Data Management Plan Template

This template is intended for creating a data management plan, based on the data management section that was part of your research proposal. NWO expects you to incorporate any comments received from the referees and/or the committee about the data management section in this data management plan.

What does NWO understand as research data?

Research data are the evidence that underpin the answer to research questions, and can be used to validate findings. Data can be quantitative information or qualitative statements collected by researchers in the course of their work by experimentation, observation, modelling, interview or other methods, or information derived from existing evidence.

For the purpose of NWO's data management policy, the definition of research data does not include physical objects such as scientific and archaeological collections, physical arts works or biobanks; however, digital information extracted from such objects are to be regarded as research data.

Software is also not included in the definition. NWO recognises that software (algorithms, scripts and code developed by researchers in the course of their work) may be necessary to access and interpret data. In such cases, the data management plan will be expected to address how information about such items will be made available.

About this template and how to proceed

You are kindly requested to complete the plan below and submit it to NWO before the start of the project. NWO will review the data management plan as quickly as possible. If necessary, NWO will call upon the help of (data) experts from your scientific discipline for the evaluation. As soon as the data management plan has been approved by NWO, the project can be started. It is advised to regularly review the data management plan when required during the course of the research project.

You are expected to consult with research data management support staff at your home institution for the completion of this plan. NWO strongly advises researchers to seek such support at an early stage. Plans that have not been consulted with institutional data management support staff will not be accepted.

You should submit the completed form via the online application system ISAAC. The main applicant has to submit the data management plan via his/her/their own ISAAC account. Data management plans not submitted via ISAAC will not be taken into consideration.

This template is in line with Science Europe's "Core Requirements for Data Management Plans".

0	General Information	
0.1	Name applicant and project number	Frans Oort, TDCC-SSH-C2024-018
0.2	Name of data management support staff consulted during the preparation of this plan Date of consultation with support staff	Emma Schreurs, data steward at the Faculty of Social and Behavioural Sciences 23rd of May 2025

1	What data will be collected or produced, and what existing data will be re-used?	
1.1	Will you re-use existing data for this research? **If yes**: explain which existing data you will re-use and under which terms of use.	☒ Yes ☐ No We will re-use data from another TDCC-SSH project, named SLIPPRS-NL. They will collect policies related to RDM within all Faculties of Social and Behavioural Sciences (FSBSs) in the Netherlands and do a policy analyses. We will re-use this information, since we require this as well, and we don't want to overcharge the contact persons with similar questions. All contact persons are made aware of the fact that SLIPPRS-NL shares information with MICR.
1.2	If new data will be produced: describe the data you expect your research will generate and the format and volumes to be collected or produced.	In WP3 we will collect use cases that are about RDM and underlying support infrastructures within the SSH faculties of collaborating universities. These are textual data that are stored in docx format. The use cases are confidential and contain some identifiable information. Therefore, we will draft a joint controller agreement between the UvA, the VU, and SURF. In WP3 we will also collect survey data on the available support infrastructures within the SSH faculties. These data are numeric and will be stored in csv format. We will also receive policies from another project, see 1.1. These will not contain identifiable information, so no privacy contract is needed. The data are textual and will be stored as docx or pdf. All file formats are standard according to DANS.
1.3	How much data storage will your project require in total?	☒ 0 – 10 GB ☐ 10 – 100 GB ☐ 100 – 1000 GB ☐ >1000 GB

2	What metadata and documentation will accompany the data?	
2.1	Indicate what documentation will accompany the data.	The documentation of the data will be stored in a closed archive of the UvA, and the sections that have no restrictions due to privacy or confidentiality limitations will be made publicly available in a repository. For example: - A description of the dataset (e.g., a research protocol with operationalizations and methods of data collection). - A codebook that lists all the names of the variables and their meanings, including all possible values that these variables can take and meaning of all those values. - A README-file with a general explanation of the files.
2.2	Indicate which metadata will be provided to help others identify and discover the data.	The project (meta)data will be uploaded in a repository upon publication. The repository demands the data to incorporate metadata according to the Dublin Core Metadata Initiative (DCMI), which we will therefore adhere to. Information that we will incorporate is (among other things): - the maker(s) of the dataset(s) - title or name of the dataset(s) - a brief description of the dataset(s) - the date on which the dataset(s) were completed - rights regarding the data (ownership, copyright) - possible restrictions of access (embargo, conditions)

3	How will data and metadata be stored and backed up during the research?	
3.1	Describe where the data and metadata will be stored and backed up during the project. Explanation:	☒ Institution networked research storage ☐ Other (please specify) All project data will be stored at the UvA in MS Teams, in a dedicated project team environment. MS Teams automatically makes back-ups of the data. Additionally, these solutions have a “trash bin” in which deleted data is stored for 30 days; they also have version control. These functionalities can be used to restore data that was deleted/edited by accident.
3.2	How will data security and protection of sensitive data be taken care of during the research?	☐ Not applicable (no sensitive data) ☒ Default security measures of the institution networked research storage ☐ Additional security measures (please specify)

	Explanation:	The UvA's security measures are implemented and checked by dedicated staff, such as data stewards, information security officers, privacy contact persons and a data protection officer. The other project partners follow similar security measures. According to UvA policy, laptops used for research need to meet the following conditions: - Laptops are encrypted (Bitlocker or FileVault is on) - Laptops are password-protected at start-up and from sleep/standby mode - Laptops automatically log off after a period of inactivity of up to 15 minutes - Firewall is enabled, anti-malware is enabled (i.e., MS Defender) - System software (e.g., MS-Windows, Linux or Mac OSX) is up to date. Managed UvA laptops meet these requirements. Self-support UvA laptops do not automatically meet these requirements, employees must have set this up themselves. The above measures also apply when using your own/ other non-UvA laptops. On top of the laptop requirements, the following security requirements apply: - Anonymize the data - If anonymization is not possible, pseudonymize the data - Encrypt the data in storage if anonymization/ pseudonymization is not possible - Restrict access to the data to researchers who are directly involved - If pseudonymisation applies, save the key-file encrypted using a unique password, preferably only accessible by the PI.
4	**How will you handle issues regarding the processing of personal information and intellectual property rights and ownership?**	
4.1	Will you process and/or store personal data during your project? **If yes**, how will compliance with legislation and (institutional) regulation on personal data be ensured?	☒ Yes ☐ No At the UvA, we have data Data Stewards that evaluate every project in which personal data are processed. If necessary, data processing agreements are set up together with contract lawyers, and impact assessments are carried out with information security officers, privacy contact persons and the data protection officer.
4.2	How will ownership of the data and intellectual property rights to the data be managed?	Data will be collected at the UvA in collaboration with the Vrije Universiteit Amsterdam and SURF. Responsibility over the data lies with the universities that collected them.

5	How and when will data be shared and preserved for the long term?	
5.1	How will data be selected for long-term preservation?	☒ All data resulting from the project will be preserved for at least 10 years ☐ Other (please specify)
	Explanation:	All data will be archived for at least 10 years in the faculty archive. Following faculty guidelines, a so-called “data package for archiving and/or publication” is created for each research project, containing all the materials, raw and processed data, all the analysis code, results, and the final manuscript.
5.2	Are there any (legal, IP, privacy related, security related) reasons to restrict access to the data once made publicly available, to limit which data will be made publicly available, or to not make part of the data publicly available?	☒ Yes ☐ No
	If yes, please explain.	Since information on policies, guidelines, infrastructure and research projects may be confidential, they cannot be published open access. If a participant formally consents, the use cases can be shared with other researchers for other research purposes, in pseudonymized version (i.e., without directly identifying information, such as names). Anonymous results can and will be shared open access.
5.3	What data will be made available for re-use?	☐ All data resulting from the project will be made available ☒ Other (please specify)
	Explanation	All data except the confidential data, such as policies, guidelines, and use cases.
5.4	When will the data be available for re-use, and for how long will the data be available?	☐ Data available as soon as article is published ☒ Data available upon completion of the project ☐ Data available after completion of project (with embargo)
	Explanation	…
5.5	In which repository will the data be archived and made available for re-use, and under which license?	We will publish the data with DANS, using a CC BY license. DANS is a certified repository and provides a DOI.

5.6	Describe your strategy for publishing the analysis software that will be generated in this project.	It is unlikely any code will be written in this project. If code is written, it will most likely be in Python or R. If applicable, we will make them available along with the other study materials and make sure that they are properly annotated.

6	**Data management costs**	
6.1	What resources (for example financial and time) will be dedicated to data management and ensuring that data will be FAIR (Findable, Accessible, Interoperable, Re-usable)?	RDM infrastructure (data stewards, metadata experts, etc.) is provided by the UvA, VU and SURF. We also have expertise within the consortium.