Research Data Management policy
Faculty of Social Sciences

Reader's guide

This memorandum describes the data management policy of the Faculty of Social Sciences (FSW) at Vrije Universiteit Amsterdam (VU). It provides a practical and specific application of the more general policy framework and guidelines that apply, such as the VU policy memo on "Research Data Management" (1), the VSNU's Netherlands Code of Conduct on Scientific Practice (2), the Standard Evaluation Protocol (SEP 2015-2021) (3), and the General Data Protection Regulation (GDPR) and the Dutch equivalents AVG and UAVG (8). This memorandum should be read as an extension of these guidelines, considering that these more general policy frameworks and guidelines apply in full to FSW research.

The policy memorandum begins with the objectives of the data management policy, followed by an in-depth discussion of a number of key principles (section 1). The faculty policy framework is then discussed in section 2, with a strong focus on the role of an appropriate Data Management Plan. Supplementary to section 2, section 3 and 4 provide instructions for saving and archiving data. Finally, section 5 outlines the wider context in which policy and monitoring are organized with regard to data management and section 6 ends with a hardship clause.

This memo applies to all FSW research from 1 January 2018 onwards and applies, in principle, to all researchers holding a position at the Faculty of Social Sciences, unless they are conducting research as part of a research collaboration whose lead agency is located elsewhere and provided the partner organization has an appropriate data management policy. The policy applies equally to research conducted by students in the context of their study programme if, and to the extent that, a) FSW researchers are involved in the research (as lecturers); or b) that the research results culminate in one or more external publications; or c) that the intention is to reuse the collected or processed data for research purposes. For student research (for Bachelor's or Master's theses, for example) to which none of the above conditions apply, separate rules will be drawn up in addition to this memorandum. Until then, the policy outlined below serves as a guideline and it is up to the lecturer involved to ensure that the principles of diligence and traceability are adhered to.

1. Objective, basic principles and variety of data

Data is essential in socio-scientific research. To the extent that conclusions in socio-scientific research rely on data, this data must be ***diligently collected*** and must be ***traceable*** for those who wish to verify these conclusions. All data also has an important ***documentation function***: data that is collected in the present can prove to be of great value to future research (provided the data has been carefully managed and documented). The purpose of the FSW's data management policy is therefore to encourage and facilitate its researchers to systematically and carefully collect, manage and archive their data and ensure that they adhere to the three principles of data management highlighted above: diligent collection, traceability and documentation.

More specifically, this policy memo aims to:

1) raise awareness of the importance of managing research data;
2) draw up faculty-specific rules and guidelines for handling research data to:
    a. demonstrate the academic integrity of FSW researchers;
    b. show that FSW research complies with the legal requirements, codes of conduct and statutory requirements of external bodies (including grant providers and journals) regarding the management of research data;
    c. ensure that reuse of research data within the faculty is facilitated as efficiently as possible.
3) clarify the responsibilities of FSW researchers, department heads and the faculty board with regard to research data;
4) clarify and organize the available facilities for the management of research data.

The principle of ***traceability*** requires excellent documentation and researchers to make every effort to demonstrate the authenticity of research data. Depending on the type of data and the type of research, this can be done by collecting participants' digital informed consent forms and/or signatures (hardcopy), and documenting them, or by recording audio and/or video clips and including or systematically documenting locations and dates of fieldwork, and/or conducting the research activities or editing the data in the presence of or with the knowledge of other researchers.

A vital aspect of ***diligent*** data collection is the constant consideration of the interests of respondents and the ***protection of respondents' rights***. In particular, this requires that:

- appropriate measures are taken for the storage of data associated with the classification of the relevant data (in terms of public, confidential or highly confidential) (21);
- taking full and consistent account of the privacy aspects and the legal requirements for the storage of personal data (23).

Proper ***documentation*** requires that data management takes place at every stage of the research process and is not limited to the original data files and Data Management Plan. The purpose of this is to provide transparency and, where possible, make data accessible for others as well as all relevant instruments used for collecting, entering, saving, using, analysing, reporting and archiving the data. Transparency and accessibility are especially important when quantitative data is used, for the purpose of data citation and – where possible – to facilitate the reuse of data (2). Whereas for most quantitative data projects the value of replication can be given priority, provided the anonymity of the data is guaranteed, in the case of observational data the protection of research subjects will often take precedence. It is essential for researchers to carefully justify their documentation procedures and the way they have handled potential trade-offs between replicability and the protection of research subjects in their data management plan.

In socio-scientific research a large variety of data is used. Different types of data come with different requirements for the use and management of the relevant data. In its broadest sense we take ***research data*** to mean all observational data recorded in the research process that serves as input for research publications. Within the Faculty of Social Sciences we can distinguish at least the following types of data:

- *quantitative data*, obtained from, for example, surveys, experiments or automatized text analysis, which are –generally – not personal or can be anonymized relatively easily according to well-established procedures;
- *observational data,* for example field notes or photo, film or audio material used to capture research activities in the field; this data that is inextricably linked to the context, visibility and identity of the subjects;
- *qualitative interview data* (reports and/or recordings), whose prime value lies in the substance of the text and whose value at least in part derives from the status of the respondent (e.g. expert or political decision-maker) , and for the use of which consent has to be given, often in the form of an informed consent form;
- *dynamic and large-scale data,* for example gathered by *scraping* websites and social media and/or by linking different data, is usually time-bound due to the fact that the underlying data sources are dynamic in nature.

Although these types of research data are extremely different, the various principles – a) diligent data collection b) traceability and c) the best possible documentation – apply to all types, even if these principles may be interpreted in different ways and may require varying considerations. Exactly these considerations need to be documented and explicated in the data management plan.

2. Management of data prior to the research: The Data Management Plan

To ensure that data is a) collected diligently, b) traceable, and c) documented as well as possible for future research, researchers are expected to draw up and manage a ***data management plan***. When a project leader has clearly been named (such as in the case of a project with indirect funding or contract-based funding) the project leader carries final responsibility. In other cases when researchers or institutions are cooperating, the researchers involved will be jointly responsible for drawing up a data management plan. In this way FSW's policy is similar to that of the Netherlands Organization for Scientific Research (NWO) (4) and the European Research Council (5), and shows overlap with the policy of numerous scientific journals (16) (17) (18).

Drawing up a new data management plan or a supplement to an existing data management plan is ***necessary*** in the event that:

- new data (either quantitative or qualitative) is collected, or
- original analyses are being conducted on third-parties' primary data (containing personal or sensitive information).

The first version of the data management plan is drawn up at the same time that the decision is made to collect data or acquire data, and before this decision is carried out. In long-term research projects with multiple lines of research, researchers themselves have to assess to what degree new research lines, with new data, can still be accommodated in the existing data management plan or whether it might be preferable to draw up a new data management plan (with a reference to the previous one).

At the various stages of the research process, additions and updates are made to the data management plan. These updates serve to clearly document all considerations and steps taken during research, including: how data was collected, whether transcription was used, whether data

was selected and how, who has access to which file, etc. This means that the edited/cleaned files, progress reports, lab journals, important emails and other documents with agreements reached or decisions made must be documented and saved using preferential file formats and a clear directory structure, preferably with version numbers. All things considered, a data management plan is a living document designed for a specific context, depending on the research method and the type of data involved. Depending on the nature of the project, the scope of the data management plan can vary from very brief to very extensive.

Every data management plan has to be saved in the right files on the G drive and be accessible to the department head and all researchers who need to access these files for research purposes.

In drawing up a data management plan, the Faculty of Social Sciences advises the use of the ***DANS template*** (see appendix) unless a research funder or a journal places other demands on research or data management. The DANS template's advantage is that it is relatively compact but does allow for a discussion of the most important issues. DANS also provides a generally accepted standard. However, DANS is mainly intended for digital quantitative data. Researchers working with other types of data will notice that certain questions do not apply or require a rather broad interpretation. At the same time, researchers can add or delete questions/elements to the template where relevant to the context of the study. Other templates may provide the necessary inspiration; they can be found in the VU Libguides and/or on VUnet. For advice and questions on drawing up a data management plan, please contact the VU's *data librarian*.

Ethical review

All data management plans are subject to ethical review or self-assessment. The first, necessary step in the faculty's ethical review process is for researchers to perform a ***self-assessment*** to determine if their research should be subject to ethical review by the faculty's Ethics Committee (EC). If the self-assessment shows that it is not necessary to submit a request for review by the EC of the Faculty of Social Sciences, then this means that the data management plan does not have to be submitted for review either. Should the self-assessment show that the research must be reviewed by the EC, then researchers must obtain approval in writing before commencing data collection. The approval form is then attached to the data management plan.

Use and ownership of research data

Unless specified otherwise in the data management plan, the Faculty of Social Sciences' guiding principle is that all research data managed within the Faculty may be used exclusively by researchers associated with the Faculty. Researchers are free to deviate from this only if the agreements are clearly discussed in the data management plan or in other relevant documents (like cooperation agreements or consortium agreements) and include a short motivation as well as explicit and specific agreements regarding the use of research data by third parties. It is also necessary to include specific agreements in the data management plan in the event that researchers terminate their employment but will still require access to data managed by the faculty (19).

Ownership of newly acquired research data is subject to intellectual property laws - (Copyright Act, Patents Act, Databases Act); Articles 1.20-1.23 of the Collective Labour Agreement for Dutch universities; and the *Knowledge, Intellectual Property and VU and VUmc participation* regulations - unless otherwise agreed with funding bodies or research funders (1). Ownership agreements have to be concluded in writing and must be drawn up and signed by all the parties involved prior to the start of the research project. These agreements usually take the form of cooperation agreements and/or consortium agreements. Researchers are required to consult lawyers from IXA or the VU

Grants Desk for assistance in drawing up agreements and documents or reviewing the proposed agreements.

If researchers are looking to use research data obtained from third parties, the researcher must, insofar as the data has not been made public, request permission from the rightful owner to use the data and include the origin and type of the data in the data management plan.

Finances
Data storage and archiving may entail special expenses that must be included in the budget for specific projects or departments. The Faculty of Social Sciences takes a pragmatic approach to data storage and archiving. FSW applies the current faculty payment arrangements for data storage, which state that costs will only be charged to departments or projects if there are specific circumstances/requests. For data archiving, the cost structure as used by the VU University Library applies (for 50GB and more, the costs will be charged to the project or department, anything below 50GB is charged to the faculty).

Privacy aspects, personal data and sensitive information
All FSW researchers must respect the privacy of others and comply with the legal requirements as stated in the General Data Protection Regulations (GDPR) / Algemene Verordening Gegevensbescherming (AVG) and implementing law (UAVG) (8). When aspects of privacy are involved, researchers have to do the following before they begin:

- familiarize themselves with possible privacy-sensitive data that has been required and/or will be used in research, and make sure access to the data is limited to individuals with clearance;
- sign a confidentiality agreement and ensure everyone else who has access to the data signs it. The agreement must also be uploaded to the G-drive before the start of the research;
- include a detailed description in the data management plan and, if applicable, explain how privacy-sensitive information/data during and after the study has been handled.

If personal data are involved, or special personal data such as race, religion or health, then the researcher will have to do the following prior to the start of the research:

- make sure he or she is aware of the terms and conditions outlined in the Algemene Verordening Gegevensbescherming (AVG). See the website for the Dutch Data Protection Authority (Dutch DPA) for more information;
- report the study to VU Amsterdam's central data processing centre by sending an email to the data protection officer: servicedesk.privacy@vu.nl .

For more information or advice on privacy issues and on handling privacy-sensitive data during research activities, please contact the legal advisors of Vrije Universiteit Amsterdam or the FSW Privacy champions. They can also draw up a Privacy Impact Assessment to see which risks may be associated with your research.

3. Management and storage of data during research

Newly acquired digital data is usually stored and managed on the university's G-drive or on Surfdrive. If VU Amsterdam's G-drive or Surfdrive is not sufficient, due to the type or size of the data, then the researcher will need to choose another data storage facility. Researchers are free to choose another data storage facility as long as it meets the legal requirements for research data storage and as long as the data is guaranteed to be stored safely and securely, in a well-structured manner, for the duration of the study. This choice has to be accounted for in the data management plan.

If newly acquired ***research data*** is (initially) collected ***on paper***, then this data and a proper description of the data must be safely stored at Vrije Universiteit Amsterdam as well. This can be done in one of the following ways: by scanning source files and saving them in a digital format and locking them, and/or by storing the original source documents in a fireproof place, safely under lock and key.

When ***secondary data*** is used for original analyses, then storing the data itself is only necessary if the data cannot be obtained again (or has to be purchased again). Exceptions include what is known as 'big data' or 'volatile data' (for example, data obtained through social media), where archiving data is not advisable or feasible considering the size of the data and/or the speed with which the data changes. If this type of data is used, the data management plan should always include an explanation of the origins of the data or where it could be found at the time in the current format.

For advice and questions on management and storage of data during research, please contact the University data librarians or University information security officers . In the event of a data breach, for example due to theft, hacked computer systems or the loss of data carriers such as USB stick, hard disks, computers or paper data, the researcher must report this to the department head and the VU IT Servicedesk immediately if privacy-sensitive information is concerned.

Specific guidelines for collecting, analysing and storing of special personal data
Gathering and analysing sensitive personal data is allowed under the AVG/UAVG provided that this data is explicitly used for research purposes and has been obtained with the express consent of the person involved. Exceptions to this provision are possible if it is impossible to apply given the particular nature of the study (for example when studying aspects of spontaneous group processes which are not to be distorted by the awareness of the research) or if its application would require disproportionate effort. In these cases, the researcher only records the origins of the data. For experimental research with participants, it is essential that researchers, in addition to actively obtaining permission for the collection and analysis of data, also offer participants the option to withdraw from the research at any stage. Both the consent forms and any possible requests for withdrawal from the study must be stored in the same place as the research data. In the event that any personal data and other personal information has been obtained that is strictly *off the record*, then the researcher will be required to document any expectations connected to this information and take great care in handling the information.

In principle, saving sensitive personal data is technically allowed for the duration of the study, and in specific situations, for longer periods of time. The above mentioned principles and guidelines on how to handle these data also apply in this case. However, for data protection purposes, saving these type of data on unsecured data storage devices or synchronized cloud services such as Dropbox and Google Drive is strictly prohibited and additional security measures will have to be taken before the data can be stored. These steps include encryption of data, anonymizing data and storing the processed data separately from the raw research data. This in preparation of the data archiving phase, where this is compulsory (also see VU Amsterdam's guideline for working with personal data in research. For questions and advice on storing sensitive data, please contact the University information security officers.

Specific guidelines for the storage of large data sets
For the storage of research data over 100GB, researchers can use SciStor, a paid VU Amsterdam service, and/or submit a request for their own database at the IT department. Vrije Universiteit Amsterdam has no standard facilities for the storage of big data. Researchers are therefore asked to start by using the storage facilities commonly used within the research disciple and inform the

faculty's research office on this so the faculty can formulate a clearer policy on this matter in the future and/or reach agreements with the university.

4. Archiving and sharing data after conclusion of the study

Research data must be properly archived *after* a study has been concluded to ensure that the data remains available for future studies in comparable fields or research areas and if other researchers wish to replicate parts of the research (if possible) (2). When data is stored in a diligent and traceable way during the research process, safe and accessible archiving becomes easier. Important next steps include choosing the right archive, or data repository, and safeguarding the quality of the archiving system.

There are three different moments in time when the researcher will need to archive data (24):

1. when an article that is based on a dataset is published;
2. no later than three months after completion of a study;
3. if a researcher has completed the data analysis and the data is static, the researcher may want to safely store this data for the time being.

The objective of archiving data is to keep it available for future research for an unspecified period of time, independent of the formal minimum retention period of 10 years (24).

Researchers are required to archive their research data in at least one place. Key considerations in choosing an archive location are whether the data is analogue or digital and whether or not it is confidential. Depending on the confidentiality of the data, stricter requirements may apply to the accessibility of the archiving location. Other considerations that play a role in choosing the archiving location are the size of the data files (small vs. large), ownership (self-acquired data vs. reuse of existing data), and the terms and conditions (including usage and rights) as stated by research funders. The final choice for a *data repository* is always documented in the data management plan and shared with everyone who needs access to it, for research purposes or for quality control of the project.

For digital data, it is preferable to use the ***digital repositories*** offered by VU Amsterdam, also because they allow you to link data files to the VU Research Portal (PURE), thus simplifying the option of citing data. If the VU repositories do not meet your requirements, then it is possible to archive the data elsewhere, as long as:

- the location complies with the rules and legal requirements for archiving research data (determined by the research funder or others);
- it can be guaranteed that the data can be stored safely and securely for a period of at least 10 years (24) and agreements on data are drawn up and recorded (via licensing and processing agreements) with the organization behind the *data repository;*
- This choice is accounted for in the data management plan and documented on FSW-VU Amsterdam's G-drive.

For the archiving of ***analogue research data***, VU Amsterdam does not have standard facilities at this moment. The responsibility for keeping privacy-sensitive data safe from fire and theft lies primarily with the researcher. He or she is also responsible for the careful documentation of the archiving procedure and for including a justification of this method in the data management plan. If desired, researchers can consult with the UBVU data librarians to see if the VU archives can be used.

If a *data repository* is chosen where the data is not publicly accessible, then the additional decisions need to be made within the research team about the use of research data after it has been archived

(19). If this is not already be done, then these agreements will be added to the data management plan.

Besides the choice of an appropriate archiving location, it is essential to safeguard the ***quality*** of the archiving process. This means that:

- agreements on archiving (such as the retention period (24)) are drawn up and agreed in the data management plan, including steps taken and motivations of decisions made, and shared with the whole research team;
- a researcher has to get at least one fellow colleague's opinion before he or she actually archives the data;
- before the data is archived, the format has to be as close to the DANS preferential file formats as possible (22) so the ten year retention period can be guaranteed.

For advice and questions about archiving research data, please contact the UBVU data librarians.

Specific guidelines for archiving sensitive personal data

Sensitive personal data is not archived unless necessary for scientific, historic or statistical purposes (see also VU Amsterdam's guideline for working with personal data in research). Separating personal data from raw research data is mandatory, and if you have not already done so during the research process, please ensure that they are archived separately. In cases where this is not possible and source files have not been anonymized and are traceable to individuals, research data may only be shared under very strict conditions. Ideally, in such cases, only the original transcription and the eventual edited files should be made accessible. Personal data (name, email address or address and telephone number) may be collected and saved for communication purposes as long as the files containing this information are encrypted and saved to the G drive. For questions and advice on storing sensitive data, please contact VU Amsterdam's information security officer.

Data citation in publications

In order to promote the scientific quality and integrity and the verifiability of research, it is increasingly important to cite data in publications. In view of the developments in this area and the expectation that the need for data citation will only increase (partly as a result of the fact that increasingly stringent conditions are applied by research funders and scientific journals), FSW advises its researchers to diligently cite data. For questions and advice about this, contact the UBVU data librarians and/or go to websites such as www.datacite.org

5. Monitoring and implementation of the policy

The researchers themselves bear primary responsibility for research data management. The Faculty of Social Sciences data management policy states that ***all researchers*** are equally responsible for proper data management and hold themselves and each other accountable, for example in situations where colleagues have been careless with data or have made mistakes handling data files and/or sensitive personal data during or after the study. In the event that the above does not lead to improvements, the department head should be informed. The department head can then take action and speak with the relevant researcher or the faculty board. Should you suspect misconduct or mishandling of research data (for example manipulation of research data or the creation of research data) by fellow researchers, then the faculty can refer you to a confidential counsellor for academic integrity (VP WI) or the FSW PhD Trustee where employees can discuss their experiences and VU Amsterdam's procedures for reporting and investigation possible violations.

In accordance with the VU Directive (1), researchers are responsible for:

- compliance with legal and ethical requirements regarding their research data, including the assessment by ethics committees if necessary;
- their research data and the fact that it is reliable and traceable during the *data life cycle* and that it has been stored properly;
- archiving their research data for at least ten years after publication, unless otherwise prescribed by law;
- sharing their research data for scientific purposes and for verification unless legal provisions prohibit that;
- reporting research to the Data Protection Officer (FG) of VU Amsterdam (servicedesk.privacy@vu.nl) if they collect and process personal data in their research. This is a legal obligation (imposed by the AVG).

Here the Faculty of Social Sciences, based on a recommendation by the Royal Academy of Arts and Sciences (*KNAW*) (12), adds that the researchers are expected to:

- maintain a data management plan for those data that require this.
- communicate the faculty-specific rules and guidelines with regard to this theme informally during research projects and the supervision of students, employees or new hires, which includes creating an open atmosphere with plenty of room to discuss mistakes and dilemmas.
- make research data available to other researchers at the faculty by observing the principle of '*as open as possible, but as limited as necessary*'.

Final responsibility for the above-mentioned responsibilities may be assigned to another researcher and/or project leader. However, this does not relieve the researcher of personal responsibility.

While the researchers carry primary responsibility for data management, this responsibility is part of the core responsibilities of the Faculty of Social Sciences as a whole (also see the recommendations of the Netherlands Academy of Arts and Sciences, KNAW (12)). The department heads and the Faculty Board also have a clear responsibility in enforcing this policy, which is further clarified below.

The ***head of department*** ensures department compliance with the rules and guidelines as set out in this memorandum. The department head is responsible for promoting a culture in which researchers take personal responsibility. He or she leads by example, inspiring others to adopt the department's scientific attitude and comply with research ethics standards and openly discuss best practices for data management. The department head is also responsible for developing additional research data management policies that are in keeping with the field's research characteristics. Data management should be an important theme in the annual interview of researchers who collect and/or process large amounts of data, which should also clearly be reflected in the annual performance assessment report.
The head of department bears a special responsibility for reaching agreements with researchers about their research data in the event that they leave the university.
Finally, the department head is responsible for supplying information to the faculty board, external review committees and/or third parties about the evaluation of the management of research data, including data storage practices and verification practices.
The department head's responsibilities may be delegated to other members of staff such as the research manager, but the department head always bears final responsibility.

The ***faculty board*** monitors the implementation of and compliance with the policy during administrative consultations with the departments and reports to the University Board. Based on its

experiences, the faculty will also evaluate the policy and makes adjustments where necessary. The faculty board will continue to keep the subject of data management alive in the faculty and to keep it on the policy agenda. The board also steps in when serious incidents occur. The faculty board also sees to it that the basic facilities (data repositories, G-drive capacity, access to Surfdrive etc.) and services (provided by University Library and the IT-Servicedesk) are fully operational, reliable and accessible to faculty researchers; allowing them to fully comply with the responsibilities laid down in the data management policy.
In the event that the facilities do not or not adequately meet the specific needs of faculty researchers, then their academic departments are responsible for providing them with any facilities, resources and support they deem necessary. The faculty's research office is also available for assistance. If the required support cannot be offered and/or if an FSW-wide provision has to be made available, then the faculty board will decide how and under which conditions to facilitate this request.

6. Hardship clause

If researchers and/or departments expressly wish to deviate from the rules and guidelines of the faculty policy, then the faculty board will take a position on this subject, if necessary on the advice of its academic review committee and/or ethics committee, and approve or reject the request.

Sources and references

Key policies

(1) Vrije Universiteit Amsterdam (2016) Research Data Management Policy, 12-01-2016. http://libguides.vu.nl/ld.php?content_id=32045526

(2) VSNU (2018), Dutch Code of Conduct VSNU Scienctific Research: http://www.vsnu.nl/files/documents/Netherlands%20Code%20of%20Conduct%20for%20Research%20Integrity%202018.pdf

(3) Standard Evaluation Protocol (SEP) 2015-2021: http://www.vsnu.nl/files/documenten/Domeinen/Onderzoek/SEP2015-2021.pdf

(4) NWO Data Management Protocol: http://www.nwo.nl/beleid/open+science/datamanagement

(5) European Research Council & Open Access https://erc.europa.eu/funding-and-grants/managing-project/open-access

(6) DSW (2018), Code of ethics for research in social and behavioural sciences involving human participants: http://www.nethics.nl/Gedragscode-Ethical-Code/

(7) DSW (2018) Guideline for archiving scientific research https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjb-9ib_ODfAhVEKlAKHZpyBMoQFjAAegQIBhAC&url=https%3A%2F%2Fwww.ru.nl%2Fpublish%2Fpages%2F826378%2Fengels_-_richtlijn_archivering_wetenschappelijk_onderzoek_voor_nederlandse_faculteiten_maatschappij-.pdf&usg=AOvVaw1b-Gae7mCEZfq73Mefj6uZ

Relevant laws and regulations:

(8) General Data Protection Regulation/Algemene Verordening Gegevensbescherming:
GDPR: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/gdpr.pdf
AVG: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf
UAVG: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/uavg.pdf

(9) Medical Sciences Research Act (WMO): http://wetten.overheid.nl/BWBR0009408/2015-12-17

(10) Code of Conduct Medical Research: https://www.federa.org/sites/default/files/bijlagen/coreon/gedragscode_gezondheidsonderzoek.pdf

(11) Experiments on Animals Act (Regulations for animal experiments, resolution for experiments on animals): http://wetten.overheid.nl/BWBR0003081/2014-12-18

Policy Memoranda

(12) Royal Netherlands Academy of Arts and Sciences (*KNAW*, 2012), handling scientific research data carefully and with integrity. https://www.knaw.nl/shared/resources/actueel/publicaties/pdf/responsible_research_data_management_and_the_prevention_of_scientific_misconduct.pdf

(13) Basic Memorandum for Academic Integrity at the Faculty of Social Sciences; 2016; Erwin van Rijswoud & Leo Huberts

(14) Data in VU FSS publications in 2013-2014; René Bekkers & Berith van Pelt; 19-07-2016

(15) Protocol for honest research department of Social and Cultural Anthropology, Vrije Universiteit, November 2013. https://fsw.vu.nl/en/Images/Protocol_voor_het_voorkomen_van_fraude_bij_SCA_tcm250-365845.pdf

Regulations for scientific journal publications (selection)

(16) Science
(17) Nature
(18) American Journal of Political Science

Practical instructions from the EMGO + Quality Handbook

(19) 'Folder and file names':
(20) 'Researchers leaving':
(21) 'Classification data for storage and transport':

Other guidelines

(22) DANS explanatory notes for filing data: https://dans.knaw.nl/nl/deponeren/toelichting-data-deponeren
(23) VU University Library guideline for working with personal information for scientific purposes (2014):
(24) VU University Library practical information for archiving your research data (2016):

DANS template for a data management plan

An excellent data management plan provides researchers and everyone involved (including executives, data support providers and research funders) timely insight into the facilities and expertise needed during research activities and after completion of the project. This ensures that research data is reusable after the study is complete – both for the researcher and for others. Open if at all possible; protected if necessary.

This template contains the core elements of a data management plan. DANS is based on information from Dutch and other European research funders and research institutions on *Research Data Management*. The template is transdisciplinary and the concept of 'data' may be interpreted in the broadest sense of the word. You can find more information in the brochure entitled *Data management plan for scientific research*[1].

Please note in advance whether your institution or funder places additional, discipline-specific conditions on a data management plan.

1	**Administrative information**	
1.a	Project name, senior researcher, funder(s), date of this plan and previous versions	
1.b	Who bears primary responsibility for data management?	
2	**Description of the data**	
2.a	Is existing data reused or new data generated?	
2.b	What kind of data is involved? Size of files; growth rate?	
3	**Standards and metadata, or all that is needed to find and utilize the data**	
3.a	Which metadata standards are used (*findability*)?	
3.b	Which encodings, among other things, are used that allow future linking with other data (*identification, interoperability*)?	
3.c	Which software and hardware is used (*identification, usability*)?	
3.d	What is documented and stored to enable replication? What agreements have been reached by the parties involved if anyone terminates	

[1] DANS/CARDS brochure on "Data management plan for scientific research", version 3, 2015, http://dans.knaw.nl/nl/over/organisatie-beleid/informatiemateriaal/dansdatamanagementplannl.pdf

	involvement prematurely?	
4	**Ethical and legal**	
4.a	How will the necessary permission be obtained from the data suppliers / test subjects / ...? What restrictions may apply during the study?	
4.b	How is sensitive data protected during and after the project?	
4.c	Will the data be accessible as Open Access data at the end of the project, possibly after an embargo has been lifted? If not, what are the conditions?	
5	**Storage and archive**	
5.a	How is sufficient storage and backup capability organized during the project, including version management? Are these expenses included, and if not, ...?	
5.b	Where and for how long will the data be made available for follow-up research and verification after the project has ended? Does it concern a Trusted Digital Repository with an international certificate? If it doesn't, how can data be traced (consider metadata, for example, or persistent identifiers such as DOI, Handle and URN), and be made permanently accessible and usable?	
5.c	Are the costs associated with data preparation and archiving covered? If not, what next/by whom...?	