

RESEARCH DATA MANAGEMENT POLICY FACULTY OF HUMANITIES, 2023

RESEARCH DATA MANAGEMENT POLICY FACULTY OF HUMANITIES, 2023

A. Introduction

This document describes the policy for research data management at the Faculty of Humanities (FGW) of the Vrije Universiteit Amsterdam (VU) and describes how the general RDM policy of the VU (v. 2.0)¹ is to be implemented on the faculty level. This policy document is informed by the VSNU's Netherlands Code of Conduct on Scientific Practice,² the Standard Evaluation Protocol (2015-2021),³ the FAIR Principles,⁴ the Research Ethics Review Protocol of the Faculty of Humanities (v. 2021),⁵ the General Data Protection Regulation (GDPR)⁶ and their Dutch equivalents (AVG and UAVG).⁷

1. This policy document applies to all research conducted at FGW, unless the responsibilities for research data management are placed at a different lead institution as part of a research collaboration.
2. For the purposes of this policy document, research data are defined as recorded information that is necessary to substantiate scientific research. At FGW, this may involve text, images, code, video, sound, spreadsheets, databases, interviews, archaeological finds, and many more.
3. Non-digital data are beyond the scope of this document. For advice on the processing of non-digital data, researchers at FGW are advised to contact the Faculty Data Steward (all contact details are listed at the end of this document).

B. Purpose of this document

This policy document aims to do the following:

1. raise awareness on the importance of proper research data management;
2. familiarize FGW researchers with the facilities available at the VU to process their data in line with the FAIR Principles;
3. make FGW researchers aware about the legal obligations when working with privacy-sensitive material, and to inform FGW researchers that they can only work with this kind of data after the approval of the Research Ethics Review Committee (ETCO);
4. define the roles and responsibilities when it comes to research data management at the Faculty;
5. inform FGW researchers about RDM support available at the Faculty and the University Library.

C. Data Management Plan

In order to ensure the transparency and verifiability of research, and to promote (if possible) the reusability of research, it is crucial that research data is properly handled throughout the different stages of a research project (and after). A Data Management Plan (DMP) is a document that helps researchers to formulate and plan their research. It is meant to offer the researcher guidance throughout their research project and a detailed DMP is often the first deliverable after having received a grant from a funding agency. A DMP covers topics such methods used for data collection, licenses, ethical guidelines, storage, and archiving.

¹ <https://edu.nl/7gebv>.

² <https://edu.nl/djeu6>.

³ <https://edu.nl/tgdm7>.

⁴ <https://www.go-fair.org/fair-principles/>.

⁵ <https://edu.nl/8guea>.

⁶ <https://edu.nl/rehfw>.

⁷ <https://wetten.overheid.nl/BWBR0040940/2021-07-01>.

1. Every new research project that receives external funding requires a DMP. Research projects without external funding are still advised, but not required, to complete a DMP.
2. Researchers are expected to use the template offered by the funding agency when drafting their DMP. If the funding agency does not require researchers to use a specific template or if the project is not financed by an external party, researchers are advised to use the DMP Online tool offered by the University Library (<https://dmponline.vu.nl>).
3. PhD candidates working with data follow the mandatory course “Writing a Data Management Plan” during the first or second year of their PhD.
 - a. PhD candidates are expected to register for this course via the website of the Graduate School of Humanities.
 - b. PhD candidates need to deliver a complete DMP, approved by the teacher and Faculty Data Steward, in order to pass for this course.
 - c. PhD candidates that do not work with data are still advised to follow this course but may be exempted from participation. PhD candidates should contact the Faculty PhD counselor and Data Steward to find out if they are eligible for an exemption.
4. A DMP is a ‘living document’. Researchers are expected to update their DMP throughout the course of a research project.

D. Privacy and Ethics Review

Research in the Humanities frequently involves the (re)use of personal data. Personal data means any information relating to an identified or identifiable natural, living person. Anyone who processes personal data needs to comply with the European General Data Protection Regulation (GDPR) and the Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). This applies to personal data of any kind, including public internet data, such as text, photographs, databases, videos, audio recordings, etc. If applicable, it is required to take additional steps throughout a research project in order to ensure the personal data is properly handled.

1. The processing of personal data **always** requires a legal ground. For advice, researchers should contact the Faculty Privacy Champion.
2. Every research project that processes personal data needs to be submitted to the FGW Research Ethics Review Committee (ETCO) **at least one month prior** to the start of data collection.
 - a. The policy document “Research Ethics Protocol of the Faculty of Humanities at Vrije Universiteit Amsterdam” (v. 25.01.2021)⁸ applies to all research projects that process personal data.
 - b. The ETCO has been given a mandate by the Board of the Faculty to formally assess research projects. Research projects that process personal data require a positive advice by the ETCO before they may commence. The positive advice issued by the ETCO is given in principle for a five-year period.
 - c. The ethics review is applicable to studies that are not medical or clinical in nature. In accordance with the Medical Research involving Human Subjects Act (WMO),⁹ research that is medical or clinical in nature needs to be submitted to an accredited MERC (Medical Research Ethics Committee). In case of uncertainty, the ETCO may request a non-WMO statement from the researcher.

⁸ <https://edu.nl/8guea>.

⁹ <https://wetten.overheid.nl/BWBR0009408/2022-07-01>.

- d. Researchers are required to use the online application form and follow the guidelines (available on the FGW website)¹⁰ when applying for ethical approval.
3. Researchers must take appropriate measures to ensure that personal data is securely stored and protected throughout the research project and after (see § E3-4).
4. In case a third party is involved in a research project that processes personal data, a data processing or joint controller agreement may be legally required.
 - a. Only the Faculty Director of Operations is allowed to sign a data processing or joint controller agreement on behalf of the researcher.
 - b. Researchers should contact the Faculty Privacy Champion for advice when drawing up a data processing or joint controller agreement.
5. When working with personal data, researchers must register their research in the VU central registry of processing activities (via <https://dmponline.vu.nl>). This takes place after the research project has received a positive advice from the ETCO.
6. If a student carries out a project that processes personal data, it is the responsibility of the researcher who authorized the research to ensure that the data is handled in accordance with ethical and legal standards. A request to the ETCO is necessary for student research when one (or more) of the following criteria apply (please note that a request to the ETCO can only be submitted by the student's supervisor):
 - a. The student's supervisor plans to publish the results of the proposed project together with the student.
 - b. The student's supervisor plans to reuse the data collected by the student for further study.
 - c. A third party has requested ethical review for the project.

E. Storage and archiving

During and after a research project, data has to be stored professionally and securely in order to optimize workflows, to minimize the risk of loss and/or misuse, and to encourage collaboration (if possible). To this end, the VU has several storage solutions available.

1. Researchers are expected to use a storage solution suitable for the type of data they work with (e.g. SURFDrive, Research Drive, YODA, SciStor). Researchers should contact the Faculty Data Steward and/or consult the [Storage Finder](#) of the University Library in case they are unsure which storage solution to use, or if they want to request access to one of these storage solutions.
2. In the interests of privacy and information security, it is not allowed to use free cloud solutions (such as Dropbox or Google Drive) for any files relating to the university.
3. Personal data needs to be stored on Research Drive or YODA over the course of a research project.
4. When sharing (personal) data with colleagues, researchers are expected to use a software program designed to do so in a secure manner, for example ZIVVER or SURFfilesender.
5. Upon publication or completion of a research project at FGW, all research data relevant to the publication or project must be stored (archived) in a trusted repository for a minimum of ten years. This applies both to raw and processed data, including relevant codes and scripts. Metadata should also be archived along with the data (i.e. project name, names of project leaders and other participating researchers, type of data, processing method, software and encryptions used, data access rights, third-party data ownership, storage time, financing of storage, etc.).
6. When archiving research data, researchers may use the facilities provided by VU Amsterdam or DANS (including DataverseNL). Researchers are also free to choose a different storage facility. When doing so, it is recommended to use a repository that has been awarded with a CoreTrustSeal (guaranteeing that the repository is

¹⁰ <https://edu.nl/phkfy>.

sustainable and trustworthy) and that provides a persistent identifier (a DOI) for your dataset (guaranteeing long term access).

7. When archiving personal data, researchers should make use of YODA, which currently provides the best GDPR-compliant option to store personal and/or sensitive data for at least 10 years at the VU. In case researchers want to store the personal data in a different repository, a data processing or joint controller agreement may be legally required (see § D4).
8. When publishing research results (including datasets), researchers are expected to publish as much as possible through Open Access channels, unless there are privacy related or intellectual property related reasons not to do so. The principle “as open as possible, as closed as necessary” applies. The Faculty encourages researchers to contact the Open Access service of the University Library, which offers support in publishing research results in open access and in making previous publications accessible to a wider public.
9. All researchers are required to register their research results (including their datasets) through the [PURE](#) portal.

F. Finances

Data storage and archiving may entail additional costs that must be included in the budget when applying for funding at institutions like the NWO. Regarding the costs for research data management, the Faculty follows the guidelines set out by the University Library. As it stands, the costs for all VU-supported storage (SURFDrive, Research Drive, YODA, and Scistor) and archiving (YODA, DataverseNL, OSF) solutions are covered up until 500 GB. Additional expenses come in to play when research projects require more than 500 GB of storage or archiving or when researchers opt for an archival solution that is not supported by the VU. If so, researchers are expected to take appropriate measures to secure finances (via project, department or faculty) before the start of their research project.

G. Ownership

Reuse of existing research data

1. If researchers intend to reuse data that has already been made available by a third party, they must make a request to the rightful owner to use the data for the purposes of the research project, unless the data is explicitly shared under an open license.
2. Insofar as copyright regulations allow, researchers must also make a request to the rightful owner of the data for the right to redistribute the data upon publication and/or completion of the project.
3. The reuse of data(sets) containing personal data is only allowed when there is a legal ground to do so, for example when the reuse of the data for further research has been explicitly included as a condition in the original informed consent form.
4. Please note that research projects that intend to reuse personal data still need to be registered in the VU central registry of processing activities (see § D5).

Newly acquired research data

5. The Faculty operates on the principle that ownership of newly-acquired research data lies with VU Amsterdam or with the funding body, and that Open Access is the norm (see § E8).
6. When researchers collaborate with parties outside VU Amsterdam, agreements must be made about the joint management and archiving of the research data. Researchers should contact the Faculty Data Steward before the start of the project for advice on this matter.

7. In the event of a researcher leaving the university, the relevant head of department will be responsible for making agreements about the management of research data after the termination of the researcher's employment contract.
8. In the case of doctoral research, the supervising professor makes arrangements with the PhD candidate about the archiving of the research data after the defense of the dissertation.

H. Responsibilities

In accordance with the general RDM policy of the VU (v. 2.0),¹¹ researchers are personally responsible for:

1. compliance with legal and ethical requirements regarding their research data (see § D, G);
2. ensuring that their research data are reliably, traceably, and securely stored and archived (see § E);
3. being able to share their research data for scientific use and verification unless there are privacy-related or intellectual property-related reasons not to do so (see § E8-9).

To this, the Faculty adds that researchers are expected to:

4. to write and maintain a Data Management Plan for every new research project that receives external funding (see § C);
5. to take appropriate measures to secure additional finances (via project, department or faculty) before the start of their research project, if necessary (see § F);
6. to ensure that student research complies with the legal and ethical requirements described in this document (including submission to the ETCO if applicable, see § D6);
7. report data leaks¹² as soon as possible to the IT Service Desk on 020-59 8000 via e-mail to servicedesk.it@vu.nl.

PhD candidates are required to:

8. follow the mandatory course "Research Integrity – Arts and Humanities" (registration via the Graduate School of Humanities), which includes a session on Research Data Management;
9. follow the mandatory course "Writing a Data Management Plan" (registration via the Graduate School of Humanities) during the first or second year of their PhD (see § C3).

Department heads are responsible for:

10. reaching agreements with researchers about their research data in the event that they leave the university;
11. to take an active role in promoting proper research data management at their department.

Lastly, the Board of the Faculty is responsible for:

12. monitoring and evaluating the implementation of this policy and making adjustments where necessary.

¹¹ <https://edu.nl/7geby>.

¹² A data leak is a security incident in which personal details may have been lost or may have been accessed, viewed, changed or used by unauthorized persons. Examples include: a lost USB stick with personal information, a stolen laptop, an email with personal information that was sent to the wrong recipient, a hacked file or hijacked computer, etc.

I. Contact information*Faculty*

FGW Data Steward

data.fgw@vu.nl

FGW Privacy Champion

data.fgw@vu.nl

FGW Research Ethics Review Committee

etco.fgw@vu.nl

FGW Research Office

research.office.fgw@vu.nl*VU*

Research Data Management support desk

rdm@vu.nl

IT Service Desk

servicedesk.it@vu.nl

Open Access support team

openaccess@vu.nl

Privacy lawyers

privacy@vu.nl**J. Author's note**

Author: Dr. Sam Heijnen, Data Steward & Privacy Champion at the Faculty of Humanities.
The Faculty Board adopted this policy document at its meeting of 4 July 2023.