance with an established model. Example: Research assignment in which the client determines the purpose and means of the research and Tilburg University collects and analyzes the Personal Data.
Tilburg is Controller together with another party	Arrangements in **a research agreement** or in a separate agreement on the division of the responsibilities. Consider: • Who arranges the rights of the Data Subjects (Access, Rectification, etc.), who informs about the Processing (Privacy Statement) and possibly a recourse scheme. • What are the parties allowed to do with the data and does confidentiality apply, for example? Example: Research assignment in which the client, together with Tilburg University, determines the purpose and means of the research.
Deviating from the standard model agreement	In view of the risks involved, it is preferable to conclude the standard model agreement. However, it may be necessary to deviate[6]. If the researcher wants to deviate from the standard model, he has to coordinate this with the Data Representative of the School. The Data Representative may request advice from the Data Protection working group coordinated by the Data Protection Officer. The Processing Agreement must be authorized by an authorized signatory, usually the Dean, the School's Managing Director, or the Executive Board.
Responsible for the realization and content of the agreement	The researcher must consult the Data Representative before concluding the agreement. The Data Representative offers assistance and may seek advice from the Data Protection Officer or Legal Affairs. The Processing Agreement must be stored centrally.
Registration/audit trail	The Processing Agreement (including the motivation in case of a deviation) must be archived centrally. For more details, see the **Processing Agreement procedure**.

[6] An extensive explanation of the model agreement has been written. It also states which aspects you may deviate from and what the risk is.

4.6. Writing and Publishing an Article

When writing an article, the researcher must prevent Traceable Personal Data from being included in the article. It sometimes happens that the researcher wants to quote from the research. This is possible if it can be done anonymously. Quotations resulting from Web Scraping may be traceable (easy to search on the Internet) and are, therefore, not Anonymous. They should preferably be paraphrased. A point to consider is the possibility that a combination of Personal Data can be traced back to individual persons. Consider, for example, singling out a manager of a large hospital in the Eindhoven region in the age category 45 to 55.

Personal Data in an article	The researcher must guarantee that no Traceable Personal Data is included in the article by:
	• Anonymizing/Pseudonymizing the research results
	• When quoting:
	  ○ Anonymizing;
	  ○ In case the quotation is obtained via Web Scraping: paraphrasing.

Sharing data for review purposes

During the publication process, data may need to be shared with peer reviewers. It goes without saying that the Personal Data must be protected as much as possible.
If data sets are shared without identifiable Personal Data, this Policy does not apply. The following rules apply:

Sharing data with peer reviewers	If Personal Data must be shared with peer reviewers:
	• If possible, Anonymize or Pseudonymize (for which the key is not sent to reviewer) (**Section 4.2**).
	• If this is not possible:
	  ○ Check whether a Processing Agreement has already been concluded with the publisher (see list of on the intranet).
	  ○ If there is no Processing Agreement yet: Conclude the Processing Agreement with the publisher of the journal (**Section 4.3**).
	• If a raw data set is required, deliver this free of Traceable Personal Data.
	• Agree (contractually) that the data set will be destroyed after the review procedure.

4.7. Rights of the Respondents during the Research

Respondents may also invoke a number of rights during the research. For more information, see **Section 2.10**.

5. AFTER THE RESEARCH

This part of the Policy describes the elements of careful handling of data that are important for the completion of every research in which Personal Data are processed and the way in which Tilburg University guarantees the careful handling of data, particularly at this stage of the research. This Chapter deals with the storage periods, data package, and the rights of Respondents successively.

5.1. Storage Period

The collected data must be carefully stored and, if they are no longer necessary, removed. The following rules apply.

Storage period	• The storage period of research data is at least 10 years after the date of the last publication. A storage period of at least 15 years applies to medical data. See also **Research Data Management Regulations** • The **directly Traceable Personal Data** (mainly contact data and Informed Consent) may be kept separately for as long as necessary, but for a maximum of 10 years, and for medical data for a maximum of 15 years, after the date of the latest publication[7]. • Discipline-specific agreements may have been made at a national level that deviate from these standards. If applicable, these are described in the guidelines for scientific research of the discipline concerned. • If a research has not led to a publication, the maximum storage period of the Traceable Personal Data (such as contact details and Informed Consent) is 15 years after completion of the research. After the maximum storage period for the Traceable Personal Data (Informed Consent), these must be destroyed in a safe manner under the responsibility of the supervisor.

5.2. Data Storage

It is important that data is carefully stored after completion of the research in line with the **Research Data Management Regulations**. The following guidelines apply.

Raw data	After a research project, the raw data should be stored carefully. This can be done on the Tilburg University servers or together with others on another location if a Processing Agreement has been concluded with them.
Data package	All research data (with the exception of Traceable Personal Data) must be included in a data package in accordance with the university's

[7] For scientific research, it is important to be able to render account within the framework of scientific ethics. To this end, it is important that it is clear which Respondents were involved. In connection with the minimum storage period for scientific research, the maximum storage period for Informed Consent Forms is related to this.

Research Data Management Regulations. The data package (including analysis files and other relevant data) is provided with a complete addition of metadata and then stored in a Trusted Digital Repository (TDR). *DataverseNL*, with, if desired, a link to DANS EASY.

If a researcher wants to use **a different TDR** and Personal Data are present in the data set, which are not Traceable Personal Data, a **Processing Agreement** must be concluded with the provider of the TDR.

5.3. Rights of the Respondents after the Research

Respondents may also invoke a number of rights during the research. For more information, see **Section 2.10.**

APPENDIX 1: TYPES OF DATA SETS

Audio and video recordings

Audio and video recordings are regularly used in scientific research. Sometimes it is possible to anonymize these recordings, for example by blurring faces, or just filming hands, but this strongly depends on the purpose of the research.
Recordings can be used for presentations or publications (e.g., in education) and it is important that the Respondent is well informed about this and gives consent.

Informing and consent of the Respondents	• The Data Subject will be clearly informed in advance of the recording by means of Informed Consent. • The Data Subject must be properly informed in advance of any use of recordings for presentations and publications and must give his or her specific Consent to do so.
Use audio and video data	In the event of audio or video recordings for scientific research, it is important that the researcher only collects Personal Data that are necessary for the purpose of the scientific research but collects sufficient Personal Data to answer the research question. If possible, the research results will be recorded (for the purpose of the research) in order to comply with the guidelines below. • No mention of names (or "mask" them later) • Do not film faces if this is not necessary (e.g., only hand movements). It is important, however, in connection with integrity guidelines, that the data is verifiable, e.g., who participated in the research. This can be done by Pseudonymization, in the form of a communication/interconnecting file and the Informed Consent Forms. **Please note**: if the voice of the Respondent is recognizable, it is never Anonymized but Pseudonymized: after all, it can be traced back to the person.

Interviews and observations, experiments in LABS

Researchers often make reports of interviews and observations. In some studies, experiments with subjects are carried out in labs. Sometimes Special Personal Data are measured, for example, a blood pressure measurement, to see if there is any stress.

It is important to avoid the inclusion of directly Traceable Personal Data (e.g. names) as much as possible.

Informing and obtaining consent from Respondents	The Data Subject must be clearly informed in advance of the purpose and the manner of scientific research by means of Informed Consent. If prior information is not desirable for the purpose of the research (e.g., research into ethnic discrimination), the Informed Consent may be general. However, this information must be provided (retrospectively) when the Data Subject is debriefed regarding the research.
Administrative handling	Sometimes participants in LABS or Respondents are paid for the participation in a research. In this case, Personal Data will be processed for payment (substantiation of financial administration). This is a Processing of Personal Data and, therefore, this process must be recorded in the Data Processing Register (not specified per research) by F&C.
Interviews, observations, and experiments	In the case of interviews and observations during scientific research, it is important that the recording (elaboration) of this information complies with the guideline below: • Do not mention names or other Traceable Personal Data when recording the interview and the observations or the lab results. It is important, however, in connection with integrity guidelines, that the data is verifiable, e.g., who participated in the research. This can be done by Pseudonymizing, in the form of a communication/interconnecting file and the Informed Consent Forms. **Please note** that additional security requirements apply to the processing of Special Personal Data. See the **Privacy & Personal Data Protection Policy** and **Section XX** with regard to Special Personal Data in scientific research.

Eye tracking

In some scientific studies (such as how people look at websites), eye tracking is used to follow eye movements. Depending on how this eye tracking is recorded, there may be an increased privacy risk for the Data Subject. This is the case if an iris scan is involved because an iris scan is used as a means of identification (and the risk of identity fraud is therefore high for the Respondent).

Informing and obtaining consent from Respondents	The Respondent must be clearly informed in advance of the manner and purpose of the research by means of Informed Consent.
Eye tracking	In case of eye tracking in scientific research it is important that: • The iris should not be photographed or scanned in connection with the Data Subject's increased privacy risk.

Medical Screening (MRI/EEG/ECG, et cetera)

A number of scientific studies use medical screening such as MRIs, EEGs, and ECGs. These are Special Personal Data. The following guidelines apply:

Informing and obtaining consent from Respondents	The Data Subject must be clearly informed in advance of the manner and purpose of the research by means of Informed Consent.
Medical screening EEG ECG MRI et cetera	In case of use of medical data, Special Personal Data are processed, for which it is important that the recording (elaboration) complies with the guideline below: • Do not mention names or other Traceable Personal Data when recording the MRI/ EEC or ECG It is important in connection with integrity guidelines, however, that the data can be verified as to whom participated in the research. This can be done by Pseudonymization, in the form of a communication/interconnecting file and the Informed Consent Forms. **Please note** that additional security requirements apply to the processing of Special Personal Data. See the **Privacy & Personal Data Protection Policy** and **Section 2.3** with regard to Special Personal Data in scientific research.

Wearables

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

Informing and obtaining consent from Respondents	The Data Subject must be clearly informed in advance of the manner and purpose of the research by means of Informed Consent.
Wearables	If wearables are used in scientific research, it is important that the recording (elaboration) of these data comply with the following guideline: • Do not mention names or other Traceable Personal Data when recording the results of the wearables.

	It is important, however, in connection with integrity guidelines, that the data can be checked as to with whom the research has been carried out. This can be done by Pseudonymization, in the form of a communication/interconnecting file and the Informed Consent Forms. **Please note** that additional security requirements apply to the processing of Special Personal Data. See the **Privacy & Personal Data Protection Policy** and **Section 2.3** with regard to Special Personal Data in scientific research.

APPENDIX 2: RESPONSIBILITIES (RASCI) FOR 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 Tilburg University Data Protection Regulations		See general RASCI in Privacy & Personal Data Protection Policy					
Definition Tilburg University Research Data Management Regulations		Tilburg University Research Data Management Regulations	Executive Board	• Taskforce Data Protection • Director LIS • Research Data Office (RDO)	• Data Protection Officer (DPO) • CISO and ITSO	• POZ • Scientific/Ethics Review Board	• Researchers • Research Support teams (RST)
Define Pre-Data Protection Impact Assessment		Pre-DPIA	Dean	Researcher	Data Representative (DR)		
Define Data Management Plan (including DPIA assessment[8])		Data Management Plan	Dean	Researcher	Data Representative (DR)	Scientific/ Ethics Review Board	Data Protection Officer if DPIA is necessary
Execution DPIA		Research Data Protection Impact Assessment	Dean	Researcher	Data Representative (DR)	Data Protection Officer (DPO)	Data Protection Officer (DPO)
Close Data Processing Agreement	Standard model	Data processing agreement	Dean	Researcher	Data Representative (DR)		Data Protection Officer (DPO)
	Adjusted standard model		Dean	Researcher	Data Representative (DR)	• Data Protection Officer (DPO) • Legal Affairs (only mandatory in case of authorization by	Data Protection Officer (DPO)

[8] In the Data Management Plan, an assessment must be made whether a DPIA is required/mandatory.

Task	Sub	Deliverable	Accountable	Responsible	Supportive	Consulted	Informed
						the Executive Board). • Security: • Chief Information Security Officer (CISO) and IT Security Officer (ITSO)	
	Supplier version (exceptional)		Dean	Researcher	Data Representative (DR)	• Data Protection Officer (DPO) • Legal Affairs (only mandatory in case of authorization by the Executive Board). • Security : CISO and ITSO	Data Protection Officer (DPO)
Register Data processing for research project	Special category of personal data	Record of Processing Activities	Dean	Researcher	Data Representative (DR)	Data Protection Officer (DPO)	
	Special circumstances		Dean	Researcher	Data Representative (DR)	Data Protection Officer (DPO)	
	Major personal data		Dean	Researcher	Data Representative (DR)	Data Protection Officer (DPO)	
	Other		Dean	Researcher	Data Representative (DR)		Data Protection Officer (DPO)
Advice regarding Data Protection research	Contractual Agreements	Advise	Legal Affairs	Legal Affairs	Data Protection Officer (DPO)		

Task	Sub	Deliverable	Accountable	Responsible	Supportive	Consulted	Informed
	Research projects	Advice	Data Representative (DR)	Data Representative (DR)	• Data Protection Officer (DPO) • Research Data Office		
Report Research data breaches or incidents		Reported incident/ data breach	Researcher	Researcher		Data Protection Officer (DPO)	Taskforce Data Protection
Analyze data breaches and report (if necessary) to AP		See general RASCI in General Policy Privacy & Data Protection.					
Raise Awareness		Awareness – knowledge data protection	Dean	Data Representative (DR)	• Data Protection Officer (DPO) • Legal Affairs • Research Data Office (RDO)		
Organize Research Data Protection Training and Education		Training and awareness	Dean	Research Data Office (RDO)	• Data Representative (DR) • Data Protection Officer (DPO) • Legal Affairs		
Monitoring and checks on compliance to law and legislation for research projects		See general RASCI in general Privacy & Personal Data Protection Policy					

APPENDIX 3 DEFINITIONS

Concept	Definition
Anonymizing/ Anonymous information	Information that does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a way that the data subject is not or no longer identifiable (for example, for statistical or research purposes)
Data Subject/Respondent	An identified or identifiable natural person to whom personal data relates Is referred to as a Respondent in scientific research
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 a natural person, data concerning health, or data concerning a person's sex life or sexual orientation.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data
Data leak (i.e., Personal Data breach)	A breach of security which accidently or unlawfully results in the destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to personal data transmitted, stored, or otherwise processed.
Third party	Any natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process Personal Data
Data Protection Impact Assessment (DPIA) or Privacy Impact Assessment (PIA)	An assessment of the impact of the envisaged processing operations on the protection of Personal Data that helps to identify privacy risks and offers ways to reduce the risks to an acceptable level. This is referred to as Data Protection Impact Assessment in the GDPR.
Traceable Personal Data	All personal data that lead to an identifiable person. These may be unique personal data (for example, BSN number) but also a combination of personal data (for example, name in combination with address).
Identity document	The legal identity papers (a passport, a Dutch identity card, an ID card or a passport from an EEA country, or a Dutch aliens' document). At Tilburg University, employees and students can also identify themselves with a driving license and the Tilburg University card with passport photo.
Informed consent	Consent form that clearly informs the Respondent about, amongst other things, the content of the scientific research and his rights.
Personal data	Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Pseudonymization	The processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Right to restriction of processing	The right to restriction means that the Personal Data may not be (temporarily) processed or modified. The fact that the processing of Personal Data is limited must be clearly indicated in the file by the controller so that this is also clear to recipients of the Personal Data. If the restriction is lifted again, the data subject must be informed accordingly (Article 18 GDPR).
Right to object	On grounds relating to his particular situation, a data subject can make use of the right to object to processing of personal data concerning him when the requirements of the Regulation are met. If a data subject objects, the controller ceases processing, unless compelling justified grounds provide otherwise (Article 21 GDPR).
Right to data portability	This means that a data subject shall have the right to receive the personal data concerning him from the controller in a structured, commonly used, and machine-readable format and shall have the right to transmit or have the data transmitted directly to another controller unless this adversely affects the rights and freedoms of others. A data subject has the right to data portability for data provided by himself (Article 20 GDPR).
Right to erasure/right to be forgotten	The controller is obliged to erase the data subject's Personal Data without undue delay, amongst other things, on the following bases: the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws his consent and no other legal ground for the processing exists; the data subject objects to the processing; the personal data have been unlawfully processed. (Article 17 GDPR)
Right to be informed	A data subject must be informed of the fact that the processing of his Personal Data is being or will be carried out and for what the purposes this is done. The GDPR indicates which information must in any case be provided, for example, information on the period, the rights of the data subject, the source of the data and the legal basis for processing. If the purpose of the processing changes, information about this must also be provided (Articles 13–14 GDPR).
Right of access	The data subject has the right to know whether his Personal Data are being processed by the controller. The GDPR contains an enumeration of the information for which the right of access applies. The controller must provide the data subject with a copy of the Personal Data that are being processed (Article 15 GDPR).
Right to rectification	The data subject has the right to rectification of inaccurate personal data concerning him or the right to provide a supplementary statement if the processing takes place on the basis of incomplete data. The rectification needs to take place without undue delay. The controller is obliged to inform every person who received the Personal Data of every rectification, unless this is impossible or would involve a disproportionate effort (Article 16 GDPR).
Respondent	Is a natural person who contributes to the research. Refers to the person called the Data Subject in the GDPR.

Consent (by the data subject)	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him (Article 4(11) GDPR).
Processor	A natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of the controller
Processor contract	The contract between a controller and processor in which agreements are made regarding the processing of Personal Data aiming to safeguard the data protection of the data subject (Article 28, Section 3 GDPR)
Processing	An operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of data.
Processing basis	A condition for the lawful processing of personal data as specified in Article 6 GDPR (e.g., consent, legal obligation).
Data processing register	The records of the processing activities as referred to in Article 30 GDPR that must contain certain data for the purpose of accountability.
Controller	The natural or legal person, public authority, agency, or other body 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, the controller or the specific criteria for his nomination may be provided for by EU or Dutch law.
Web Scraping	A computer technique using software to extract and possibly analyze information from web pages. The software usually tries to explore part of the world wide web using the code-based Hypertext Transfer Protocol (HTTP), or by simulating surfing behavior with a web browser