Research Data Management Policy at the Faculty of Humanities

Adopted by the Board of the Faculty of Humanities on 26 November 2019.

Introduction

In January 2016, Vrije Universiteit Amsterdam (VU Amsterdam) published its policy document on Research Data Management (RDM) and has since updated it where necessary. The latest version dates from February 2020. The key points of this policy document, which also defines the responsibilities of the various parties, can be summarized as follows:

VU Amsterdam attaches great importance to the accessibility of its research output, both in terms of publications (Open Access) and the data on which they are based. The research data must be reliable, traceable and securely stored. This is important in ensuring the observability, controllability, reuse and (if possible) repeatability of the study. This requires responsible management during the research phase and subsequent sustainable storage, in accordance with the FAIR Principles; the rules of the Netherlands Code of Conduct for Research Integrity drawn up by the Association of Universities in the Netherlands (VSNU, 2018); and the rules set out in the Standard Evaluation Protocol (SEP 2015-2021) for independent research assessment. The following legislation and regulations also apply: the Medical Research involving Human Subjects Act (WMO); the General Data Protection Regulation (GDPR) and the Dutch law governing their implementation in the Netherlands (UAVG).

The aim of the RDM policy is, where necessary, to make researchers more aware of their responsibility with regard to the careful handling of their research data, so that they can demonstrate the academic integrity of their research and comply with current requirements regarding the management of their data. This serves the wider aim of maximizing the impact of research at the university and making follow-up research possible.

VU Amsterdam has asked its faculties to draw up their own specific policy documents, elaborating on the university-wide principles in such a way that they reflect the specific circumstances in all departments and research institutes within the faculty. In addition, the Standard Evaluation Protocol requires any unit undergoing an independent research assessment to have a clear policy on academic integrity, a protocol in place to check compliance, and regulations in the event of negligence.

What are the objectives of the faculty's policy on RDM?

Within the faculty, each researcher should be aware of their responsibilities for storing their own research data. When submitting a research proposal to the Dutch Research Council (NWO) or the European Research Council (ERC), a data management plan is now requested as standard. For the correct archiving of research data, both raw and processed data at each research phase should be stored in accordance with the guidelines of the academic discipline concerned. In addition, security against loss, theft and misuse must be ensured and version control must be applied, so that it is always clear how the data has been processed. The following requirements also apply: details of who has access to the data during the research phase (and how this is arranged); details of who has access to the data once the research has been completed (and how this is arranged); details of where and for how long the data is archived (at least 10 years, unless legal provisions or discipline-specific guidelines prescribe otherwise, for example for personal data).

VU Amsterdam's web pages on the theme of research data and the RDM web pages of the University Library provide sound guidelines for recording data of this kind. They also contain a wealth of

information about archiving research data. However, it is the faculty's responsibility to raise awareness among researchers about the importance of research data management and to make them aware that they have clear responsibilities in this area.

The faculty's objectives in this regard are:

- To familiarize researchers with VU Amsterdam's policy on RDM, the faculty's policy derived from it, and the underlying codes of conduct, and to inform them where they can find the relevant policy texts on the VU website, on the University Library's RDM pages and on their own faculty's RDM pages.
- To familiarize researchers with the support offered by the University Library and how to obtain it.[1]
- To familiarize researchers with the role of the faculty's Ethics Review Committee (ETCO) and with the duties of the faculty's privacy officers, and to enable researchers to use the flow charts on the faculty website to check whether their data is privacy-sensitive (i.e. can be traced to individuals).
- To inform researchers that they can only work with privacy-sensitive data subject to the approval of the faculty's Ethics Review Committee.[2]
- To make researchers dealing with privacy-sensitive data aware of their additional obligations under the Netherlands Code of Conduct for Research Integrity drawn up by VSNU and the relevant legislation and regulations, as laid down in the GDPR;[3] relevant information can be found on the University Library website, on VUnet and on the faculty website.
- To offer researchers support, in cooperation with the University Library,[4] so that they can draw up data management plans for research applications and arrange correct storage of raw and processed data during and after their research.
- To cooperate with the University Library[5] to offer researchers RDM training courses on request.
- To oblige PhD researchers to take the annual Research Integrity course run by the Graduate School of Humanities, which covers RDM and privacy policy.

The faculty endorses the new Netherlands Code of Conduct for Research Integrity drawn up by VSNU and the standards for good research practice it contains, particularly in Chapters 2 and 3.
The faculty recognizes its own duty of care as set out in Chapter 4 of this code and has established an Ethics Review Committee and appointed privacy officers for education and research and a confidential counsellor for academic integrity.
In addition, the faculty data steward assists researchers in drawing up data management plans and advises them on suitable ways to store data and metadata before, during and after their research. To this end, the data steward produces an overview of the various storage facilities inside and outside VU Amsterdam, and updates this information as required.

---

[1] Information about the support offered by the University Library can be found on the University Library website. General questions on RDM can be submitted by email to rdm@vu.nl.
[2] The website is still partly under construction.
[3] The Association of Universities in the Netherlands (VSNU) is working on a new version of its Code of conduct for using personal data in scientific research. Once it has been published online, a link will be added to this paragraph.
[4] The position of data steward is currently vacant (autumn 2020). As soon as a new data steward has been appointed, he/she will assist on this course.
[5] Idem.

The data steward also plays a role in the Research Integrity course for PhD students, assessing the data management plans the students draw up on the course.

A more detailed look at the faculty's RDM policy

How to store data during a research project

The University Library website provides sound guidelines for the secure and traceable storage of data during and after research (also known as the data life cycle). Secure storage during research is obviously important to prevent data loss and to enable data sharing and proper data management and processing in cases where research is being carried out jointly. Researchers employed by VU Amsterdam or with guest status can securely store their data on the G drive and/or H drive of the university's computer system.[6] To share data within a faculty research group, a joint project folder can be created on the G drive. A SURFfilesender can be used to transmit data securely and data can be securely shared with researchers outside VU Amsterdam using a SURFdrive or EDUgroepen. In the interests of privacy and information security, VU Amsterdam does not permit the use of free cloud solutions (such as those offered by Dropbox, Google and Amazon) for any files relating to the university. These free solutions do not guarantee the provider's compliance with European privacy laws. Nor do they enable VU Amsterdam to exercise its rights as the owner of the documents. For more information on this issue, see the VUnet pages on storing or sharing documents and data.
As soon as privacy-sensitive data is used, additional rules and guidelines for the secure storage, sharing and transmission of the data must be met. For more information, see the sections below.

What kind of data should be stored after research and for how long?

Researchers are expected to publish as much of their work as possible through Open Access channels and to register their publications on the Pure database. Once data have been used in an article or study, they must be archived within three months of publication (online, or if there is no online version, three months after the publisher's official publication date). As a rule, all data should be archived, even data that have not been used in a publication.
This applies both to raw data and the processing and analyses, including relevant codes and scripts. The analyses of data from third parties or from databases made available should also be archived; this requirement covers both quantitative and qualitative data. Examples of work that should be archived include texts, spreadsheets, databases, statistics, audio and video material (including transcripts), digital maps (GIS), images of archive documents, artworks and images of artworks. Metadata[7] 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.) It is advisable to set out this information in a data management plan at the start of the research project and to supplement it where necessary as the project progresses, even if this is not a requirement imposed by a funding body. For guidance on how to draw up a data management plan, go to the VU RDM Support Desk and dmponline.vu.nl where you can find templates from organizations such as the Dutch Research Council (NWO), the European Research Council (ERC) and Horizon 2020. Two

[6] Access rights for several users can be assigned to folders saved to the G drive. The H drive is strictly personal. Under normal circumstances, these folders cannot be accessed by third parties.
[7] Basic metadata are easy to register in Pure and this contributes to the findability of the datasets.

templates produced by VU Amsterdam can also be found at this address. For templates from the Data Archiving and Networked Services of the Royal Netherlands Academy of Arts and Sciences (KNAW), go to the DANS website.
When storing their research data, researchers can use the facilities provided by VU Amsterdam or DANS (including DataverseNL, to which VU Amsterdam is connected), or the CLARIN infrastructure. Researchers are free to choose one or the other storage facility,[8] in line with the guidelines of their field, provided that all privacy-sensitive data is stored in accordance with the relevant legislation.
In principle, all raw and processed data used in published research, along with the associated metadata, are retained for at least 10 years after publication (starting from the moment of online publication or, if no online version is available, the official publication date supplied by the publisher). This is important both for verification purposes and for potential follow-up research. Depending on the nature of the data, these two objectives may coincide. This will not always be the case for privacy-sensitive data and other retention periods may apply.
VU Amsterdam has no central storage capacity for non-digitized research data. Digitization of data is therefore encouraged as much as possible. The researcher is personally responsible for the proper and secure storage of analogue research data.
Agreements should be made with the faculty about the costs of archiving, especially with regard to research projects that require large amounts of storage space during and after the research. Storage costs for datasets larger than 50GB are not fully covered by VU Amsterdam's central resources and should be included in a project application.

Who is responsible for data storage?
The faculty's researchers are personally responsible for storing their own research data correctly. This requirement also applies to PhD students (including external PhD students) and postdocs. Research carried out by students is the responsibility of the member of the university's academic staff who authorized the research. If at the end of a student research project, a lecturer wishes to use the data collected by the students for further research, she/he bears responsibility for the correct storage of that data.
Each student is required to archive her or his own thesis by uploading it to the University Library's website. The University Library will also be asked to provide storage facilities for the research data and metadata relating to the theses. As the retention period for theses is seven years, a seven-year retention period is also recommended for the associated data and metadata.

Who is responsible for the storage of privacy-sensitive data?
The faculty's researchers are aware that special rules and guidelines apply to the collection, processing and archiving of privacy-sensitive data. The Ethical Research Review protocol[9] drawn up by the Faculty's Ethical Review Committee details the procedure researchers have to follow in submitting research relating to living persons to this committee for review before they are allowed to proceed with their study. Researchers working with privacy-sensitive data submit a data management plan as part of the data to be reviewed by the Ethics Review Committee. This plan also specifies the tools the researcher will use to collect, process and analyse the relevant data. If online tools are used for this purpose, it is mandatory to use tools supplied by organizations with whom the university has signed a processing agreement. It is therefore advisable to make use of such online

[8] For a list of repositories, see www.re3data.org
[9] The English version is not available yet.

tools; if not, the researchers have to arrange their own alternative, in consultation with the faculty's privacy officer.
Guidelines on how to work securely and responsibly with personal data, once permission has been obtained, are described on VUnet: Services – security – privacy & information security.
Researchers are obliged to comply with the conditions stated in these guidelines. They cover rules on encryption (and by extension on anonymization and pseudonymization), secure data sharing, and the proper archiving of privacy-sensitive data during and after research.
If students conduct research involving privacy-sensitive data for a tutorial, the lecturer is responsible for selecting the software used to collect and analyse that data. At the end of the tutorial, these data will be destroyed, unless the lecturer wishes to use them in order to carry out further research. In that case, the lecturer is responsible for the proper handling and storage of these data and requests permission from the Ethics Review Committee for her/his research plans concerning these data and the method of storage during and after the proposed research.
If a student wishes to carry out research involving privacy-sensitive data for a thesis, prior permission must be obtained from the Ethics Review Committee. After permission has been granted, the student will consult her/his thesis supervisor when selecting the software to be used to collect and analyse this data. The student is required to archive her or his own thesis by uploading it to the University Library's website, and is obliged to follow the guidelines for secure and responsible working practices and storage of personal data. The University Library will also be asked to provide storage facilities for the research data and metadata relating to the theses.

The Ethics Review Committee keeps a register of approved projects relating to research with privacy-sensitive data carried out within the faculty (in accordance with GDPR requirements).

Who owns the research data?
In theory, VU Amsterdam is the owner of the research data collected by its employees. In practice, the agreements made mainly concern knowledge transfer and patent rights and seldom relate to research data as intellectual property: does the researcher, the faculty, the university or even an external funding body own these rights?
The Faculty of Humanities operates on the principle that ownership lies with VU Amsterdam or with the funding body, and that Open Access is the norm, unless there are good reasons for excluding data, the main reason being that the data is privacy-sensitive. When researchers collaborate with parties outside VU Amsterdam, agreements must be made about the joint management and archiving of the research data.
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. This is in accordance with the provisions of VU Amsterdam's RDM Policy (version 2020, page 5). In the case of doctoral research, the supervising professor makes arrangements with the PhD candidate about the archiving of the research data after the defence of the dissertation. These arrangements form part of the candidate's data management plan.
The Director of Research has random checks carried out to ensure compliance with these arrangements.

What measures are taken with regard to quality assurance?
Within each of the three departments, an annual meeting is held to discuss best practices in research data management and Open Access, and how to apply privacy legislation to research and education.

The head of department invites the faculty's privacy officers and the faculty's data steward to this meeting. The departments share examples of best practice with each other and with the Faculty Board.
Once a year, the Director of Research selects one publication per department on behalf of the Faculty Board and asks the data steward to conduct a critical examination of the publication process. Is it an Open Access publication and if not, why not? Have the publication and the dataset been registered in Pure? Has the research data been archived and made available for follow-up and/or repeat research? The data steward then reports to the board of education, which in turn reports to the Faculty Board, so that the Dean can provide an account of the research data policy pursued at the Consultative Meeting for Portfolio Holders.
The Committee on Scientific Practice will be asked to advise on RDM and Ethical Review policy.
The policy on Research Data Management is evaluated once every two years by the Director of Research and modified where necessary. Any changes to these policy documents will always be submitted to the Committee on Scientific Practice and the faculty's Ethics Review Committee for advice. The policy is adopted by the Faculty Board after consultation with the faculty's Management Team and Joint Assembly.

Author's note

The following resources were consulted in the writing of this policy document: the RDM policy documents of the Faculty of Social Sciences and the Faculty of Science at VU Amsterdam (both available on the University Library website: http://libguides.vu.nl/researchdata/policies-and-regulations); the RDM policy document of Tilburg University's School of Humanities (undated); the University of Amsterdam/Amsterdam University of Applied Sciences Data Protocol Guide (version: July 2015); the Scientific Research Archiving Directive of the Dutch faculties of Social and Behavioural Sciences (version: 2 July 2017); and the policy documents and other material referred to in links and footnotes.
An editorial decision was taken to limit the length of the document by incorporating links to relevant online references, most notably to VUnet and the VU University Library website.

The draft version of this document was amended in response to feedback from Lex Bouter (Full Professor of Methodology and Integrity) and was discussed in the Committee on Scientific Practice. Feedback provided by Jolien Scholten (RDM specialist at the University Library), Eric Akkerman (privacy officer for education at the Faculty of Humanities) and Onno Huber (specialist in Humanities Computing/data steward at the Faculty of Humanities) has also been incorporated. The Committee on Scientific Practice approved the amended version. In its final stages, this version was submitted for advice to all chair holders (by email on 31 October 2019). This did not result in any further additions or modifications.
The Faculty Board adopted the final version at its meeting of 26 November 2019, and the author delivered the update on 22 September 2020.

Author: Liesbeth Geudeke, Senior Research Policy Officer at the Faculty of Humanities