RDM Policy Comparisons

FSW Data Steward

24 October 2023

Contents

General Data Protection Regulation (GDPR)

Date: 2018

Last reviewed: 25/07/2023

URL: https://gdpr-info.eu

GDPR	FSS
Note:	The GDPR is too large to include a full comparion here.

Netherlands Code of Conduct for Research Integrity , Standards for good research practices

Date: Sep-18

Last reviewed: 15/06/2023

URL: https://doi.org/10.17026/dans-2cj-nvwu

Code of Conduct	FSS
9. In research with external partners, make clear written agreements about research integrity and related matters such as intellectual property rights.	FSS guidelines include instructions to do this. The primary contact for FSS researchers about this is IXA-GO.
10. As necessary, describe how the collected research data are organized and classified so that they can be verified and reused.	FSS guidelines include instructions to write a readme file which covers this. A template readme file is also provided.
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.	The possible exceptions listed (in a footnote in the original text) are included in FSS guidelines, including a requirement to record in the DMP the reasons not to publish data.
12 a. In the event of an investigation into alleged research misconduct, make all relevant research and data available for verification subject to the confidentiality safeguards established by the board of the institution	FSS guidelines ensure that all data is archived in a place where it can be accessed for verification purposes.
12 b. In highly exceptional cases, there may be compelling reasons for components of the research, including data, not to be disclosed to an investigation into alleged research misconduct. Such cases must be recorded and the consent of the board of the institution must be obtained prior to using the components and/or data in question in the scientific or scholarly research. They must also be mentioned in any results published.	There are currently no provisions for this in the FSS guidelines, since it is not clear what steps should be taken, and what criteria should be satisfied, to qualify for these exceptions.
22. Ensure that sources are verifiable.	Verifiability is the cornerstone of the FSS RDM guidelines. All FSS Data should be archived in such a way that verification is possible.
23. Describe the data collected for and/or used in your research honestly, scrupulously and as transparently as possible.	FSS RDM Guidelines ask for full documentation of all datasets, and for the data sets to be described with descriptive metadata or readme file. Researchers should also follow this point in their publications, but that goes beyond the scope of the FSS RDM Guidelines.
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.	The FSS guidelines specify this.
25. Contribute, where appropriate, towards making data findable, accessible, interoperable and reusable in accordance with the FAIR principles	The FSS guidelines follow the FAIR principles explicitly.
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.	From the perspective of the VU guidelines, this is redundant with item 11.

VU RDM Policy

Date: Feb-20

Last reviewed: 15/06/2023

URL: https://libguides.vu.nl/ld.php?content_id=32045526

VU RDM Policy	FSS
1. Researchers are responsible for compliance with legal and ethical requirements regarding their research data, including review by ethics committees if necessary.	This is included in FSS Policy.
2. Researchers are responsible for ensuring that their research data are reliably, traceably and securely stored throughout the data life cycle 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.	FSS guidelines ask researchers to use VU-provided infrastructure whenever needed, and if not ensure that the infrastructure lives up to this standard.
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.	FSS guidelines follow this. If the data is not archived for 10 years, motivation is required in the DMP.
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. 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.	FSS guidelines follow this, and explicitly recommend not publishing personal data, unless the researcher can ensure that they meet all legal and ethical requirements for publishing.
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).	Researchers register their data sets on PURE.

(continued)

VU RDM Policy	FSS
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 in the faculties are the first point of contact for support on these matters.	VU guidelines include explict references to GDPR, and the privacy register.
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.	FSS guidelines include a section on what to do upon contract termination.
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.	FSS has an RDM policy that specifically acknowledges the variety of disciplines within the faculties.

Guidelines for the archiving of academic research for faculties of behavioural and social sciences in the Netherlands

Date: Mar-22

Last reviewed: 15/06/2023

URL: https://zenodo.org/record/7583831

DSW	FSS
1. Preamble [...] Researchers working in the social and behavioural sciences at a Dutch university will be held to these standards to ensure that research integrity in general and transparency in particular can be ensured. Given the various distinct methodologies of scholarly research carried out under the general "social science" header, there are two main approaches that can be identified and should be implemented to ensure scientific integrity and its future assessment. The first is primarily for quantitative research designs and quantitative data that can most often relatively easily be de-identified (pseudonymized or anonymized) and stored in a repository in full. The second is for scientific research that is structured by qualitative and interpretive research designs and epistemologies that generate data and information that may have a different character and most often cannot be de-identified and stored in an identical manner as quantitative data. Regardless of methodological approach, all researchers have an obligation to follow the standards of integrity and transparency set in this document. All researchers must be aware of the specific regulations that govern their type of research and adhere to these regulations (except where motivated exceptions are allowed).	FSS guidelines follow the spirit of these guidelines, but FSS disagrees that qualitative and quantitative data should be treated differently. The reasoning for this can be summarized as follows: 1. While there is difference in the ease of de-identification of quantitative vs qualitative data, this difference is not such that it should have implications for the way data is handled: it is often still very difficult to fully anonymize quantitative data, and it is possible to pseudonymize qualitative data. 2. Even if pseudonymization of qualitative data is impossible, non-pseudonymized data can still be archived following our guidelines. 3. Much of our research combines elements of quantitative data analysis and qualitiative data analysis, making a distinction problematic to put into practice. 4. A distinction would further divide social sciences and complicate efforts to promote inter-disciplinarity. FSS therefore does not differentiate based on qualitative or quantitative, but on the specific nature of the data: for example the privacy risks posed by the data, the IP rights over the data, whether the data is available elsewhere, etc.

(continued)

DSW	FSS
1.1 Purpose of these guidelines These guidelines for the archiving of academic research set out the preconditions for the archiving of data, materials and information that form the basis for publications – in other words, (descriptions of) data, materials and information that are needed in order for academic peers and other consumers of the research to replicate, reproduce, and/ or assess the published research results. These guidelines relate to the data, materials and information with respect to publications that appear in their definitive form as of 1 September 2021 . The guidelines are based on the principle of retroactive accountability, i.e. reporting after a publication has appeared. The norm behind these guidelines is that each researcher is responsible for archiving data, materials and information, and the publications based on them, in a responsible and transparent way, in order to keep the data for future verification or checking by academic peers, and re-use. In situations where this document does not provide clear-cut rules, researchers are expected to act in the spirit of these guidelines rather than observing them to the letter. Faculties will be expected to apply these national guidelines. The guidelines will be evaluated every two years, under the responsibility of the deans of the faculties of social and behavioural sciences (DSW).	FSS endorses this purpose.
1.2 To whom do these guidelines apply? These guidelines apply to all faculty staff members who conduct research in the context of a temporary or permanent employment contract, all PhD candidates who conduct research under the supervision of a professor, and all research master's students. The guidelines do not apply to bachelor's and one-year master's students, unless their research results in an academic publication. Research conducted by bachelor's and one-year master's students falls under the formal responsibility of their supervisors. All researchers at the faculty must adhere to The Netherlands Code of Conduct for Research Integrity . These guidelines are a concrete embodiment of the principle of transparency and the related norms set out in the UNL Code of Conduct. The Netherlands Code of Conduct also requires researchers to make data as open as possible after publication or to document valid reasons for not sharing the data.	FSS adopted this exact wording in the RDM guidelines.

(continued)

DSW	FSS
1.3 Raw data, personal data and research data Within the framework of the transparency and replicability of research, raw data must of course be retained. Raw data are the unedited data that are collected within the framework of a research project, for example: - Registrations derived from experimental research - Survey data from questionnaires completed within the framework of research (including longitudinal research), collected by the researcher themselves or by an external fieldwork organization - (Transcripts of) video material collected within the framework of qualitative research (open interviews, observations) - Notes taken within the framework of qualitative research or research using source material - Raw data must always be de-identified as soon as and insofar possible so that they cannot be directly traced back to people or groups of people. Data that can be directly or indirectly traced back to a person are known as personal data. This includes not only name and address details, but also photographs, audio - and video material, and other identifying information. The de-identified raw data and the personal data together form the research data	FSS guidelines do not use the word "de-indentificaion" as it can mean both anonymization and pseudonymization, which are related but have different implications for the data. It is assumed the DSW guidelines mean pseudonymization in this section, so that is the wording used in this comparison. FSS do not include the advice to pseudonymize all raw data, for the following reasons: - Once data is pseudonymized, it may no longer be considered raw. - Fully pseudonymizing some forms of data (e.g. audiovisual data) is extremely complex and time consuming. - The identity of the data subject, or factors making indirect identification trivial, may be of crucial importance to the research. Pseudonymization will damage the data set in such cases. FSS therefore takes a pragmatic approach with respect to pseudonymization. It is considered as one of many measures available to the researcher to secure their data, and it is up to the researcher to decide which measures appropriately secure their data.
2. Guidelines concerning publication packages These guidelines relate to all research publications listed in the faculty's academic annual report. In order to ensure the transparency of qualitative and quantitative empirical research, all information that is needed to be able to assess the results must be archived (in English). This information is stored in a 'publication package'.	The FSS RDM guidelines do not mention the term "publication package". The term may lead to confusion: first, a researcher may think that the package itself must be published. Second, they may think that all elements need to be archived together. However, neither is the case: data may be archived in a restricted-access repository, and it is acceptable to have some items in a public repository, while others are in a restricted archive, as long as the various components link to each other.
2.1 What must be stored in a publication package? We make a distinction between publication packages resulting from quantitative research and from qualitative research projects, while noting the existence of mixed methods that employ both qualitative and quantitative elements and should be handled according to their main focus.	As stated above, FSS does not make a distinction between qualitative data and quantitative data. In the interest of brevity, specific instructions on what to archive are not included in the FSS RDM Guidelines. The focus is instead on the reasoning behind selecting data to archive: "all data than can be reasonably deemed necessary to verify the findings of the research." A separate document with specific FSS Archiving Guidelines exists which is linked to in the general RDM guidelines. The FSS Archiving Guidelines closely follow the DSW guidelines for quantitative data.
2.1.1 Quantitative research The following materials must be stored for each published empirical study (article, volume, book chapter, PhD thesis chapter, Research Master's thesis, consultable internal report, etc.):	NA
1. The published (or accepted) manuscript or publication.	Included in FSS Archiving Guidelines.
2. A brief description of the problem definition, research design, data collection (sampling, selection and representativeness of informants) and methods used. An electronic version of the published manuscript will generally suffice.	This is considered redundant with point 1.

(continued)

DSW	FSS
3. The instructions, procedures, the design of the experiment and stimulus materials (interview guide, questionnaires, surveys, tests) that can reasonably be deemed necessary in order to replicate the research. The materials must be available in the language in which the research was conducted. The publication package must be in English.	This has been reworded slightly in the FSS Archiving Guidelines, since replication is not possible for all research at the faculty. We therefore only talk about verification. The FSS guidelines require materials to be available in the original language, and in English.
4. When using primary data, the (de-identified) raw data files (providing the most direct registration of the behaviour or reactions of test subjects/respondents, for example an unfiltered export file of an online survey or raw time series for an EEG measurement, e-dat files for an E-Prime behaviour experiment, recordings or transcripts of interviews, descriptions of observations, archive and other source or media material). Documentation of the steps taken to de-identify the data and a blank consent form. If the raw data files have been accessibly stored in an external archive (such as storage facilities at DANS), making reference to the files in this archive will suffice. Such externally archived raw data may include primary or secondary data. Raw data may not be changed once they have been made digitally available.	FSS Archiving Guidelines do not require the data to be pseudonymized, as outlined above, but otherwise this is included.
5. Computer code (for example Atlas.ti, SPSS/JASP syntax file, MATLAB analysis scripts, R code) describing the steps taken to process the raw data into analysis data, including brief explanations of the steps in English, for example a brief description of the steps taken in the qualitative analysis of primary research data, i.e. themes, domains, taxonomies, components.	Included in FSS Archiving Guidelines for applicable data sets.
6. The data files (either raw or processed) that were eventually analysed when preparing the article (e.g. an SPSS data file after transforming variables, after applying selections, etc.) The latter is not necessary if the raw data file was directly analysed.	Included in FSS Archiving Guidelines, with an exception for cases where this data can easily be constructed from the raw data by running a script. In such cases providing the script and the raw data suffices.
7. Computer code (for example syntax files from SPSS/JASP, Atlas.ti, Matlab, R; syntaxes of tailored software) describing the steps taken to process the analysis data into results in the manuscript, including brief explanations of the steps in English.	Included in FSS Archiving Guidelines for applicable data.
8. The data management plan	Included in FSS Archiving Guidelines.

(continued)

DSW	FSS
9. A readme file (metadata) describing which documents and files can be found where and how they should be interpreted. The readme file must also contain the following information: a. Name of the person who stored the documents or files b. Division of roles among authors, indicating at least who analysed the data c. Date on which the manuscript was accepted, including reference d. Date/period of data collection e. Names of people who collected the data f. If relevant: addresses of field locations where data were collected and contact persons (if any) g. Whether or not an ethical assessment took place before the research, and, if relevant, study reference from and statements made by the Ethics Review Committee h. Whether the data is made open or not and if not, a valid reason for not opening up the data	Included in FSS Archiving Guidelines. A VU template is expected to be available soon.
The readme file must be sufficiently clear. A relevant fellow researcher must be able to replicate the results discussed in the publication based on the components of the publication package.	Included in FSS Archiving Guidelines, without the word "replicate".
10. Documents relating to the ethical approval or a reference to such documents.	Included in FSS Archiving Guidelines, with wording specific to our ethics committee.

(continued)

DSW	FSS
2.1.2 Qualitative research For qualitative, interpretative methodologies, a distinction should be made between the two main criteria for research integrity, i.e., transparency and reproduction. Transparency is a valid and legitimate demand also for qualitative research (and data), but reproduction is not considered possible in all cases, due to the very nature of the research designs and epistemology. Qualitative data are often impossible to fully de-identify and the research data is often gathered in forms and formats that cannot be stored in a digital repository. Of course, some of these data may be highly sensitive and cannot be shared with others without breaking ethical rules and the confidentiality that is often guaranteed to informants and other (human) sources of information. But as the aim of these guidelines is not sharing data but storing data, qualitative research should also be archived. Sensitive data should be stored on secured faculty servers. And when the format does not allow researchers to store original objects, it suffices to store pictures of the material. These data should be stored safely in a way that is accessible to the researcher who gathered the data. Researchers are therefore expected to store their data safely and to make specific plans for the time period of storage of their data, where and in which manner the data will be stored, and what will be done with the data once the research project ends or, for longterm ongoing research, once the researcher retires from research reporting etc. This calls for an elaborate and transparent data management plan or another, similar or equivalent form of data storage plan that describes: what kind of data will be gathered, by whom, in what format, where and in which form these will be stored, and to what extent and under what conditions this data will be shared and with whom, and any specific steps that will be taken to share the data that is safe to be shared. The researcher should be aware that according to the Netherlands Code of Conduct for Research Integrity there may be (highly exceptional) cases in which there are compelling reasons for components of the research, including data, not to be disclosed to an investigation into alleged research misconduct. Such cases must be recorded and the consent of the board of the institution must be obtained prior to storing the components and/or data in question. This documented exception must also be mentioned in any results published. In addition to safely storing data, the (qualitative) researcher shall make sure to maintain a record of the following metadata: 1. The dates that the researcher carried out the data collection (e.g. dates of interviews or observation, period(s) of time spent in the field (start date and return date), etc.; 2. The type of activities carried out (e.g., participant observation, number of interviews, frequency and character of observation, familiarizing oneself with the field, informal and formal conversations, other types of recording activities); 3. Interview and	FSS does not provide separate archiving guidelines for qualitative data. Archiving of qualitative data is important for verification purposes, and there is no reason why qualitative data should not be archived along the standards outlined above.

(continued)

DSW	FSS
2.2 When must a publication package be stored? A publication package must be stored within one month after the definitive publication of the manuscript. A publication package must be stored for each submitted research master's thesis. A publication package must be stored for each empirical chapter of a PhD thesis submitted to the thesis committee (or one single publication package if the thesis is a monograph). Once a publication package has been stored, it will be fixed and can then no longer be modified (read only).	FSS guidelines follow this.
2.3 Who is responsible for storing publication packages? If the first author works at one of the faculties of behavioural and social sciences, they will always be responsible for the archiving of the publication package, i.e. the storage of raw and edited data, syntax and materials, and additional information about the publication process as discussed above. Second or later authors who work at a faculty of behavioural and social sciences must know that the data have been carefully stored and how this has been arranged. This is particularly relevant if the first author does not work at a faculty of behavioural and social sciences.	If an FSS researcher is first author, they are responsible for archiving. If they are second or later, they "must know that the data have been carefully stored and how this has been arranged.", regardless of first author affiliation.
If the first author works at one of the faculties of behavioural and social sciences, the second or later author may assume that the first author will follow the guidelines of his or her own university, and the second or later author will not have to create a publication package.	See above.
For PhD candidates and research master's students, the primary supervisor or the day-today supervisor respectively are responsible for storing publication packages. The primary supervisor or day-to-day supervisor may delegate the execution of this task, but they will continue to bear final responsibility.	This is in FSS guidelines.
In collaborative projects a specific plan to clarify responsibilities related to the data after the project might be required. The person who coordinates the research programme that covers the publication (which, depending on the faculty in question, could be a professor, head of programme or head of department) is ultimately responsible.	This is not explicit in the FSS guidelines.
Adherence to the guideline will be discussed in performance and appraisal interviews. Formal final responsibility lies with the dean.	This is in FSS guidelines.

(continued)

DSW	FSS
2.4 Who has access to the publication package? Publication packages should be accessible by more than one researcher. The first author will have reading rights, but no right to delete or change versions. The first author will have writing rights for adding new versions. If a faculty has appointed a 'co-pilot' to check the analysis or a data steward to consider data management compliance, they will also be assigned reading rights. The faculty board can assign reading rights to a specific official to prepare for audits of publication packages on its behalf, for example, the coordinator of a research programme or a member of an academic integrity committee. After publication, academic peers should be granted access to the publication package if they make a reasonable request to verify or examine the published research results in the context of academic debate.	The archiving infrastructure offered by the VU (the Yoda Vault) follows this.
3. Minimum storage period For the retention period regarding research, a distinction is made between research data (and software) and the documentation of the process that has been carried out. Publication packages must be centrally stored on a secure faculty server facility for at least 10 years after the publication appeared. In the event of research (or secondary research) data including personal data, the principle of data minimization (conform GDPR regulation) must be applied as soon as possible. The Netherlands Code of Conduct for Research Integrity offers options to deviate from the retention period of 10 years. However, in that case the raw and processed data must be saved for a period suitable for the discipline and the methodology. The following could be taken into consideration when deciding on the - the nature (and especially the privacy sensitivity) of the data; - the need for source material to substantiate the results; - the applied scientific value of the research results; - the effort to make the data available for re-use; - the efforts of long-term preservation; - the usefulness of source material for follow-up research. The retention period of data management plans and data management protocols of projects, faculties and research institutes is at least 10 years, but not shorter than the retention period of the dataset . These documents primarily relate to policy making, execution and financing of research, and quality assessment. Also included here are the (legal) advice of ethical committees and evaluations and further agreements with research partners.	Following VU policy, the FSS guidelines say to archive for 10 years, with the possibility to deviate if motivated in the DMP.

(continued)

DSW	FSS
3.2 Data minimization and retention Data that can be traced back to individuals may in principle not be linkable to research data when this is no longer necessary for the purposes of the study. These personal data must be destroyed once they are no longer necessary for the purpose for which they were collected. Some specific studies may require retention of data that can be traced back to individuals, for example for the purpose of follow-up research or for longitudinal studies. Technical and organizational measures to protect the rights of data subjects need to be documented and will preferably be standardized for specific research scenarios. Protecting the right of data subjects is particularly important for raw data that cannot be de-identified (for example, video- and audio data). One complicating factor lies in the wish to retain personal data for the purpose of reviewing the integrity of the research itself, for example to check whether the participants did indeed participate in the research. If such integrity reviews are regarded as part of the research whose integrity is reviewed and considered necessary in the field it is allowed to store data that can be traced back to individuals for this purpose. When research is published, such personal data must be stored separately; not in the publication package. As an alternative option, researchers, faculties and research institutes can develop a protocol to monitor the integrity of the research before archiving, after which the personal data can be deleted. It is not necessary to store the personal data for the sole purpose of enabling participants to exercise their rights under the GDPR. The head of the relevant department or research program is responsible for monitoring the destruction of the research data on the required date. Official final responsibility lies with the dean.	The discussion by DSW ignores the fact that once data is pseudonymized, it is no longer raw data. The decision on what directly identifying data to keep and what not is thus extremely context-dependent. FSS trusts its researchers to make the right call, and thus takes a pragmatic approach here, where researchers decide on a case-by-case basis what to keep, and keep a record of their decisions in their DMP.
3.3 How are storage and archiving of research data arranged? The raw de-identified data must be saved on a faculty server that satisfies the relevant requirements for data storage in terms of security, robustness and automatic back-up facilities. The recommendation is to save the raw data in read-only format, before the data are made available for processing. Raw data stored in this way become fixed, which means that researchers will no longer be able to modify them deliberately or by accident.	The FSS guidelines recommend researchers use VU infrastructure (such as Yoda) which satisfy this.

(continued)

DSW	FSS
All data that can be traced back to individuals must be stored on a second faculty server, which is physically separate from the first faculty server and thus from the raw data. If a key is required to link pseudonymized raw data to the personal data, this key must be stored on the second faculty server. This includes raw data that cannot be de-identified and must be stored, such as audio- and video data in its original format that cannot be transcribed.	The FSS guidelines don't include this as a hard requirement, since few researchers have access to a second server. Currently, suggested alternatives to this are: - Encrypting directly identifying data. - Making sure that directly identifying data is not synced to local devices.
External storage of raw data, for example in national or international data archives such as DANS – which makes the data publicly available, retrievable and citable – is recommended and in some cases required, for example when NWO requires this in a contract. However, this does not relieve researchers of their duty to store the data internally on the first faculty server.	FSS does not comply with this, as archiving data twice puts an undue burden on researchers, and risks creating conflicting versions of data sets.
Individual storage on an own hard drive, USB stick or cloud solution such as Dropbox does not suffice. Data that are collected within the framework of PhD or postdoc research must be archived in such a way that continuity is ensured when the PhD candidate or postdoc in question leaves the faculty.	This is not explicit in FSS policy, but data needs to be stored on VU infrastructure.
These storage requirements do not apply to sections of raw data that are managed by external organizations. Researchers who use data from external organizations must verify that the organization in question stores its data in accordance with a protocol that satisfies the requirements of these faculty guidelines.	FSS guidelines are not explicit about this.
4. Faculty-specific policy Individual faculties can choose to add the following rules to the above-mentioned guidelines concerning publication packages and storage of raw data: 1. Faculties may decide that the guidelines also apply to data collected within the framework of one-year master's and bachelor's research projects. The supervisor can then be appointed as the responsible party. 2. Faculties may decide to extend these guidelines to include storage of all data, including research that has not been published. This must be set out in a data management plan. 3. Faculties may define rules concerning ownership of data, for example that storage of data in a publication package will not result in a change of ownership. 4. Faculties may decide to make random inspections to check the existence and quality of publication packages. 5. Faculties may use different time periods and, for example, indicate that a publication package must be archived upon acceptance (rather than publication) of a manuscript. 6. Faculties may decide that each manuscript must state where the data are stored (a data statement) and which roles the various authors played.	1. FSS does not extend to Bachelor and 1-year Master students, as sufficient infrastructure is not available for this. 2. For now, FSS policy only applies to published research. 3. VU has central policy that data is owned by the VU. FSS encourages department heads to ensure that researchers who leave FSS can continue to work with their data. 4. Random inspections do not fit within the culture of trust that FSS aims to cultivate. 5. DSW guidelines and VU guidelines are both for 10 years, and there is no reason to deviate. 6. This is included in the FSS guidelines.

FAIR Principles

Date: Mar-16

Last reviewed: 15/06/2023

URL: https://www.go-fair.org/fair-principles/

FAIR Principles	FSS
F1. (Meta)data are assigned a globally unique and persistent identifier	FSS guidelines require data to be archived in a repository that issues a unique and persistent identifier.
F2. Data are described with rich metadata (defined by R1 below)	FSS guidelines are for researchers to do this on PURE (at a minimum).
F3. Metadata clearly and explicitly include the identifier of the data they describe	FSS guidelines are for researchers to do this on PURE (at a minimum).
F4. (Meta)data are registered or indexed in a searchable resource	PURE meets this criterion.
A1. (Meta)data are retrievable by their identifier using a standardised communications protocol A1.1 The protocol is open, free, and universally implementable A1.2 The protocol allows for an authentication and authorisation procedure, where necessary	Public data repositories provide a link that works for this. For private data, researchers have to provide persistent contact details.
A2. Metadata are accessible, even when the data are no longer available	FSS relies on PURE and Yoda for this.
I1. (Meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation.	FSS does not have specific guidelines to ensure machine readability, but does recommend all archiving to be done in English.
I2. (Meta)data use vocabularies that follow FAIR principles	FSS requires all documentation to be uploaded in the same repository, under the same identifier as the data.
I3. (Meta)data include qualified references to other (meta)data	FSS has no specific guidelines for this.
R1. (Meta)data are richly described with a plurality of accurate and relevant attributes R1.1. (Meta)data are released with a clear and accessible data usage license R1.2. (Meta)data are associated with detailed provenance R1.3. (Meta)data meet domain-relevant community standards	FSS requires all public data to include licenses , and all personal data to have information about the informed consent procedure. Data that is not made publically available, but only archived for verification purposes, should only be made available under strict data transfer agreement that limit the use of data to the verification of the findings of the original research. To ensure provenance, FSS requires researchers to upload the rawest data they can, and a description of all modification to this data.

Guidelines for Anthropological Research: Data Management, Ethics and Integrity

Date: 2019

Last reviewed: 15/06/2023

URL: https://antropologen.nl/app/uploads/2019/01/guidelines-for-anthropological-research.pdf

ABV	FSS
Data ownership, data protection, and Open Science: Anthropological research materials cannot be considered as disembodied and transferable 'data'. As much anthropological knowledge is co-produced with our interlocutors, we cannot transfer possession, access, or ownership rights of 'our data' to others (such as employers, fellow-scientists, or the general public) without their consent. Based on relations of trust, our interlocutors often share personal and sensitive material with us. We are responsible for keeping such personal and potentially sensitive materials protected and confidential. Providing open access to fieldwork materials is therefore limited; in the case of an integrity inquiry we can at most provide confidential access.	The definition of data as used by the ABV is slightly different than that used by most of the policies that the FSS RDM guidelines are based on. Therefore, for the purposes of the FSS RDM Guidelines, anthropological research materials are considered data. However, the FSS RDM policy fully supports researchers stiving to keep personal and potentially sensitive materials protected and confidential: protection of respondents' privacy is a valid reason not to grant open access to data.
Anonymizing ethnographic research materials is often not a workable solution, as it is not only overly time-consuming but above all removes so much detail, that the material becomes virtually meaningless	The FSS RDM Guidelines are written with the realization that anonymization (or more often pseudonymization) comes at a real cost (in terms of time, effort, and data quality), and that only the researcher can determine whether the costs of anonymization/ pseudonymization outweigh the benefits. It therefore lists pseudonymization as something researchers can do to further secure their data, not as something they must do.
Anthropological knowledge production: Anonymity as default option and non-disclosure of fieldwork data are a precondition for anthropological knowledge production before they are turned into ethical concerns. If we do not allow for anonymity and the protection of our fieldwork material, many of our interlocutors would be hesitant, if not positively reluctant, to share their insights with us. Moreover, much of the knowledge we co-produce with our interlocutors is embodied and personal. Our fieldnotes function as a memory bank, rather than a complete record of knowledge acquired. Using this material without such personal knowledge runs the serious risk of misinterpretation of the material. This character of anthropology as a science dealing with research materials that can often not be reduced to 'data' has serious ethical consequences, especially regarding the following.	This relates to the points above: for the FSS RDM Guidelines, field notes would fall under the category "data", but the practical implications are limited: it is not necessary for data (and thus field notes) to be published or be interpreted by others. For verification purposes, the data should be archived as a record of the steps the researcher took to arrive at the conclusions in publications. Such archived data will only be accessed in case of doubts regarding academic integrity.

Academy of Management Code of Ethics

Date: undated

Last reviewed: 15/06/2023

URL: https://aom.org/about-aom/governance/ethics/code-of-ethics

AoM	FSS
2.4.1. When maintaining or accessing personal identifiers in databases or systems of records, such as division rosters, annual meeting submissions, or manuscript review systems, AOM members delete such identifiers before the information is made publicly available or employ other techniques that mask or control disclosure of individual identities.	FSS guidelines require pseudonymization before publication of data sets.
2.4.2. When deletion of personal identifiers is not feasible, AOM members take reasonable steps to determine that the appropriate consent of personally identifiable individuals has been obtained before they transfer such data to others or review such data collected by others.	FSS requires researchers to follow GDPR which has a more comprehensive approach on what can and cannot be done without consent.
2.5. Electronic Transmission of Confidential Information: AOM members use extreme care in delivering or transferring any confidential data, information, or communication over public computer networks when conducting AOM work. AOM members are attentive to the problems of maintaining confidentiality and control over sensitive material and data when the use of technological innovations, such as public computer networks, may open their communication to unauthorized persons.	Following GDPR, FSS requires researchers to take appropriate technical measures to secure personal data.

Beroepscode Nederlandse Kring voor Wetenschap der Politiek

Date: May-08

Last reviewed: 15/06/2023

URL: http://politicologie.nl/wp-content/uploads/2021/10/Beroepscode-2008.doc

NKWP	FSS
II.5: Politicologen dienen bij het verrichten van onderzoek maximaal zorg te dragen voor de intersubjectieve controleerbaarheid van hun bevindingen die zowel mogelijk dient te zijn voor collega-politicologen alsook voor derden die niet tot de kring der politicologen behoren. Daartoe zijn zij verplicht om, na de eerste publicatie dienaangaande, hun originele gegevens en relevante documentatie daarvan, eventueel onder bepaalde restricties, ter inzage en ter beschikking van derden te stellen teneinde replicaties en vergelijkingen mogelijk te maken. Het verdient aanbeveling de gegevens na op zijn laatst twee jaar onder te brengen in een openbaar data-archief.	This matches closely FSS Guidelines. FSS requires researchers to archive data in such a way that findings are verifiable, and also recommends publishing data.
III.4 Gegevens die ten behoeve van wetenschappelijke doeleinden zijn verzameld, mogen uitsluitend voor wetenschappelijk onderzoek worden gebruikt en dus niet worden aangewend voor justitiële of commerciële doeleinden.	FSS guidelines makes no such requirement, as it may be difficult to put in practice. “Commercial purposes” is poorly defined, and excluding those purposes may prove more restrictive than anticipated. It is therefore advised to make published data available under that doesn’t limit such use. For more information see: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3234435/
III.5 De direct identificerende gegevens van de informanten blijven anoniem voor derden, tenzij de informanten uitdrukkelijk toestemming hebben gegeven om hun identiteit in de openbaarheid te brengen. Onder direct identificerende gegevens worden verstaan: naam, adres, telefoonnummer, fiscaal nummer, kortom, gegevens die onmiddellijk tot één persoon te herleiden zijn. Reeds in het proces van gegevensverzameling dient vertrouwelijk te worden omgegaan met identificerende persoonsgegevens. Vertrouwelijkheid in deze fase houdt onder meer in dat direct identificerende persoonsgegevens gescheiden van andere gegevens worden bewaard en daaraan verbonden zijn door versleuteling. Als politicologen het vergaren van gegevens laten verrichten door anderen, zien ze er op toe dat die het in dit artikel gestelde in acht nemen. Politicologen zorgen ervoor dat direct identificerende gegevens niet in handen van derden komen, tenzij deze derden gehouden zijn aan de regels van deze code. Direct identificerende gegevens worden na afloop van het veldwerk vernietigd als ze niet meer nodig zijn voor het controleren van verzamelde gegevens. Als regel wordt een termijn van zes maanden na het afsluiten van het veldwerk aangehouden.	FSS guidelines are roughly in line with these requirements, but explicitly acknowledge that it may be difficult to remove directly identifying information while simultaneously maintaining data integrity and provenance.

Beroepscode Nederlandse Sociologische Vereniging

Date: 2002

Last reviewed: 15/06/2023

URL: https://www.nsv-sociologie.nl/?page_id=17

NSV	FSS
5. Sociologen dienen bij het verrichten van onderzoek maximaal zorg te dragen voor de intersubjectieve controleerbaarheid van hun bevindingen die zowel mogelijk dient te zijn voor collega-sociologen alsook voor derden die niet tot de kring der sociologen behoren. Daartoe zijn zij verplicht om, na de eerste publicatie dienaangaande, hun originele gegevens en relevante documentatie daarvan, eventueel onder bepaalde restricties, ter inzage en ter beschikking van derden te stellen teneinde replicaties en vergelijkingen mogelijk te maken. Het verdient aanbeveling de gegevens na op zijn laatst twee jaar onder te brengen in een openbaar data-archief.	FSS guidelines are in line with this.
5. Gegevens die ten behoeve van wetenschappelijke doeleinden zijn verzameld, mogen uitsluitend voor wetenschappelijk onderzoek worden gebruikt en dus niet worden aangewend voor justitiële of commerciële doeleinden.	FSS guidelines makes no such requirement, as it may be difficult to put in practice. “Commercial purposes” is poorly defined, and excluding those purposes may prove more restrictive than anticipated. It is therefore advised to make published data available under that doesn’t limit such use. For more information see: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3234435/
6. De direct identificerende gegevens van de informanten blijven anoniem voor derden, tenzij de informanten uitdrukkelijk toestemming hebben gegeven om hun identiteit in de openbaarheid te brengen. Onder direct identificerende gegevens worden verstaan: naam, adres, telefoonnummer, fiscaal nummer, kortom, gegevens die onmiddellijk tot één persoon te herleiden zijn. Reeds in het proces van gegevensverzameling dient vertrouwelijk te worden omgegaan met identificerende persoonsgegevens. Vertrouwelijkheid in deze fase houdt onder meer in dat direct identificerende persoonsgegevens gescheiden van andere gegevens worden bewaard en daaraan verbonden zijn door versleuteling. Als sociologen het vergaren van gegevens laten verrichten door anderen, zien ze er op toe dat die het in dit artikel gestelde in acht nemen. Sociologen zorgen ervoor dat direct identificerende gegevens niet in handen van derden komen, tenzij deze derden gehouden zijn aan de regels van deze code. Direct identificerende gegevens worden na afloop van het veldwerk vernietigd als ze niet meer nodig zijn voor het controleren van verzamelde gegevens. Als regel wordt een termijn van zes maanden na het afsluiten van het veldwerk aangehouden.	FSS takes a pragmatic approach here, where researchers need to decide on a case-by-case basis what to keep, and keep a record of their decisions in their DMP.