Delft University of Technology: XYZ - DO NOT USE: test template of TU Delft DMP template (2021)

0. Administrative questions TEST

1. Name of data management support staff consulted during the preparation of this plan.

Guidance:

For dedicated data management plan support contact your Faculty Data Steward.

Example Answer:

My faculty data steward, [Name, Surname of the data steward], has reviewed this DMP on [date].

2. Date of consultation with support staff.

Guidance:

Please indicate the date of the consultation with the support staff

3. TEST

I. Data description and collection or re-use of existing data

3. Provide a general description of the type of data you will be working with, including any re-used data:

Example Answer:

Type of data	**File format(s)**	**How will data be collected (for re-used data: source and terms of use)?**	**Purpose of processing**	**Storage location**	**Who will have access to the data**
Anonymised data on household type electricity usage for Zuid-Holland province in 2018	.csv files	Re-use of existing data from EON company (data available under a data processing agreement)	To understand the differences in electricity usage between different types of households	SURF drive	The company and the project team (the PI and the two postdocs: John Doe and Mary Robinson).
Age, occupation, household type	.csv files	Online survey	To collect the age of the respondents and their occupation to make appropriate correlations	Project storage drive	The project team (the PI and the two postdocs: John Doe and Mary Robinson).
Microscopy images	.TIFF files	Confocal microscope	To visualize the effect of a given inhibitor on the cells	Project storage drive	The project team (the PI and the two postdocs: John Doe and Mary Robinson).

Guidance:

Types of data

Describe very briefly what type of data are you planning to collect/work with. For example:

- GIS data
- Measurements of material parameters
- Microscopy images
- Quantitative interview data
- Email addresses and/or other addresses for digital communication
- IP addresses
- Gender, date of birth and/or age
- Etc

How will the data be collected?

E.g. with a survey, datasets received from someone else (specify the source and terms of use), observations, recordings etc.

Purpose of processing

Briefly explain the purpose for data processing i.e. why do you need to collect the data.

Storage location

Explain the storage solutions which will be used to store research data for the duration of the research project. It is recommended that research data are stored on a dedicated Project Storage drive, which can be requested from the ICT department (request via TopDesk).

Data stored on Project Storage is only accessible by authorized individuals (ICT provides access control). In addition, confidential data should be encrypted. Encryption can be done at file or folder level with the use of a tool such as VeraCrypt. In addition, it may be a good idea to use a password manager such as KeePass (keepass.info) to avoid file access issues due to forgotten passwords. TU Delft ICT offers manuals for full disk encryption of TUD computers (not the Project storage drive) (BitLocker for Windows users and FileVault for Mac users). Alternatively, you can request support from ICT for customised solutions (privacy-tud@tudelft.nl).

Who will have access to the data?

Please explain who will have access to the data. Note that access to personal or other types of confidential data should be restricted as much as possible, based on 'need to have' principle.

Access includes using third party service providers such as cloud storage providers or survey platforms. If parties outside of your research team will have access to the confidential data, explain if you already have appropriate data processing agreements in place. If you don't yet have processing agreements in place, get in touch with the privacy team: privacy-tud@tudelft.nl.

4. How much data storage will you require during the project lifetime?

- 250 GB - 5 TB
- < 250 GB
- > 5 TB

Guidance:

The PI can request a dedicated Project Storage folder through the self-service portal: Project Storage at TU Delft

Requests for more than 5TB of Project Storage will have to be approved by your Faculty IT Manager.

II. Documentation and data quality

5. What documentation will accompany data?

- Data dictionary explaining the variables used
- Methodology of data collection
- Documentation in an Electronic Lab Notebook
- I will adhere to disciplinary metadata standards - please explain which standards in the box below
- Data will be deposited in a data repository at the end of the project (see section V) and data discoverability and re-usability will be ensured by adhering to the repository's metadata standards
- README file or other documentation explaining how data is organised
- Other - explain below

Guidance:

Reusing data is difficult if you don't know what the data is about and how it was created. Therefore, it is important to provide appropriate data about your data (metadata) and also to keep track of changes to your data (version control)

Metadata

Descriptive metadata is indispensable for the preservation, retrieval and re-use of datasets. It provides answers to questions concerning the person creating the data, the subject of the data, the type of file(s), geographic information and other aspects.

There are multiple types of metadata, for example:

- Embedded metadata
- Additional data documentation
- Discovery metadata in data repositories
- Disciplinary metadata

Embedded metadata
Sometimes metadata can be embedded directly within data files. Some scientific instruments will record metadata information about the files automatically. These are then recorded within the document properties, or embedded within the files themselves. Some examples include:

- FASTQ files - these are files in txt format used in life sciences (bioinformatics in particular) which store information about nucleotide sequence
- TIFF files - these files often contain additional information about images and how these were recorded
- FITS files - this is a file standard widely used in astronomy to store images and tables. FITS files contain a headers with metadata with information about the data

Additional data documentation
Metadata about the data can be also recorded outside of the actual data files. The most common way of doing this is to create dedicated README files. These are usually txt documents with necessary information about the data, which are stored next to the data files. 4TU.ResearchData offers useful guidance on how to create README files.

Some researchers, especially in the social sciences, create code books which explain the dataset and provide information such as code, field and label descriptions. The Data Documentation Initiative provides useful guidance on how to create a code book for your data.

Discovery metadata in data repositories
When you upload your data into a data repository, the data repository will also make your data discoverable. Discoverability is ensured through the use of discovery metadata: information such as the title of the dataset, the names of the authors, keywords, institutional affiliation etc. Data repositories usually adhere to metadata standards. For example, 4TU.ResearchData uses DataCite metadata schema as well as additional Dublin Core metadata.

Disciplinary metadata standards
Some disciplines have community-agreed metadata standards, which define the minimal information which is needed to understand and re-use research data.

FAIRsharing is a registry where you can find disciplinary standards for data.

Documentation in an Electronic Lab Notebook
An electronic laboratory notebook (commonly known as an ELN or a digital lab notebook) is a software system designed for scientists to help you document and maintain the reproducibility of your research and share information more easily. Electronic lab notebooks provide a text editor for writing notes in a way that replicates a paper notebook along with other functionalities such as spreadsheet tools for calculations and formatting of tables and graphs, protocol templates for documenting standard procedures, laboratory inventories for documenting samples, reagents, and apparatus and collaboration tools for sharing experimental information. TU Delft has a subscription to two electronic lab notebook tools: eLABJournal and RSpace.

III. Storage and backup during research process

6. Where will the data (and code, if applicable) be stored and backed-up during the project lifetime?

- Git(lab)/subversion repository at TU Delft
- SURFdrive
- Project Storage at TU Delft
- OneDrive
- Qualtrics (survey tool)
- Other survey tools - please specify below
- Another storage system - please explain below, including provided security measures

Guidance:

Storage options explained

Project Storage at TU Delft
Project Storage is the TU Delft provided storage facility with backup for research projects. It is only accessible to project members. Provisions for storing confidential data are possible. It is possible to give access to external collaborators (external members can be added). Please note that the access rights apply to the whole storage drive instead of individual folder/file. Project Storage can be requested through Top Desk. To make changes (such as storage size or give access to others), contact the Service Desk of your faculty: http://servicedesk.tudelft.nl

Location on your computer:
U: or \\tudelft.net\staff-umbrella\ (Windows) or /tudelft.net/staff-umbrella/ (Linux servers) or sftp.tudelft.nl:/staff-umbrella/

GitLab at TU Delft
TU Delft provided version control system with backup facility. Access to external collaborators can be provided. Note that public code sharing is disabled. You can create a GitLab repository yourself at https://gitlab.tudelft.nl. More information and a form to request access for external users can be found at Top Desk.

Subversion at TU Delft
TU Delft provided version control systems for data with backup facility. Access can be controlled by the repository owner.
Subversion repository can be requested through Top Desk.

SURFdrive
SURFdrive provides researchers with up to 500GB of cloud storage space. However, it should not be used as a primary storage location for research data because access to data is lost upon departure from TU Delft. SURFdrive can only be used as temporary storage. Do not use SURFdrive for highly confidential data such as state secrets, sensitive personal data or highly sensitive IP material.

SURFdrive can be used to share a folder/file with external collaborators by creating a public link and adding password protection as well as an expiry date. SURFfilesender can be used to send a folder/file.

OneDrive
TU Delft provided OneDrive to researchers with up to 1TB of cloud storage space. However, it should not be used as a primary storage location for research data because access to data is lost upon researcher's departure from TU Delft. OneDrive can only be used as temporary storage. Do not use OneDrive for highly confidential data such as state secrets, sensitive

personal data, or highly sensitive IP material.

OneDrive can be used to share a folder/file with external collaborators by specifying users one by one with their email address.

Qualtrics (survey tool)
Qualtrics survey software allows you to create online questionnaires for your research.
When using Qualtrics, it may happen that you gather details of your data subjects that can be traced back to the individual persons.

Additional guidance
The data (and code) should be stored safely ensuring transfer of responsibility if needed and backup. In addition, data needs to be stored securely, with access management and, for highly confidential data, with encryption. Our advice is to use the Project Storage at TU Delft. Your local drive or free cloud solutions (apart from SURFdrive and TU Delft provided OneDrive) do not qualify for securely storing research data, unless encryption, a proper backup-strategie and specific authorizations are applied. The group storage does not qualify for confidential data (authorizations are not limited to the users that need access).

For GitLab/subversion repositories (especially external ones), you need to make sure the responsibility is secured (i.e. a second person (faculty member) can take over the responsibility when needed) for as long as the project runs (or for 10 years after the projects ends if you plan to use the repository to publish the data, code, etc.).

Tools and apps also store data. Please consider the online tools that you use, e.g. Qualtrics and Microsoft Forms, and enter the information here.

6B. Automatically request Project Storage through TOPdesk

Only applicable if the box 'Project Storage at TU Delft' is checked in the previous question.

- Yes, I want to request Project Storage through TOPdesk

Guidance:

Please note that this automatically generated request can only be made at the time of plan creation, and cannot be changed later.

IV. Legal and ethical requirements, codes of conduct

7. Does your research involve human subjects or 3rd party datasets collected from human participants?

- Not sure
- No
- Yes

Guidance:

If your research project involves human subjects or 3rd party datasets collected from human participants, you are required to submit an application to the Human Research Ethics Committee (HREC). If you are unsure whether your research involves human subject or not, or if you need help with filling in the HREC application, please contact HREC@tudelft.nl

8A. Will you work with personal data? (information about an identified or identifiable natural person)

If you are not sure which option to select, ask your[Faculty Data Steward] for advice. You can also check with the [privacy website] or contact the privacy team: privacy-tud@tudelft.nl

- No
- Yes

Guidance:

Personal data - all information about an identified or identifiable natural person (the data subject). A person is considered identifiable if he or she can be identified directly or indirectly based on one or more items of personal data, for example, name and address, ethnicity, date of birth and IP-address. In general, it can be assumed that personal data include all data relating to a living person that makes it possible to identify this person or to distinguish him or her uniquely from other persons.

8B. Will you work with any types of confidential or classified data or code as listed below? (tick all that apply)

If you are not sure which option to select, ask your[Faculty Data Steward] for advice.

- Yes, data falling under export control regulations
- Yes, national security data (e.g. nuclear research)
- No, I will not work with any confidential or classified data/code
- Yes, I work with other types of confidential or classified data (or code) - please explain below
- Yes, politically-sensitive data (e.g. research commissioned by public authorities, research in social issues)
- Yes, confidential data received from commercial, or other external partners
- Yes, data which could lead to reputation/brand damage (e.g. animal research, climate change, personal data)
- Yes, data related to competitive advantage (e.g. patent, IP)

9. How will ownership of the data and intellectual property rights to the data be managed?

For projects involving commercially-sensitive research or research involving third parties, seek advice of your [Faculty Contract Manager] when answering this question. If this is not the case, you can use the example below.

Example Answer:

If no confidential information:

The datasets underlying the published papers will be publicly released following the TU Delft Research Data Framework Policy. During the active phase of research, the project leader from TU Delft will oversee the access rights to data (and other outputs), as well as any requests for access from external parties. They will be released publicly no later than at the time of publication of corresponding research papers.

Guidance:

Explain who will be the owner of the data, meaning who will have the rights to control access:

- Explain what access conditions will apply to the data? Will the data be openly accessible, or will there be access restrictions? In the latter case, which? Consider the use of data access and re-use licenses.
- Make sure to cover these matters of rights to control access to data for multi-partner projects and multiple data owners, in the consortium agreement.
- Indicate whether intellectual property rights are affected. If so, explain which and how will they be dealt with.

- Indicate whether there are any restrictions on the re-use of third-party data.

Make arrangements about data exploitation explicit:

- Document any agreements between yourself and other parties involved in your Data Management Plan
- Your faculty contract manager will be able to advise on these agreements

Remember that the TU Delft Research Data Framework Policy expects you to deposit your research data, code and any other materials needed to reproduce research findings in a research data repository in accordance with the FAIR principles (Findable, Accessible, Interoperable and Reusable), unless there are valid reasons not to do so.

Re-using data of others

If you want to re-use data of others, first check if there is a data licence. The data licence should inform you what you can and cannot do with the data. In case of doubts, contact your faculty contract manager or your Faculty Data Steward.

Need help?

Get in touch with your Faculty Data Steward.

10A. Which personal data will you process? Tick all that apply

- Access or identification details, such as personnel number, student number
- Email addresses and/or other addresses for digital communication
- IP addresses
- Names and addresses
- Telephone numbers
- Copies of passports or other identity documents
- Citizen Service Number (BSN)
- Financial information, such as bank account numbers
- Gender
- Date of birth and/or age
- Photographs
- Video material
- Audio material
- Performance appraisals or students results
- Signed consent forms
- Data collected in Informed Consent form (names and email addresses)
- Other types of personal data - please explain below

Guidance:

Various types of personal data are explained on this privacy page. If you are unsure which boxes to tick, contact the Privacy team: privacy-tud@tudelft.nl.

10B. Which special categories of personal data will you process? Tick all that apply

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex life, sexual orientation
- Criminal Offence Data

- No special categories of personal data will be processed

Guidance:

More information on special categories of personal data and data pertaining to criminal matters can be found on this page. If you are unsure which boxes to tick, contact the Privacy team: privacy-tud@tudelft.nl.

11. Please list the categories of data subjects

Guidance:

Examples of categories of data subjects are: (hospital) patients, mental or physically handicapped, customers, consumers, (school) children, students, elderly, elected officials, prisoners, whistleblowers, product users, employees, entrepreneurs, app-users, felons, athletes, residents of a certain city, asylum seekers, specific professionals, general public in a certain area, etc.

If you are not sure how to answer this question, contact the Privacy team: privacy-tud@tudelft.nl.

12. Will you be sharing personal data with individuals/organisations outside of the EEA (European Economic Area)?

- No
- Yes

Guidance:

TU Delft has to maintain a record of transfers of personal data to recipients outside the EEA. Such a transfer is generally prohibited unless:
=> the recipient is located in a jurisdiction that is deemed to provide an adequate level* of data protection,
=> appropriate safeguards are in place, or
=> a derogation or exemption applies

Knowing to what countries personal data is transferred will enable TU Delft to put appropriate measures in place.

If you require assistance on answering this question, please get in touch with the privacy team: privacy-tud@tudelft.nl.

13. To which countries will you be transferring personal data:

- Guernsey
- United States of America, (also) to organisations not certified under the Privacy Shield framework
- Canada (only to commercial organisations)
- Argentina
- Andorra
- Canada (also to non-commercial organisations)
- Faroe Islands
- Israel
- Isle of Man
- Japan
- Jersey
- New Zealand
- Switzerland

- Uruguay
- United States of America (only to organisations certified under the Privacy Shield framework)
- Other

Guidance:

TU Delft has to maintain a record of transfers of personal data to recipients outside the EEA. Such a transfer is generally prohibited unless:
=> the recipient is located in a jurisdiction that is deemed to provide an adequate level* of data protection,
=> appropriate safeguards are in place, or
=> a derogation or exemption applies

Knowing to what countries personal data is transferred will enable TU Delft to put appropriate measures in place. More information about the country list above can be found here.

If you require assistance on answering this question, please get in touch with the privacy team: privacy-tud@tudelft.nl.

14. Please contact the privacy team (privacy-tud@tudelft.nl) for advice on data transfer.

Please record below their advice, the data transfer mechanism used and agreed security measures:

15. What is the legal ground for personal data processing?

- Informed consent
- Other - please explain and contact the privacy team (privacy-tud@tudelft.nl). If you have already contacted the privacy team and received their advice, please record their advice below

Guidance:

TU Delft Informed Consent form template
The Human Research Ethics Committee at TU Delft provides a template for an informed consent form. If you have any questions about the template or your plans for ensuring that your participants are able to provide you with informed consent for study participation and data processing, please contact the Human Research Ethics Committee: HREC@tudelft.nl

Other grounds for data processing
Sometimes it might be impossible or impractical to ask your participants for informed consent for study participation and data processing, therefore it might be necessary to explore other legal grounds for data processing. In this case, please contact the privacy team at: privacy-tud@tudelft.nl. Please ensure that you provide the privacy team with the copy of your data management plan so far, so that they know the details of your project.

16. Please describe the informed consent procedure you will follow:

Guidance:

The UK Data Service provides excellent guidance on informed consent: https://www.ukdataservice.ac.uk/manage-data/legal-ethical/consent-data-sharing

The Human Research Ethics Committee at TU Delft provides a template for an informed consent form. If you have any questions about the template or your plans for the ensuring that your participants are able to provide you with informed consent for study participation and data processing, please contact the Human Research Ethics

Committee: HREC@tudelft.nl

If you need help answering this question, contact the Human Research Ethics Committee: HREC@tudelft.nl

Example Answer:

All study participants will be asked for their written consent for taking part in the study and for data processing before the start of the interview.

17. Please indicate below where will you store the signed consent forms

Guidance:

If you collect hard copy consent forms, store them in a secure location: for example, in a locked cabinet, in a locked office space. Alternatively, if signed consent forms are digital, or can be digitized, they should be stored securely, in a similar manner as your research data.

If you need help answering this question, contact your faculty data steward.

18. Does the processing of the personal data result in a high risk to the data subjects?

If the processing of the personal data results in a high risk to the data subjects, it is required to perform a Data Protection Impact Assessment (DPIA). In order to determine if there is a high risk for the data subjects, please check if any of the options below that are applicable to the processing of the personal data during your research (check all that apply).

If two or more of the options listed below apply, you will have to complete the DPIA. Please get in touch with the privacy team: privacy-tud@tudelft.nl to receive support with DPIA.
If only one of the options listed below applies, your project might need a DPIA. Please get in touch with the privacy team: privacy-tud@tudelft.nl to get advice as to whether DPIA is necessary.

If you have any additional comments, please add them in the box below.

- None of the above applies
- The processing prevents data subjects from exercising a right or using a service or a contract
- Innovative use or applying new technological or organisational solutions for data processing
- Data concerning vulnerable data subjects
- Sensitive personal data
- Systematic monitoring
- Automated-decision making with legal or similar significant effect
- Evaluation or scoring
- Data processed on a large scale
- Matching or combining datasets

Guidance:

Evaluation or scoring
Processing that includes profiling and predicting, especially from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

Examples of these types of processing are research on the movement of students and employees through the campus areas or research on migrants movements in cities/countries with the aim to have a predicting function.

Automated-decision making with legal or similar significant effect
Processing that aims at making decisions on data subjects, without human intervention, producing legal, or similarly significant, effects concerning the natural person which may lead to the exclusion or discrimination against individuals.

Systematic monitoring
Processing that is used to observe, monitor or control data subjects, including data collected through networks or systematic monitoring of a publicly accessible area.

Sensitive personal data
Processing of special categories of personal data, personal data relating to criminal convictions or other types of sensitive data such as financial data and location data. Please note that photo and video materials of research participants are also considered as sensitive personal data. Please see TU Delft GDPR terminology for more information.

Data processed on a large scale
Processing that includes any of the following criteria: a significant portion of any relevant group of subjects, a high volume of data (over 10.000 subjects), research data collection lasting for a long duration (more than 1.5 years), with a large geographical extent (data processing activities in more than two countries or data processing activities outside the European Economic Area).

Matching or combining datasets
Processing that includes two or more data processing operations (datasets) performed for different purposes, i.e. not for this research.

Data concerning vulnerable data subjects
Processing of data from any group where there is a power imbalance between the data subjects and the data controller. Vulnerable groups may include children, employees, mentally ill persons, asylum seekers, the elderly, or patients.

Innovative use or applying new technological or organisational solutions for data processing
Processing includes the use of new technology or organisational solutions since these novel forms of data collection and usage possibly come with a (currently unknown) high risk to the data subject.

The processing prevents data subjects from exercising a right or using a service or a contract
Processing that includes operations that aim at allowing, modifying or refusing data subjects' access to a service or entry into a contract. For example, where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

19. Did the privacy team advise you to perform a DPIA?

- No
- Yes

Guidance:

If you have not been in touch yet with the privacy team, or if you are unsure how to answer this question, get in touch with the privacy team as soon as possible: privacy-tud@tudelft.nl

20. Please include below the outcome of the DPIA, what measures did you take?

Guidance:

If you have not been in touch yet with the privacy team, or if you are unsure how to answer this question, get in touch with the privacy team as soon as possible: privacy-tud@tudelft.nl

21. Please indicate below where will you store the DPIA documents (document on data processing features and document on risk assessment)

Guidance:

The security measures resulted from DPIA are sensitive information to protect research data. It is recommended that the DPIA documents are stored securely, ideally using the Project Storage drive.

If you need help answering this question, contact your faculty data steward.

22. What will happen with personal research data after the end of the research project?

- Anonymised or aggregated data will be shared with others
- Personal research data will be destroyed after the end of the research project
- Other - please explain below
- Personal data will be shared with others - please explain which personal data will be shared, with whom, how and whether you have specified this in the informed consent form

Guidance:

Depending on the type of data, the choices made here will influence the future sharing possibilities of the data, and need to be considered carefully.

Pseudonymization: This can be done by assigning a unique participant number to each participant either on the informed consent form or a separate key document. When recording data from your participants, use only this unique participant number and not their names. Please note that this is not anonymization, since it is possible to trace each unique participant number to the corresponding participant. Therefore pseudonymised data is also considered as personal data.

Anonymization: Please be aware that full anonymization is often difficult to achieve. For instance, even if it is not possible anymore to trace each unique participant number to the corresponding participant, it might be still possible to identify a specific individual by putting together indirect identifiers.

For datasets that are anonymised public sharing is the best choice. Consent forms can ask participants for public sharing of anonymised research data, without specifying the purpose (this is sometimes referred to as an ‘open consent’). Note that in accordance with the TU Delft Research Data Framework Policy, research data should be stored for at least 10 years. TU Delft researchers can archive their anonymised research data (up to 1TB per year) free of charge at 4TU.ResearchData. 4TU.ResearchData will take care of data archiving and preservation for at least 15 years.

Alternatively, if datasets cannot be anonymised, and it is necessary to restrict the access to research outputs, the informed consent form needs to clearly define how and for what purpose datasets can be accessed or re-used. The informed consent form can ask for specific permissions, for example, limiting the groups of people who would be able to reuse the data, or limiting the purpose for which data can be used. It is also possible that some parts of the data will be suitable for public sharing, whereas others will require restricted access conditions. If data are not suitable for public sharing, please contact researchdata@4tu.nl for advice.

If you need help answering this question, contact your faculty data steward.

23. How long will (pseudonymised) personal data be stored for?

- Other - please state the duration and explain the rationale below
- 10 years or more, in accordance with the TU Delft Research Data Framework Policy

Guidance:

Process only the personal data that is necessary and relevant to achieve the research purpose. It might be the case that personal data can be destroyed upon analysis and/or anonymization. Destroying the personal data also means that you do not have to take responsibility for their privacy and security anymore.

But if you need the personal data for validation, reproduction or reuse purposes, you can keep it if the participants agree with it in the informed consent form. As with any personal data, be transparent to your participants about the following in the informed consent form and ask their consent for these activities: what personal data you are collecting, where it is going to be stored and for how long, what steps will be taken to safeguard and maintain the confidentiality of the personal information, to whom the data will be accessible to.

24. What is the purpose of sharing personal data?

- Other - please explain below
- For research purposes, which are in-line with the original research purpose for which data have been collected

Guidance:

Depending on the type of data, the choices made here will influence the future sharing possibilities of the data, and need to be considered carefully.

For datasets that are anonymised public sharing is the best choice. Consent forms can ask participants for public sharing of anonymised research data, without specifying the purpose (this is sometimes referred to as an ‘open consent’). Note that in accordance with the TU Delft Research Data Framework Policy, research data should be stored for at least 10 years. TU Delft researchers can archive their anonymised research data (up to 1TB per year) free of charge at 4TU.ResearchData. 4TU.ResearchData will take care of data archiving and preservation for at least 10 years.

Alternatively, if datasets cannot be anonymised, and it is necessary to restrict the access to research outputs, the informed consent form needs to clearly define how and for what purpose datasets can be accessed or re-used. The informed consent form can ask for specific permissions, for example, limiting the groups of people who would be able to reuse the data, or limiting the purpose for which data can be used. It is also possible that some parts of the data will be suitable for public sharing, whereas others will require restricted access conditions. If data are not suitable for public sharing, please contact researchdata@4tu.nl for advice.

If you need help answering this question, contact your faculty data steward.

25. Will your study participants be asked for their consent for data sharing?

- Yes, in consent form - please explain below what you will do with data from participants who did not consent to data sharing
- No - please explain below

Guidance:

Even if you are planning to fully anonymise the data, it is always important to ask your study participants for their consent for data sharing.

V. Data sharing and long-term preservation

26. What data will be publicly shared?

- All data (and code) produced in the project
- All validated non-positive results

- Not all data can be publicly shared - please explain below which data and why cannot be publicly shared
- No data can be publicly shared - please explain below why data cannot be publicly shared
- All data (and code) underlying published articles / reports / theses

Guidance:

The TU Delft Research Data Framework Policy expects you to:

- Ensure that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a research data repository in accordance with the FAIR principles (Findable, Accessible, Interoperable and Reusable) for at least 10 years from the end of the research project, unless there are valid reasons not to do so.

- Should data not be made available in a repository, ensure that the relevant metadata is discoverable and any research publications resulting from the project have a statement explaining what additional datasets/materials exists; why access is restricted; who can use the data and under what circumstances.

27. Apart from personal data mentioned in question 22, will any other data be publicly shared?

- All other non-personal data (and code) underlying published articles / reports / theses
- All validated non-positive results which do not contain personal data
- Not all non-personal data can be publicly shared - please explain below which data and why cannot be publicly shared
- I do not work with any data other than personal data
- All other non-personal data (and code) produced in the project
- No other data can be publicly shared - please explain below why data cannot be publicly shared

28. How will you share your research data (and code)?

- All data will be uploaded to 4TU.ResearchData
- My data will be shared in a different way - please explain below
- My data can’t be shared in a repository, but the metadata will be registered in 4TU.ResearchData and all research publications resulting from the project have a statement explaining what additional datasets/materials exists; why access is restricted; who can use the data and under what circumstances.
- I will share my data and code via git(lab)/subversion and also create a snapshot in a repository
- I will upload the data to another data repository (please provide details below)

Guidance:

The TU Delft Research Data Framework Policy expects you to:

- Ensure that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a research data repository in accordance with the FAIR principles (Findable, Accessible, Interoperable and Reusable) for at least 10 years from the end of the research project, unless there are valid reasons not to do so.

- Should data not be made available in a repository, ensure that the relevant metadata is published in a suitable repository and any research publications resulting from the project have a statement explaining what additional datasets/materials exists; why access is restricted; who can use the data and under what circumstances.

Repositories which have the Core Trust Seal certification will usually store data according to the FAIR principles. If you intend to use a repository which is not certified, you will need to make sure that the data, code etc. is findable (via a metadata repository), accessible (for those who can use the data) and interoperable (i.e. using open file formats when possible) for at least 10 years.

Help
Not sure how to answer this question? Talk to your Faculty Data Steward.

29. How will you share research data (and code), including the one mentioned in question 22?

- My data will be shared in a different way - please explain below
- I will share my data and code via git(lab)/subversion and also create a snapshot in a repository
- All anonymised or aggregated data, and/or all other non-personal data will be uploaded to 4TU.ResearchData with public access
- I will upload the data to another data repository (please provide details below)
- All pseudonymised data will be uploaded to 4TU.ResearchData with restricted access
- My data can’t be shared in a repository, but the metadata will be registered in 4TU.ResearchData and all research publications resulting from the project have a statement explaining what additional datasets/materials exists; why access is restricted; who can use the data and under what circumstances.
- No data can be publicly shared - please explain below

Guidance:

The TU Delft Research Data Framework Policy expects you to:

- Ensure that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a research data repository in accordance with the FAIR principles (Findable, Accessible, Interoperable and Reusable) for at least 10 years from the end of the research project, unless there are valid reasons not to do so.

- Should data not be made available in a repository, ensure that the relevant metadata is published in a suitable repository and any research publications resulting from the project have a statement explaining what additional datasets/materials exists; why access is restricted; who can use the data and under what circumstances.

Repositories which have the Core Trust Seal certification will usually store data according to the FAIR principles. If you intend to use a repository which is not certified, you will need to make sure that the data, code etc. is findable (via a metadata repository), accessible (for those who can use the data) and interoperable (i.e. using open file formats when possible) for at least 10 years.

Help
Not sure how to answer this question? Talk to your Faculty Data Steward.

30. How much of your data will be shared in a research data repository?

- > 1 TB
- 100 GB - 1 TB
- < 100 GB

Guidance:

At 4TU.ResearchData, TU Delft researchers can deposit 1TB of data per year free of charge.

31. When will the data (or code) be shared?

- At the end of the research project
- As soon as corresponding results (papers, theses, reports) are published
- Other - please explain

Guidance:

If research data supports a research paper or another public report, they should be shared no later than at the time of the publication of the corresponding research paper/report.

32. Under what licence will be the data/code released?

- Other - Please explain
- AGPL-3.0
- LGPL-3.0
- GPL 3.0+
- BSD
- MIT License
- CC BY-NC-ND
- CC BY-NC-SA
- CC BY-NC
- CC BY-ND
- CC BY-SA
- CC BY
- CC0
- GPL-2.0
- Apache
- EUPL-1.2

Guidance:

EUDAT's licence selector can help you make a suitable choice or visit the 4TU.ResearchData page on Licensing.

If you are unsure how to answer this question, talk to your Faculty Data Steward.

VI. Data management responsibilities and resources

33. Is TU Delft the lead institution for this project?

- Yes, the only institution involved
- Yes, leading the collaboration
- No - please provide details of the lead institution below and your role in the project

Guidance:

If TU Delft is not the lead institution for this project please only consider the data for which TU Delft researchers will be responsible whilst filling in this form. Please also ensure that you have discussed with your collaborators how data stored elsewhere will be managed.

34. If you leave TU Delft (or are unavailable), who is going to be responsible for the data resulting from this project?

Guidance:

Please provide name, surname and an email address. Ideally, provide functional details and e-mail address.

For Master students and doctoral candidates:

Please make sure that you share your plan with your supervisor in the "Sharing" tab.

Example Answer:

The Head of the Department of the Best Experiments (hod-bestexperiments@tudelft.nl)

35. 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)?

Example Answer:

4TU.ResearchData is able to archive 1TB of data per researcher per year free of charge for all TU Delft researchers. We do not expect to exceed this and therefore there are no additional costs of long term preservation.

[if applicable, add]:

The dedicated data manager hired in the project (see the project proposal and staff allocation) will be responsible for data management in the project.

Guidance:

An increasing number of research funders require researchers to comply with their requirements for formal management and sharing of research data. Activities related to good data management often cost time and money and therefore might have to be formally included in the project budget.

The costs of research data management can be roughly split into 'Personnel costs' and 'Other costs'.

Personnel costs

More and more research projects hire dedicated data managers to take the lead on data management tasks (see examples of data management tasks below). This is accepted by most funding bodies, see example here). The exact number of "Person-Months" (PMs) for data management tasks vary depending on the nature of the project and the types of data collected.

TU Delft offers a data management costing tool to help you budget for data management personnel costs in your proposal. In addition, we also have a collection of 'Data Manager' job advertisements from other universities which may help you drafting a job description/estimating the salary of the person.

Your Faculty Data Steward can provide tailored guidance on data management costs.

Other costs

Other data management costs might include the costs of hardware, the costs of infrastructure us, software costs and publishing costs.

Hardware and infrastructure costs

These might apply if you are planning to use hardware or other pieces of infrastructure, which are not provided free of charge by TU Delft. These might include:

- Costs of access to any specialist infrastructure, such as High Performance Computing.
- Cloud computing costs
- Storage costs: TU Delft offers 5TB of storage for free to every researcher. If you need to store more than 5TB of data, speak with your Faculty IT Manager about possible costs which might have to be included in the grant proposal.

Software costs

- Purchase of licences for software to support good data management, such as Electronic

Lab Notebooks, application for conducting interviews, project management software etc. (if licences for these applications are not already centrally provided by TU Delft).

Publishing costs

Here you might want to include the following costs:

- Data publication in data repositories other than 4TU.ResearchData (where TU Delft researchers can publish free of charge for up to 1TB of data per researcher per year).
- Publication of papers about datasets or software in dedicated journals.