Research Data Management policy

Vrije Universiteit Amsterdam | Version 2.0, 17-2-2020

INTRODUCTION

Vrije Universiteit Amsterdam is strongly committed to the accessibility of research output, namely publications and data.[1] They are important to the visibility, verifiability and reusability of research.[2]

This policy document summarizes the university-wide principles for careful handling of research data. At the level of the faculties, these principles are developed into faculty guidelines that comply with the central policy and cover all departments and research institutes.

This document shows how the responsibilities with respect to research data are covered within the VU, based on the Netherlands Code of Conduct for Research Integrity (previously Netherlands Code of Conduct for Academic Practice) from the VSNU, the Standard Evaluation Protocol (SEP) for Research Assessments in the Netherlands 2015-2021, the FAIR principles[3] for research data and relevant legislation. In addition, it presents the facilities provided by the VU for managing research data. The document may be updated if required by new developments.

PURPOSE OF THE RESEARCH DATA MANAGEMENT POLICY

This policy is intended to promote:
1. the careful handling of research data by researchers in order to:
   - enhance the impact of their research,
   - demonstrate the scientific integrity of their research,
   - comply with legal requirements, codes of conduct and funding bodies' demands regarding Research Data Management;
2. awareness of the importance of Research Data Management among researchers;
3. clarity about the responsibilities regarding Research Data Management among researchers.

---

[1] Research data are defined as recorded information that is necessary to substantiate scientific research. Depending on the discipline concerned, this may involve, for example, text, images, sound, spreadsheets, databases, statistical data, geographic data, etc. Non-digitizable research data are outside the scope of this policy.

[2] See also the Vrije Universiteit's strategic plan.

[3] See FORCE11's website (https://www.force11.org/group/fairgroup/fairprinciples) for a description of the FAIR data principles and the article by Wilkinson et al. (2016; doi:10.1038/sdata.2016.18) for an elaborate discussion.

POLICY PRINCIPLES

1. The VU is strongly committed to the accessibility of research output, namely publications and data. They are important to the visibility, verifiability and reusability of research.

2. The VU subscribes to the Netherlands Code of Conduct for Scientific Integrity, drawn up by the Association of Dutch Universities (VSNU).[4] On the subject of handling research data, this code includes the following clauses:

   - 3.2.10 As necessary, describe how the collected research data are organized and classified so that they can be verified and reused.
   - 3.2.11 As far as possible, make research findings and research data public subsequent to completion of the research. If this is not possible, establish valid reasons for their non-disclosure.
   - 3.3.23 Describe the data collected for and/or used in your research honestly, scrupulously and as transparently as possible.
   - 3.3.24 Manage the collected data carefully and store both the raw and processed versions for a period appropriate for the discipline and methodology at issue.
   - 3.3.25 Contribute, where appropriate, towards making data findable, accessible, interoperable and reusable in accordance with the FAIR principles.
   - 3.4.35 Be transparent about the method and working procedure followed and record them where relevant in research protocols, logs, lab journals or reports. The line of reasoning must be clear and the steps in the research process must be verifiable. This usually means that the research must be described in sufficient detail for it to be possible to replicate the data collection and its analysis.
   - 3.4.45 As far as possible, make research findings and research data public subsequent to completion of the research. If this is not possible, establish the valid reasons for this.

   Additionally, the code of conduct defines the following duties of care for institutions:
   - 4.4.11 Provide a research infrastructure in which good data management is the rule and is facilitated.
   - 4.4.12 Ensure that, as far as possible, data, software codes, protocols, research material and corresponding metadata can be stored permanently.
   - 4.4.13 Ensure that all data, software codes and research materials, published or unpublished, are managed and securely stored for the period appropriate to the discipline(s) and methodology concerned.
   - 4.4.14 Ensure that, in accordance with the FAIR principles, data is open and accessible to the extent possible and remains confidential to the extent necessary.
   - 4.4.15 Ensure that it is clear how data, software codes and research material can be accessed.

3. Standard Evaluation Protocol (SEP) for Research Assessments in the Netherlands 2015-2021:
   - "The assessment committee considers the research unit's policy on research integrity and the way in which violations of such integrity are prevented. It is interested in how the unit deals with research data, data management and integrity."
   - "Self-assessment includes explaining how the unit deals with and stores raw and processed data."

---

[4] This refers to the code of conduct from 2018 (https://www.vsnu.nl/en_GB/research-integrity). NB: the previous version of this Research Data Management policy (2016) was based on the Code of Conduct for Academic Practice 2004 (version 2014).

4. Research must comply with all relevant legislation and regulations, including:
   - General Data Protection Regulation (GDPR)
   - Implementation Act for the General Data Protection Regulation (UAVG)
   - Medical Research Involving Human Subjects Act (WMO)
   - Code of Conduct for Health Research
   - Experiments on Animals Act

5. Ownership of the research data is subject to intellectual property laws (Copyright Act, Patent Act, Databases Act), the Collective Labour Agreement for Dutch Universities (Article 1.20-1.23), and the regulations for Knowledge Exploitation VU[5] (in Dutch), unless otherwise agreed upon with funding bodies.

---

[5] Knowledge Exploitation VU: https://vunet.login.vu.nl/services/pages/manual.aspx?cid=tcm%3a164-916527-16 (in Dutch).

VRIJE
UNIVERSITEIT
AMSTERDAM

RESPONSIBILITIES

RESEARCHERS

1. Researchers are responsible for compliance with legal and ethical requirements regarding their research data, including review by ethics committees[6] if necessary.[7]

2. Researchers are responsible for ensuring that their research data are reliably, traceably and securely stored throughout the data life cycle[8] and that they are able to report the storage location of their data to the department head, for example upon termination of their employment at the VU. At the same time, department heads are also responsible for making agreements with researchers on such issues, see article 7 under 'Responsibilities' in this policy.

3. Researchers are responsible for archiving their research data for a minimum of ten years after research results are published, unless legal requirements, discipline-specific guidelines or contractual arrangements dictate otherwise. The moment of publication is defined as the first online appearance of the publication. If there is no online publication date, the formal publication date of the publisher applies. If a researcher's employment terminates between the events of submitting a publication and the actual moment of publication, agreements must be made regarding these data archiving responsibilities according to articles 2 and 7 under 'Responsibilities' in this policy.

4. Researchers are responsible for being able to share their research data for scientific use and verification, by making them accessible (A in FAIR) to others, preferably and where possible with a Persistent Identifier.[9] Before research data are shared for reuse or verification, a researcher has to make sure that this is compliant with applicable legislation and ethical requirements. When research data include personal data, an assessment must first take place to determine whether these data can be shared and if so, under which conditions.

5. The VU ensures that research data that are generated at the VU are Findable (F in FAIR) by including descriptions of these datasets in the Current Research Information System (CRIS) of the VU.[10] Researchers' responsibilities in this process are as follows: researchers can perform this registration themselves, or they or their research support staff can request the CRIS administrator (vuresearchportal.ub@vu.nl) to do this registration by providing the necessary information (e.g. the storage location of the dataset, author information, project information).

---

[6] See the LibGuide Research Data Management (http://libguides.vu.nl/researchdata/laws-and-regulations#s-lg-box-wrapper-16956668) for an overview of ethics committees.

[7] The university (Stichting VU) is ultimately legally responsible for compliance with the applicable legislation, including the GDPR.

[8] The data life cycle encompasses the various components of dealing with research data in the different stages of the research process (design, analysis and conclusion): preparing, creating, collecting, processing, analyzing, storing, publishing and reusing data.

[9] See for example the website by the Dutch Digital Heritage Network for a description of Persistent Identifiers (https://www.netwerkdigitaalerfgoed.nl/kennis-en-voorzieningen/digitaal-erfgoed-houdbaar/persistent-identifiers/).

[10] NB: This solely concerns the registration of archived datasets. To archive the data, researchers can use digital VU repositories or, where appropriate, external repositories provided that no legal or ethical rules are violated in doing so.

6. Researchers who collect and process personal data for their research, must comply with the requirements of the GDPR and the UAVG and, additionally, they must register these activities in a processing register. Keeping a record of processing activities is a legal requirement (imposed by the GDPR). The Privacy Champions[11] in the faculties are the first point of contact for support on these matters.

DEPARTMENT HEADS

7. Department heads are responsible for arranging agreements with researchers in their departments regarding the management of research data, particularly when a researcher's employment is ending. See article 2 of this policy for more detail.

FACULTIES

8. Faculties must establish their own Research Data Management policies which are applicable to all of their departments and institutes, and that include, where necessary, discipline-specific protocols.
9. The dean annually reports on their faculties' Research Data Management policies at the PO (*Portefeuillehoudersoverleg* or Portfolio Holder) meeting.

UNIVERSITY

10. The university is ultimately responsible for compliance with all applicable legislation (primarily the GDPR and UAVG) by the VU and researchers at the VU.
11. The university is responsible for providing basic Research Data Management facilities.[12] The university also facilitates the findability of research data through the registration of datasets in CRIS (see also article 5 under 'Responsibilities' in this policy) and supports researchers, whenever possible, with this dataset registration process.[13]
12. The university is responsible for providing Research Data Management training, support and advice to researchers.

FACILITIES

1. The VU supports researchers in planning, managing, analyzing and archiving research data. The LibGuide Research Data Management[14] offers a summary of all relevant products and support services and provides more information on all aspects of Research Data Management.
2. For the registration of research with personal data the VU has a record of processing activities. Each faculty and business unit has one or more Privacy Champions who provide first-line support. There is a list of these Privacy Champions[15] available on VUnet. In addition, the VU has legal experts on matters relating to privacy[16] at the department of Institutional Affairs, who provide second-line support. The VU also has a Data Protection Officer (DPO)[17]

---

[11] See VUnet for the list of Privacy Champions (https://vunet.login.vu.nl/services/pages/categorydetail.aspx?cid=tcm:165-890669-16&category=tcm:165-892563-1024).

[12] The available facilities can be found on the Research Data theme site on VUnet (https://vunet.login.vu.nl/themes/pages/standaard.aspx?cid=tcm%3a165-414220-16) and the LibGuide Research Data Management (http://libguides.vu.nl/researchdata).

[13] The University Library (UL) will provide this support.

[14] LibGuide Research Data Management: http://libguides.vu.nl/researchdata.

[15] List of Privacy Champions: https://vunet.login.vu.nl/services/pages/categorydetail.aspx?cid=tcm:165-890669-16&category=tcm:165-892563-1024.

[16] Legal privacy experts: https://vunet.login.vu.nl/services/pages/categorydetail.aspx?cid=tcm:165-851499-16&category=tcm:165-851784-1024.

[17] Data Protection Officer:

who monitors compliance with legislation regarding the protection of personal data by the VU. The DPO has an independent advisory role.

3. The VU provides the following support regarding IT and information security:

   a. General questions from researchers about information security can be addressed via the RDM Support Desk (rdm@vu.nl). These concern practical questions, for example, about choosing a suitable storage facility for research data.

   b. (Potential) security incidents must be reported to the IT Service Desk (servicedesk.it@vu.nl). Security incidents occur when the confidentiality, integrity or availability of information or data processing systems has been threatened, or potentially threatened, for example, attempts to gain unauthorized access to information (hacking), the loss of a USB stick containing sensitive information, or data or hardware theft.

   c. For tailored advice or support, contact IT relationship management. The IT relationship managers bring researchers into contact with the correct people so that they can request IT capacity for the purpose of setting up and/or assessing security plans. Security plans generally need to be drawn up when: research projects have complex infrastructures (e.g. international collaboration, the use of various data sources and databases); customized technical solutions are required; or funding agencies or external partners require such a plan.

   d. For questions about the assessment of policy and strategy concerning information security contact the Information Security Officer (ISO)[18]. This, for example, concerns questions about the consequences of using new techniques for information security, or which steps research groups need to take to work according to guidelines for information security.

---

https://vunet.login.vu.nl/services/pages/practicalinformation.aspx?cid=tcm%3a164-913083-16.
[18] Information Security Officer:
https://vunet.login.vu.nl/organization/pages/department.aspx?cid=tcm%3a165-882892-16.