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.

VU VRIJE UNIVERSITEIT AMSTERDAM

© 2020 Vrije Universiteit, Amsterdam

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).

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.