Research Data Management Regulations

Introduction

Research data are of great value for Tilburg University and should be managed in a responsible manner. Responsible research data management is essential, on the one hand, from the principle of “verifiability” as is also stated in The Netherlands Code of Conduct for Scientific Practice (VSNU). On the other hand, it is in line with the conditions of national and European research funding organizations as regards the storage and management of research data for stimulating open access and reuse of research data.

The VSNU Netherlands Code of Conduct for Scientific Practice denominates the administrative responsibilities to promote and maintain compliance with the code. The Tilburg University Strategic Plan 2014–2017 contains the intention to develop a code of conduct for storing and sharing research data (Strategic Plan 2014–2017, p. 17). These Regulations intend to give shape to this intention.

Although managing research data may vary a lot per research discipline, the Executive Board chooses to offer one set of university-wide regulations in the form of these Research Data Management Regulations, in which the joint point of departure for responsible management of research data is stated. The aim of research data management is to guarantee accessibility to and protection of research data against theft, misuse, damage, and loss. The researcher should take care to adequately store and archive research data, and make them retrievable and accessible. Responsible data storage not only leads to transparency but also offers possibilities for knowledge dissemination, meta-analysis, and re-analysis. Schools will specify the Research Data Management Regulations in an operating procedure/policy for their School, tailored to the specific circumstances of the research discipline in question and internal School processes.

University policy for storage and management of research data (EB resolution of September 5, 2017)

1. **The research data generated at Tilburg University are stored, managed, and made accessible in accordance with the legal demands (copyright act, privacy act etc.) developed to this purpose, and the relevant codes of conduct:**
   a. *The Netherlands Code of Conduct for Scientific Practice. Principles of good academic education and research. Decreed 31 October 2014. VSNU:* http://vsnu.nl/files/documenten/Domeinen/Onderzoek/The_Netherlands_Code%20of_Conduct_for_Academic_Practice_2004_(version2014).pdf
   b. *Tilburg University Scientific Integrity Regulations, 2012: https://www.tilburguniversity.edu/about/tilburg-university/conduct-integrity/download-letter/*
   c. *Code of Conduct for the use of personal data in academic research, 2005:* www.tilburguniversity.edu/about/university-library/about-the-university-library/research-support/dataverse-nl/download-code-of-conduct-personal-data/ *(the code is under construction, taking into account the new European regulation about data protection)*

Research data generated by a Tilburg University researcher are:

a. accurate, complete, reliable and authentic and provided with metadata;
b. securely stored with minimal risk of loss;
c. traceable and accessible;
d. open and citable.

2. Definitions data management policy

Research data

By research data is meant: all (digital and non-digital) data collected and generated during academic research, as well as the instruments with which the research data were collected and other relevant information (for instance questionnaires, software, scripts, and lab journals).

Metadata

By metadata is meant: documentation and/or information on research data required to understand the content and context of the data.

3. Responsibilities

The researcher/project manager is responsible, at implementation level, for:

a. data storage during and after the research;
b. proper data management in accordance with points of departure of the Research Data Management Regulations and the additional School's data management policy;
c. creating a data management plan preceding a new research project in accordance with the provisions of the School's data management policy and observing the obligations mentioned in Article 9 of these Research Data Management Regulations in case personal data are processed for the research;
d. observing Article 10 of the Research Data Management Regulations when research is conducted with or for third parties;
e. familiarizing students and PhD candidates (performing activities within the area of a Tilburg University researcher's responsibility) with these Research Data Management Regulations and the School's data management policy and supervising this.

The Dean of the School in question is responsible for:

a. elaborating these Research Data Management Regulations in a School policy;
b. informing the academic personnel about the Research Data Management Regulations and the School's data management policy;
c. supervising compliance with the data management in accordance with the Research Data Management Regulations and the supplementary School data management policy;
d. reporting to the Executive Board in the annual research report on how the data management has been given form and content.

The Executive Board is responsible for:

a. formulating a general university policy framework as determined in these Research Data Management Regulations;

b. offering the flanking knowledge, advice, and support regarding data management;
c. offering an adequate infrastructure for data storage and management insofar as the Schools need additional adequate facilities for data storage;
d. carrying out and supervising audits.

4. Storage

The raw and processed research data should be stored securely during the research.

Research data should be stored securely and permanently at least at the end of the research, or even sooner if other applicable rules are outlined, together with at least all information required for possible reuse and verifiability of the research data (as referred to in Article 5 of the Research Data Management Regulations) in facilities made available or designated by or via Tilburg University (e.g., DataverseNL). Alternatively, it is possible to store and archive research data after the research in discipline-specific repositories or data archives of third parties if they meet the following requirements:

a. provide facilities to enable research data stored in the repository to comply with the Research Data Management Regulations;
b. use open standards for access and metadata wherever possible;
c. are preferably certified;
d. are technically and organizationally sustainable.

5. Access

The researcher should provide research data with adequate metadata. In case of encrypted research data, the researcher should keep the key in question separately from the research data and store and archive it not later than at the end of the research project or even sooner if the possible applicable rules outline, as determined in Article 4.

6. Storage period

If no other period is required by an applicable legal, contractual, or subsidy rule, all raw and processed research data must be stored for a period of at least ten years after the moment that the research is formally completed.

7. Control

Research data, generated in the scope of employment, internship, or secondment to or on behalf of Tilburg University, are, in principle the property of Tilburg University, unless otherwise agreed in a separate contract by Tilburg University. Advice on the control of research data is obtained from or via the Research Data Office.

8. Public disclosure

Tilburg University applies the basic principle that research data are made publically available for academic research, as far as reasonably possible, if and insofar as this does not conflict with agreements with research funders, confidentiality obligations , the Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens, WBP*) and/or intellectual property rights of third parties. Advice on this is obtained from or via the Research Data Office. In any case, the metadata must be made publically available.

9. **Personal data**

If the research data contain personal data, the management of those personal shall be subject to additional rules from the Dutch Personal Data Protection Act (replaced as of May 25, 2018 by the EU General Data Protection Regulation 2016/679). Personal data are processed in accordance with the WBP. Researchers who process personal data should report the intended processing in advance to the Data Protection Officer (*Functionaris persoonsgegevens, FG*) and fill out the schedule for assessment of the processing of personal data, in order to comply with the obligation of transparency, recorded in the WBP.

10. Third parties

Researchers not employed by Tilburg University, such as research fellows and/or students working under the responsibility of a Tilburg University researcher, who conduct research at Tilburg University and/or in cooperation with Tilburg University and thus generate research data should declare in writing that they comply with the Research Data Management Regulations and the applicable School's research data management policy.

In the event of cooperation with another research organization and/or third party, it is agreed and recorded in writing that if the research data are generated at the other organization, Tilburg University also has the right to store the research data in conformity with these Research Data Management Regulations. If the research data are generated by both or more research institutions, written agreements are made with those other knowledge institutions on the management, storage, and access of the research data, as much as possible in conformity with the Research Data Management Regulations and the School's research data management policy.

When research including research data is conducted on behalf of an external client, it is agreed with the client as far as possible that Tilburg University has the right to manage, save, store, and grant access to the research data, in conformity with the Research Data Management Regulations and School's research data management policy.

The Dean's consent is required in advance when agreements with third parties involve a deviation with regard to the Research Data Management Regulations and School's data management policy,

11. Entry into force and period of validity

The Research Data Management Regulations apply to research commencing after the effective date of January 1, 2018. The Research Data Management Regulations are valid until a new version is adopted or the decision is made to revoke the Research Data Management Regulations.

Guideline for the Research Data Management Regulations

Content

Readers' Guide

This guideline elaborates on a number of practical points from the Research Data Management Regulations. The guideline serves, on the one hand, as an aid for Schools in the development of School policy and, on the other hand, as an explanation of Article 9 (Personal Data) and Article 10 (Third Parties) of the Research Data Management Regulations. This guideline will be included in the web portal of the Research Data Office.

The guideline offers:

1. an overview of items that may be part of a School data management policy (the checklists in Chapters 1 through 4);
2. instructions for dealing with the obligations of the General Data Protection Regulation 2016/679 which entered into force on May 1, 2018 if research is carried out with personal data (Chapters 5 and 6);
3. Explanation of the support services for research data management via the Research Data Office (RDO) (Chapter 7).

Information on School policy already adopted by the TSB and TSHD is available on the university's intranet:

- **TSB *Data Handling & Methods Reporting Guideline (DHMR*):** https://www.tilburguniversity.edu/intranet/organization-policy/tsb-1/science-committee/
- **TSHD *Data Management Policy for TSHD*** https://www.tilburguniversity.edu/intranet/organization-policy/ERB/strategy-policy/humanities.htm
- **TLS *Ethics Review Board*** https://www.tilburguniversity.edu/intranet/information-for/scientists/research/policy/erb/tls-ethics-review/

1. Data Management Plan

A data management plan (DMP) is a digital document in which the researcher describes what data he or she will collect during a research project, how he or she will store and manage the data during the project, and what will happen to the data after the project has ended. The DMP is drawn up at the start of a new research project. Various models (templates) and checklists are available for drawing up a data management plan. The completed template forms the data management plan. During the course of the project, regular checks are carried out to ensure that the plan is still up to date or needs to be adjusted.

The Research Data Management Regulations require that a data management plan is written at the start of each new research project or program. In the School's data management policy the following matters can be agreed:

- Who draws up the data management plan for a project?
- For which type of research should a data management plan be drawn up? (for example, projects of PhD candidates and research funded by the NWO or other research funds);
- How is the drafting of data management plans supervised? To whom should a data management plan be submitted? For information or consent?
- How is the updating of data management plans monitored?
- Are data management plans stored centrally? If so, where? and who has access to it?
- Which matters should at least appear in a data management plan?

- Which matters that appear in a data management plan can be arranged at the level of the School or institute?

More information on data management plans on the university intranet: https://www.tilburguniversity.edu/intranet/information-for/scientists/research/management/data-policy/datamanagementplan/

On this page you can also find a template for a data management plan.

2. Roles and Responsibilities

Persons who (may) play an advisory, supporting, operational, or supervisory role in research data management:

a. Domain chairperson, research director
b. Director of the School or Research Institute
c. Research leader (principal researcher)
d. Researcher, lector
e. PhD candidate
f. Student
g. Data steward
h. Ethics Committee
i. Policy officer
j. Secretary's office

The School data management policy may describe who has what responsibilities or duties in dealing with research data within the School or Research Institute.

Explanation Data Steward

A data steward is an official, usually a researcher, who is responsible for the research data management in one or more research projects. He or she has the experience and expertise needed to advise and support researchers and checks and reports at least once a year on the state of affairs regarding research data management. The research director, the head of the research group, the principal researcher (leader of the research project) or a lector can fulfil the role of data steward, and he or she can delegate tasks to one or more others.

If desired, the position of data steward can be further defined in the School's data management policy, for example, by recording the following matters:

- Who designates the data steward?
- Who can fulfill the role of data steward?
- What is the scope of the position: per research project, research group, School/Research Institute?
- What are the duties of the data steward?
- What are the powers of the data steward?
- Can the data steward delegate duties? If so, which and to whom?
- To whom does the data steward report? In what form? With what frequency?
- How is continuity guaranteed when a data steward leaves?

3. Rules and Agreements on Storage, Access, and Archiving

Storage

There are countless ways to lose data: a file is accidentally deleted, a laptop is stolen, the context of the data is unclear, software becomes unusable, a file can no longer be opened, etcetera. It is, therefore, important that every researcher pays attention to storing, organizing, and describing his or her data. It is also good to make agreements about this at the level of the School, Department, or Research Institute. The following could be considered:

- How do you organize the safe collection of research data?
- Where are data stored for ongoing research?
- How are data stored?
- How is it organized that the raw data file cannot be changed after storage?
- How are the data protected against loss, theft, misuse, unauthorized access?
- How is it ensured that it is clear, at all times, which processing the data have undergone?
- How is version management handled?
- What agreements apply to non-digital data and documentation? How is the connection between non-digital and digital data guaranteed? This includes, for example, completed Informed Consent forms, but also samples, models, etc.

More information about storing research data on the university intranet:
https://www.tilburguniversity.edu/intranet/information-for/scientists/research/management/storage-archiving-data/

Access

Ongoing research

Data from ongoing research will of course be accessible to the researcher(s) directly involved, but there are more parties for whom access to the data may be necessary. In the School's operating procedure/policy, it can be described:

- Who have access to data from current research? This includes students who participate in the research project; the data steward; an ethics committee; a fellow researcher who must continue the research if the original researcher unexpectedly drops out;
- How is this access organized? By whom is access granted?

Completed research

Tilburg University is committed to ensuring that data from completed research is publicly accessible and available for reuse in new research. Researchers can ensure this by placing their data after completion of a research project in a data archive that offers the possibility of publishing the data and assigning a persistent identifier to the data (a unique code used to refer/link to the dataset) (see also the section on archiving). Tilburg University offers its researchers the institutional data repository DataverseNL. Tilburg University Dataverse has obtained the CoreTrustSeal quality mark.

Datasets containing sensitive data—intellectual property rights of third parties, personal data, corporate information, information that can cause damage when made public—cannot be made freely available. However, these data may be useful for new research. For many data archives it is possible to publish a description of this data and to make the data available only on request.

If an external party outside the regular scientific process submits a request for access to research data, the researcher shall contact the Research Data Office for legal advice. This is to prevent that datasets are provided in violation of the rights of third parties. Conditions may be attached to the consent.
Before the researcher decides to file his/her dataset publicly, he/she will also consider whether the dataset may have commercial value. If so, the researcher may decide to file the dataset with restricted/monitored access.

The following points can be included in the School's operating procedure/policy:

- Which data are made publicly accessible? Which data are not?
- When will data suitable for this purpose be made publicly accessible? Who monitors this?
- How are data made publicly accessible? Does the School or Research Institute prefer a particular data archive? If so, which one?
- Under which license are data made public?
- Who handles requests for access to non-public data?
- What are the criteria for granting/rejecting requests for access to non-public data?

More information about publishing research data can be found on the university intranet:
https://www.tilburguniversity.edu/intranet/information-for/scientists/research/management/sharing/

Archiving
The Research Data Management Regulations require the storage of research data. For raw and processed research data, a storage period of at least ten years applies. Archiving is done in such a way that the data can be consulted with a minimum of time and action by the researcher him-/herself and by any other researchers (external or otherwise) who wish to use the data for new research.

In the School's operating procedure/policy practical matters can be arranged, such as:

- What data are archived? What are the criteria for archiving?
- Where are data archived and by whom?
- How are the data archived? What are the requirements for the description of the data (metadata)?
- Who oversees archiving and storage periods?
- Who decides whether to extend the storage period?
- What criteria are used to determine whether the storage period is extended?
- What happens to data for which the storage period is not extended?
- What happens to data from researchers leaving the School or Research Institute?
- Are researchers who are no longer attached to the School or the Research Institute informed about the extension of the storage period or the destruction of data they have collected? If so, how, when, and by whom?

More information about archiving research data on the university intranet:
https://www.tilburguniversity.edu/intranet/information-for/scientists/research/management/storage-archiving-data/

The School's data management policy may also provide further instructions for PhD candidates to file the data associated with their thesis in a subject-specific, national, or institutional data archive, for example:

- Who ensures that a PhD candidate files his or her data?
- When should the dataset be filed?
- Does the School or Research Institute have a preference for a particular data archive? If so, which one?
- Should the dataset, if possible, also be made publicly accessible? If so, under which license?
- Who registers where the dataset is filed?
- Should a copy of the dataset be left with the School or Institute? If so, where is it stored and who supervises it?
- Who handles any requests for access to the data?

4. Support and Training

The School's operating procedure/policy may describe which support, education, and training will be arranged for whom, and by whom. For example:

- (additional) training of researchers
- training and supervision of PhD candidates
- training and guidance of students
- training of data steward(s)
- practical support

5. Rules and agreements with third parties

It is also important that research data are handled carefully in accordance with the Research Data Management Regulations when collaborating with or conducting research on behalf of a third party. However, third parties are not necessarily bound by the Research Data Management Regulations. Third parties may be bound by internal regulations of their own institution or organization. It is, therefore, important that the subject of data management is part of the agreements made prior to the research and that these agreements are added to the collaboration agreement or commission agreement.

Students are also considered as third parties in this respect. If a student participates in a research under the responsibility of a Tilburg University researcher, the researcher will have to ensure that the student signs a statement in which he/she declares that he/she is familiar with the Research Data Management Regulations and will act in accordance with them. A standard model for such a statement will become available.

In the event that the research data contain personal data, it may be necessary to conclude a so-called processing agreement. In many cases, the use of software and/or tools for the storage and/or collection of research data must also be based on a processing agreement with the owner of the software and/or tools. This also applies if a third party collects and/or stores the data on behalf of the researcher. LIS stores a list of parties with whom a processing agreement has already been concluded.

Also see: "Rules and agreements in case research data contain personal data and third parties" (later in this document).

6. Rules and Agreements with Respect to Personal Data

If personal data is used for research purposes, a researcher encounters the General Data Protection Regulation 2016/679 (GDPR), which imposes additional rules and obligations.

The "VSNU Code of Conduct for the Use of Personal Data in Scientific Research" (hereinafter referred to as the "Code of Conduct for the Use of Personal Data") is a translation of the GDPR for societal and behavioral science research. This Code of Conduct for the Use of Personal Data gives the researcher a practical assessment framework on how to handle personal data with care. In the Code of Conduct, personal data is defined as any data relating to an identified or identifiable natural person, i.e. any data that, without disproportionate time or effort, can lead to the identification of a natural person. Personal data are either directly identifying (personal) data or not directly identifying (personal) data.
It is not the intention to discuss the Code of Conduct in its entirety here. Only the starting points for the standard cases are mentioned here:

http://www.vsnu.nl/files/documenten/Domeinen/Accountability/Codes/Gedragscode%20persons data.pdf (Dutch only)
(NB the sections and page numbers mentioned here refer to the text of the Code of Conduct for the Use of Personal Data)

- Only use lawfully collected data obtained with the consent of the respondent for a research. Exceptions are possible (see Section 3.3 onwards on page 12 of the Code of Conduct for the Use of Personal Data).
- Collect data sparingly: no more personal data may be collected than is necessary for the research; anonymous data should be used if possible; personal data will only be processed if there is no other option (see Section 3.2 on pages 11–12 and page 25 onwards of the Code of Conduct for the Use of Personal Data).
- When processing directly identifying data, two files should be created (communication data and research data). Linking takes place via an empty administration number and the access rules for the files must differ (see Section 3.6, page 13 and page 27 of the Code of Conduct for the Use of Personal Data).
- Personal data must be protected during processing and storage so that unauthorized persons (those not involved in the research) cannot have access to them (see Chapter 4, page 15, page 29, and page 30 of the Code of Conduct for the Use of Personal Data).
- Publication may only be made if this cannot be traced back to persons.

Transparency: report to the Data Protection Officer and schedule
If the research consists of processing data that can be directly or indirectly traced back to a natural person, the researcher must fill in the "Integrated form for Ethics (if applicable), Data Management and the Data Processing Register". The form helps to map out the processing operations that will take place for the purpose of the research. The completed schedule should then be sent to the appropriate e-mail address of the School.

On the basis of the completed inventory schedule, the DPO, if necessary in consultation with Legal Affairs, can advise on compliance with the legal conditions for the protection of personal data and the Code of Conduct. It can also be tested whether further assessment of the security measures by the Computer Emergency Response Team (CERT) of LIS is desirable.

It is important to comply with the GDPR in order to protect the privacy interests of those involved. Another reason has been added since 2016: the Authority for Personal Data may impose a fine for breaches of the GDPR (with a maximum of €820,000).

Storage of personal data

The Netherlands Code of Conduct for Scientific Practice[1] states that, in the context of verifiability, a minimum storage period of ten years applies to raw research data.
Verifiability is an aspect of ethical research. On this basis, it is justifiable to store the personal data file for a minimum of ten years if this is necessary for verifiability. However, a distinction must be made between direct and indirect identifying data.

Main rules from the Code of Conduct on personal data (see Section 3.10, page 14 and the explanation on page 29)

1. Communication file: all communication data (except sex, place of residence, and year of birth, Section 3.8, page 14) should be deleted as soon as it is no longer necessary for the purpose of the research to have them and data are no longer necessary for contacting the person concerned. If the communication data are kept longer than six months after being obtained from data subjects, the processing of personal data must be reported to the DPO. This notification can be made immediately upon the first notification by stating in the "schedule for assessment of the processing of personal data" that the communication data will be stored for longer than six months.
2. Files containing directly or indirectly identifying personal data, in which no distinction is made between communication and research files, may be kept for as long as it is reasonably foreseeable that it will be necessary for the research. Files containing anonymous data may be kept as long as it is certain (by means of new analysis techniques) that these data do not allow individuals to be traced.

Data leaks: report

On January 1, 2016, the Data Breaches (Reporting Obligation) Act came into force. This duty to report means that organizations that process personal data must immediately report to the Authority for Personal Data as soon as there is a data leak. See also the Data Leaks Protocol (Dutch only): https://www.tilburguniversity.edu/web/nl/intranet/ondersteuning-werk/juridisch/privacy/avg/download-procedure-melding-en-afhandeling-datalekken.htm

Rules and agreements in the event that research data personal data are shared with third parties

If you share research data that includes personal data, for which Tilburg University is responsible, with a third party (e.g., a hospital, a researcher who is not employed by Tilburg University, or the data is stored by a third party), further conditions apply. When you engage a third party to process data for your research (for example in the case of the storage of research data with personal data by a third party), the third party is often seen as a so-called processor. In such situations, it is a legal obligation to conclude a processing agreement between Tilburg University, as the party responsible for the data processing, and the processor. In this agreement, the parties lay down, for example, the purposes for which the data may be processed by the processor and the security measures to be taken by the processor. The processing agreement, like collaboration or research agreements, must be signed by the School Board. Legal Affairs has a model is available.

[1] As of October 1, 2018, there is a new Code of Conduct for Scientific Integrity. The text of this Guidance has not yet been amended accordingly. More information about the new Code of Conduct and research data management can be found on the Research Support weblog.

In other situations in which research data with personal data are shared with third parties, this is only allowed on the condition that further processing of the personal data by this third party is not incompatible with the purpose for which the data were originally collected by you.

If students are involved in the research who will also process personal data, the students will have to sign a confidentiality agreement. Care must also be taken to ensure that the personal data processed by the students are protected against loss or unlawful processing.

7. Research Data Office

The Executive Board has appointed LIS for carrying out its responsibilities set out in the Research Data Management Regulations. In order to support the implementation of the Research Data Management Regulations, LIS will set up a Research Data Office (RDO). This Research Data Office will function as a central hub in which various divisions of Tilburg University bundle their support services regarding research data. Coordination of the RDO is the responsibility of LIS, which, depending on the subject, calls in specialist assistance from Legal Affairs, IT Services, Academic Services, and other parties involved.

The RDO:

- provides supervision and manages external relations regarding research data management;
- manages a supporting website on research data management http://www.tilburguniversity.edu/datamanagement;
- participates in policy development and audits.

The details of the RDO's service package for the Schools will be set out in another memorandum.

If you have any questions about the Research Data Management Regulations, this guideline and research data management (RDM) in general, please contact the authors of this guideline at researchdataoffice@uvt.nl. Intranet: http://www.tilburguniversity.edu/rdo/

Please note. The university intranet is currently being revised, which means that links may change. In that case, use http://www.tilburguniversity.edu/datamanagement and navigate to the right subject.

Tilburg, January 31, 2019
Version 3.1 (adapted to procedural changes in the context of the introduction of the General Data Protection Regulation on May 25, 2018)