Research Data Management Policy
Faculty of Behaviour and Movement Sciences

Introduction

This document describes the implementation of research data management policy within the Faculty of Behavioural and Human Movement Sciences (FGB). It supplements the Research Data Management Policy of Vrije Universiteit Amsterdam (dated January 12, 2016; a new version is expected in 2019), and is informed by the VSNU Code of Conduct for Research Integrity, the VSNU Code of Conduct on the Use of Personal Data in Scientific Research, the Federa Code of Conduct for Responsible Use of Human Tissue in Medical Research, the Federa Code of Conduct for the Use of Data in Health Research, the Standard Evaluation Protocol (SEP 2015-2021), ICH Good Clinical Practice Guidelines, the Medical Research with Humans Act (WMO), the Medical Treatment Agreement Act (WGBO), the General Data Protection Regulation (GDPR) and the national implementation of the GDPR (UAVG). Data are defined within the FGB and this policy as not only the values of quantitative or qualitative variables, but also audiovisual recordings, handwritten text notes, imaging data, such as MRIs, and bodily tissues.

Purpose of the FGB Research Data Management Policy

This policy supplements the general VU Research Data Management Policy by:

1. Defining the roles and responsibilities within the FGB regarding research data management
2. Advising researchers on the balance between open science and data protection legislation
3. Informing FGB researchers of FGB specific tools, guidelines and support services for research data management

Definitions

Research project: The research activities described in a research proposal that is submitted for ethical review. Where ethical review does not apply, a research project is any research activity aimed at answering a hypothesis; all activities aimed at answering one overarching hypothesis can be described as a single research project.

Personal data: Any data that can be linked to an individual person. These may directly identifiable data, such as name, address, video recordings or photographs, but they may also be indirectly identifiable information, such as IP or MAC addresses, genetic information, unique physical measurements of high-level athletes or any other characteristics, such as ethnicity, gender, occupation or education, that when combined make it possible to identify a person.

Archiving research data: The long-term storage of research data in a manner that prevents modification, loss, damage or obsolescence so that the data remain (re)useable well into the future.

Publishing research data: An extension of archiving research data; published data are also findable, accessible and reusable by other researchers. This does not mean that data are open access; access can also be restricted to only approved researchers.

FAIR principles: Guiding principles for achieving high-quality data, as well as the associated metadata, so that the data can be reused by other researchers. FAIR (meta)data should be findable, accessible, interoperable (i.e. should be functional in any digital environment) and reusable.

Metadata: Data that describes research data so that this data can be properly understood and reused well into the future.

Policy Principles

In addition to the points listed in the general VU Research Data Management Policy, the following policy principles apply within the FGB:

1. Research data management is an essential component of every research project. Every research project requires a data management plan, regardless of whether or not this is required by the funder. Data management plans should be reviewed and updated throughout the research lifecycle.

2. Data should be made accessible for reuse through the application of the FAIR principles, while also respecting the constraints of privacy, ethics, facilities, and finances.

3. Effective research data management skills and the FAIR-principles are essential elements in the education of PhD candidates and students following research-based Masters and Bachelors programs.

4. Research data management requires teamwork within the faculty. Every individual should know their own responsibilities, but should be aware of the support services available to them and make use of these services as required.

Responsibilities

Researchers

1. It is assumed that researchers know and apply the VSNU scientific code of conduct, the VSNU Code of Conduct on the Use of Personal Data in Scientific Research, the VU RDM Policy, and the FGB RDM policy. Researchers conducting research projects that fall under the purview of the WMO should also be familiar with the relevant legislation and codes of conduct as described by the CCMO and the METc VUmc.

2. Researchers who work with personal data are required to understand and comply with the privacy requirements of the GDPR and UAVG and conduct their research in a manner that ensures that data confidentiality and integrity are maintained throughout the project
    a. Researchers must send a copy of the data management plan and, if applicable, the data protection impact assessment to the research data officer.

   b. Researchers must ensure that students and interns working temporarily within the FGB can work in a manner that meets the privacy requirements[1] .
   c. Researchers must ensure that the research assistants and data managers, for whom they are responsible, are sufficiently aware of their privacy requirements and that they are able to transport data securely when working remotely[1].
   d. Interns and other individuals not officially working for the VU must sign a confidentiality statement if they will be working with confidential data.

3. Researchers are responsible for determining who is allowed to access the research data both within the faculty and between institutions. Senior researchers, project co-ordinators and project leaders should assist junior researchers and interns with this determination; advice from the research data officer can be requested, when necessary.
   a. Researchers are responsible for completing the appropriate data sharing agreements with any external parties prior to starting a research project. In the case of research using personal data, a co-collaboration agreement should be completed between all parties that are responsible for the personal data. A processing agreement must be signed if a third-party processor has been hired to process personal data on behalf of the VU.
   b. Research that is solely conducted within the VU is owned by the Stichting VU. For any collaborative, multi-institutional projects, it is recommended that all parties sign data ownership agreements prior to the commencement of the research project.
   c. If research data are collected from third parties, FGB researchers must ensure they have permission from the owners to use these data.

4. Researchers are responsible for determining which documents (e.g. data management plans, data protection impact assessments (DPIA), data classifications) must be completed for their research project and for the completion of these documents
   a. The completion of documents may be delegated, but senior researchers (project leaders, project co-ordinators and, where applicable, department heads) are ultimately responsible for the content of these documents.
   b. All researchers and research assistants involved in a project should review and comply with the research data management plan. Researchers should involve experts (1. data managers for the project, 2. the research data officer for the FGB, 3. University Library RDM experts) in writing the data management plan to provide expert advice and to help identify potential problems and possible solutions prior to commencement of the project.
   c. Researchers should update documents as needed, as well as maintaining project-specific metadata (e.g. lab notes, codes and descriptions of data manipulations and analyses, and codebooks) throughout the research lifecycle.
   d. Researchers should instil good documentation and data management practices in any students or interns under their supervision[1], particularly when the research conducted by these students is used for publications and/or future research projects.

[1] See SOPs for “Safe Transfer of Data Outside of the VU” and “Safe Practices for Students Working with Personal Data” in annex 2 for more information.

5. Researchers are expected to determine the appropriate facilities, systems and tools for effective research data management, seeking advice from ITVO, TO3 and the research data officer as required.

6. Researchers are expected to seek advice regarding the ethics and scientific integrity of their research. They are responsible for determining if the project must be approved by the METc, CCMO or an external body as required by their research funder. If none of these conditions apply, researchers are strongly advised to submit their research proposals for ethical review by the Scientific and Ethical Review Board (VCWE), while recognizing that the VCWE cannot be held accountable for the researchers' ethical conduct[2].

7. Research data must be archived according the local FGB implementation of the DSW National Guidelines on Archiving[3].
    a. Researchers are required to make their archived and/or published datasets findable by other researchers; it is recommended to utilize VU UB services, such as PURE, for this purpose.

Department heads

8. Department heads[4] are ultimately responsible for the data collected by researchers in their department. In addition to managing research data when researchers terminate their employment at the VU:
    a. Departments heads will represent the "data owner" in documentation where a specific individual must be named, such as on data classification forms;
    b. Department heads are responsible for maintaining reading rights to all archived research data within their department;

Faculty board

9. The board will require teaching FAIR data management principles in the bachelor, masters, and graduate level curricula.
    a. For further information on this topic, contact Marleen de Moor, FGB Coordinator Methods-Curriculum Bachelor Programmes Psychology and Education.

10. The board will assess and ensure the compatibility between the RDM policies of the faculty and the interdisciplinary institutes.

11. The faculty board will report to the university board about the RDM policy for the FGB.

12. The board will appoint a research data officer who will:

[2] The local implementation of the "Code of Ethics for Research in the Social and Behavioural Sciences Involving Human Participants" outlines the ethical standards expected of every FGB researcher.
[3] Detailed information on the requirements for data archiving within the FGB can be found via the VCWE webpage in the "Guidelines for Archiving of Academic Research for Faculties of Behavioural and Social Sciences-Local Implementation". For research projects conducted by an interdisciplinary research institute, the institute may have separate guidelines on archiving data.
[4] In this section, the responsibilities of a department head are tied to the position of department head, not the individual. When one individual steps down from this role, the new individual takes over the responsibilities of his or her predecessor.

a. Develop and maintain a library of tools, guidelines, protocols and courses that help FGB researchers to comply with good RDM practices and to promote the achievement of the FAIR data principles;
b. Provide advice to FGB staff about RDM and privacy issues, as required;
c. Conduct internal audits to monitor compliance with this RDM policy;
d. Maintain a registry of data processing activities which is required by the GDPR for every research project.

Faculty director

13. The director will ensure the proper functioning, security, and reliability of FGB facilities for data storage and management.

14. The director will sign contractual agreements with third parties, such as processing agreements with data processors, data sharing agreements and so forth, on behalf of the Stichting VU.

Inter-faculty institutes

15. For institutions that span multiple faculties, a separate RDM policy may be created, while still acknowledging the spirit of the policies from the respective faculties. Any major conflicts in RDM policy between faculties can be discussed with the research data officers or data stewards from the respective faculties and with the University Library RDM experts to determine an appropriate compromise.

Procedures

1. This RDM policy takes effect as of February 1, 2019. All responsible parties are expected, at this time, to be aware of their tasks and to have reviewed any applicable documents.

2. The data archiving requirements will be phased in over the course of 2019[3]. The FAIR data practices will be introduced in 2019 and their application to research activities is strongly recommended, but not an absolute requirement. Reassessment will take place in the fall of 2019 and will be included in the FGB annual report for 2019.

3. Research institutes will report annually on their activities to support data management.

Facilities and Support

1. The FGB provides access to mass storage with backups within the VU network. Expansion needs will be yearly evaluated.
    a. IT for Research (itvo.ucit@vu.nl) can be contacted for more complex storage requirements or if high performance computing is required.
    b. IT for Research also assists researchers in meeting data security obligations by helping to determine the most appropriate and secure storage solutions for their data.
    c. The FGB, in collaboration with the other faculties, will work to improve upon existing mass storage options to create solutions specific to the types of data created within

the FGB that also meet the research requirements of FGB researchers. A particular focus will be given to extremely large data files, for example, fMRI data.

2. The technicians from TO3 provide technical support to researchers. They manage and develop equipment, devices, software and hardware that are necessary for high quality research within the FGB. Tasks include developing apps and web forms, providing support with online questionnaires, developing innovative research solutions such as wifi-linked accelerometry or non-invasive stress measurements, and providing technical support in a variety of laboratory settings, ranging from human movement and psychological experiments to animal- and cell-based research.
    a. Researchers requiring technical support should contact the TO3 technicians as early as possible in their project planning.

3. The research data officer for the FGB can be contacted (research.data.fgb@vu.nl) for questions about research data management, privacy issues and the FAIR data principles
    a. The research data officer/Privacy Champion is the first point of contact for advice on research data management and privacy issues within the FGB; this advice will assist FGB staff in meeting their data management and privacy obligations. In most cases, official approvals are not required for these obligations; self-monitoring is sufficient. Where an official approval is required, the research data officer will facilitate this process by helping FGB researchers determine from whom this official approval can be obtained.

4. Lawyers from IXA (info@ixa.nl) can be contacted to draw up consortium agreements for data sharing (if the standard VU model does not meet researchers' requirements) and data ownership agreements when working with parties external to the VU. See the IXA webpage for more information on the types of agreements that IXA can help with.

Annex 1. FGB Policy Positions on the GDPR

1. Directly identifying personal data (name, address, contact information) may be maintained for the entire duration of a research project if this information is required to carry out the project. For example, it may be necessary to: contact individuals about the next phase of the project; contact participants for a follow-up project, if they have given consent to be contacted; or for communications with participants' caregivers or teachers who may need to provide supplementary information about participant, but who should not know the ID codes of the participants. Directly identifying personal data should be stored separately from other research data, at a higher level of security than indirectly identifying information and they should only be accessible to those individuals (usually research assistants and data managers) who absolutely require access.
    a. Details on archiving directly identifying personal data can be found in the local FGB implementation of the DSW National Guidelines on Archiving[3].

2. The fundamental legal basis for conducting a research project using personal data should, in the majority of cases, be the informed and freely given consent of participants. Legitimate interests can be invoked as an alternative legal basis for conducting a research project using personal data if obtaining informed and freely given consent is impossible or would impair the aims of the project. In order to use legitimate interests as a legal ground for conducting a research project, the benefits of the research project must outweigh the rights of the individuals. FGB researchers who wish to invoke legitimate interests as a legal basis for their research project must complete a Legitimate Interests Assessment prior to commencement. Additional conditions are also required if special categories of personal data will be processed on the basis of legitimate interests (see Rule 5 from Privacy in Scientific Research – 10 Key Rules). Situations where legitimate interests may be more appropriate than obtaining consent include, but are not limited to:
    a. Child abuse (cannot ethically inform the parents, but the child is <16 years old)
    b. Youth crime (cannot ethically inform the parents, but the child is <16 years old)
    c. Misconduct in public organizations/the church/social support (cannot inform the individuals responsible for misconduct without risking harm to other individuals and to the aims of the research project)
    d. Historical research where it is no longer possible to contact the data subjects

    This is not an exhaustive list. There are many cases where legitimate interests may be an appropriate legal ground for conducting a research project; advice on this matter should be sought from the VCWE, the research data officer and, when necessary, the VU data protection officer. **NOTE**: legitimate interests CANNOT be used as grounds to conduct clinical research that falls under the purview of the Good Clinical Practice Guidelines and/or the WMO; informed and explicit consent is a requirement for these types of research, except in the extreme case of emergencies (WMO Article 6.4 and ICH-GCP E6/R2 Addendum 4.8.15).

3. The FGB will work together with the VU and the National Coordination Point for RDM to determine how best to manage publication of FAIR datasets that fall under the purview of the GDPR. While a comprehensive solution is developed, researchers wishing to or who must publish research data which cannot be fully anonymized must obtain consent for this publication from study participants during the informed consent process. For research

projects that have already started, but for which consent to data publication was not obtained during the informed consent process, as well as any other questions about this topic, refer to the research data officer.

4. If research data, that fall under the purview of the GDPR, were obtained from a third party, such as a public repository, and it would require excessive effort to determine who the study participants were and what their current contact information is, then it is not necessary to contact these individuals regarding the new usage of their data. However, if researchers have a method of passively informing individuals about the reuse of research data, such as a study website or a twitter feed, then the researchers should post an information letter, containing the requirements described in Article 14 of the GDPR, about this new usage. Researchers are also expected to appropriately cite the data used in their publication.
    a. Advice on this topic can be sought from the research data officer. The research data officer will also develop templates for the information letter described above.

5. A research project is exempt from the GDPR's right to be forgotten if data erasure "renders impossible or seriously impairs the achievement of the objectives". If a study participant wishes to exercise this right, but the study is already in the analysis phase or later, researchers may refuse this right: once data have been analysed, published and/or archived, the data can no longer be deleted without severely impairing the aims of the research. Requests for the right to be forgotten must always be forwarded to the Data Protection Officer for the VU, who will lead the communications between the requesting participant and the researchers.
    a. If a participant revokes consent to a research project, the usage of the data already collected depends on the nature of the research project and the phase of the research cycle. If a research project consists of repeated measurements and a participant revokes consent by saying that they no longer wish to be contacted or to take part in the study, all of the data collected up until that point may still be used, unless the individual exercises the right to be forgotten and the erasure of the data is not detrimental to the aims of the research project. If a participant revokes consent to the entirety of the research project, without invoking the right to be forgotten, and the research project is still in the data collection phase, the data do not need to be deleted, but they may not be used for analysis; if the research project is in the analysis phase or later when the participant revokes consent to the entirety of the research project, the data cannot be deleted; these data however should be flagged as not to be used for any follow-up research projects.

6. Any requests from a research participant for the GDPR's right to data portability[5] will be reviewed on a case-by-case basis with the VU Data Protection Officer. Such requests are not expected to occur very often, and as such, researchers are **NOT** required to prepare for any such requests (i.e. by ensuring that the data in question are machine-readable). Researchers are not obliged to execute requests for data portability if this would risk the privacy of other

[5] There are limitations to the right to data portability. It can only be exercised if the legal basis for processing was consent or for the performance of a contract, and only if the data are digital. The data must have been directly obtained from the subject and not further manipulated (therefore a depression score would not apply, whereas an MRI would). The data provided must be in a machine-readable format, such as XML, JSON etc. The research data officer and TO3 can assist in making machine-readable documents.

individuals or severely harm the aims of the research project, but, ultimately, the decision to approve a request for data portability lies with the Data Protection Officer for the VU.

7. Long-term research projects should occasionally update consent. This should be done if there are any fundamental changes to the nature of the study, such as a change to the purpose of the study, the types of data collected, or any planned data sharing that was not mentioned earlier. Researchers should also review their consent forms every ten years to see if consent needs to be refreshed.
    a. Consent forms from long-term research projects that started prior to the implementation of the GDPR should be reviewed for compliance with the GDPR. If found to be non-compliant, researchers must attempt to refresh participant consent. If it is not possible to obtain refreshed consent from all participants, data may continue to be used based on the original consent, but an updated information form about the changes to consent and participant rights should be made public, such as on a study website, so that the individuals who could not be contacted can find such information and can contact the researchers if necessary.

8. Researchers are expected to assess the need for a data protection impact assessment (DPIA)[6] and when advice on a completed DPIA must be sought. Within the FGB, the research data officer will provide initial advice on DPIAs; if the issues are very complex, the research data officer will forward the issues to the Data Protection Officer for the VU.
    a. DPIAs should be occasionally refreshed for long-term research projects. For cohort studies with discreet collection phases, DPIAs should be conducted prior to each new collection phase if 5 years have elapsed since the last collection phase. Long-term registries, that are continuously collecting data, should conduct a new DPIA at least every 5 to 10 years. Any research project that previously required a DPIA must complete a new DPIA if there are fundamental changes to the project, such as new purposes, new methods of data collection or new technologies being utilized for data collection and analysis.

9. Non-digital personal data (such as saliva samples or written documents) must be protected from theft, loss, damage and unauthorized access, just like any other personal data. Safe transport of non-digital data is described in the SOP for transporting personal data[1].

[6] The Dutch Personal Data Authority has created a checklist (in Dutch) for when a DPIA must be completed. Details on when a DPIA must be carried out can also be found on this page under the section "Vragen over DPIA". Ultimately, most research projects will need to complete a DPIA. Some helpful models for completing a DPIA are available from the Dutch Government (only available in Dutch), as well as the Data Protection Authorities for France and the UK (both available in English). For further information, contact the FGB research data officer.

Annex 2. Standard Operating Procedures

SOP: Safe Practices for Students Working with Research Data

SOP: Safe Data Use Outside of the VU

Annex 3: Supplementary Documentation

General Data Protection Regulation: Take Home Points for FGB Researchers

Links for the Labyrinth: Where to Find the Information You Need

Reference Material

FGB implementation of the "Guidelines for Archiving of Academic Research for Faculties of Behavioural and Social Sciences" (2019)

Research Data Management Policy of the VU Amsterdam (expected 2019, version from 2016 can be found on VUnet)

VSNU Code of Conduct for Research Integrity (2018)

VSNU Code of Conduct on the Using Personal Data in Scientific Research (2005; new version expected in 2019)

Standard Evaluation Protocol (SEP 2015-2021)

General Data Protection Regulation (2018)

The Dutch national implementation of the GDPR (UAVG, in Dutch only; 2018)

Federa Code of Conduct for Responsible Use of Human Tissue in Medical Research (2011)

Federa Code of Conduct for the Use of Data in Health Research (2003)

ICH Good Clinical Practice Guidelines (2016)

Medical Research with Humans Act (WMO; 1998)

Medical Treatment Agreement Act (WGBO)