Delft University of Technology: TU Delft Data Management Plan template (2025)

0. Adminstrative questions

1. Provide the name of the data management support staff consulted during the preparation of this plan and the date of consultation. Please also mention if you consulted any other support staff.

Example Answer:

[Name, Surname of the Data Steward], Data Steward at the Faculty of [Faculty Name], has reviewed this DMP on [date of review].

Guidance:

Some funders (such as NWO and ZonMw) require that you consult data support staff (in the case of TU Delft, the Faculty Data Steward) in the creation of your Data Management Plan. It is also advised to consult the Faculty Data Steward for DMPs created as part of the ethical approval process at TU Delft. For dedicated Data Management Plan support, please contact your Faculty Data Steward.

You can leave the feedback date empty until you receive feedback from the Data Steward. If you received advice from other support staff, such as the Privacy team, the Copyright team, or ICT, you can also indicate here who provided advice and the date on which you obtained the advice.

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

- Yes, the only institution involved
- Yes, leading the collaboration – please provide details of the type of collaboration and the involved parties below
- No – please provide details of the lead institution below and TU Delft's role in the project

Guidance:

If TU Delft is not the lead institution for this project, please only consider the data/code 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/code stored elsewhere will be managed. When describing TU Delft's role in the project, give a brief description of the work being done and how it relates to the data/code being collected/generated. For larger projects or consortia you may refer to relevant work packages.

Example Answer:

Example 1 for consortium projects:
In this project, TU Delft [Partner 1] is leading the research design and developing the research hardware. [Partner 2] is sharing commercial data on the performance of current tools and the proprietary schematics described in the table in question 3.

Example 2 for consortium projects:
[Partner 1] is leading the consortium. TU Delft [Partner 2], along with [Partners 4, 5, and 6], are members of the consortium. TU Delft is responsible for work packages WP1 and WP2.3.

I. Data/code description and collection or re-use

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

Example Answer:

Type of data/code	**File format(s)**	**How will data/code be collected/generated?** *For re-used data/code: what are the sources and terms of use?*	**Purpose of processing**	**Storage location**	**Who will have access to the data/code**
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.	SURFdrive	The company [name] and the TUD project team (the PI and the two postdocs: John Doe and Mary Robinson).
Age*, occupation, household type	.xlsx files, .csv files	Online survey using Microsoft Forms; responses collected anonymously.	Required to address the research question by comparison to the anonymised household data.	MS Forms (temporary storage) / Project Data Storage (primary storage)	the TUD project team
Personally Identifiable Information (PII) of participants: name, email	.xlsx file	Contact information for participants taking part in survey, received from participant sign-ups.	For administrative purposes: obtaining consent and communicating with participants.	Project Data Storage	As above
Informed consent forms	PDF	Informed consent forms signed digitally.	To obtain and document informed consent.	Project Data Storage	As above
Microscopy images	.TIFF files	Confocal microscope.	To visualize the effect of a given inhibitor on the cells.	Project Data Storage	As above

Research code	Mostly .py files, some .sh scripts. A local database may be used (.sql)	A new software package developed for this project. It will be released under the licence specified in Q31. This package will make substantial use of EON's API which cannot be shared.	Estimates values for household electricity usage based on input demographic data.	GitLab	As above

*Ages collected as 5-year age ranges

Guidance:

Types of data/code

Describe briefly the names of the type of data/code you are planning to collect/work with. For example:

- Geospatial data (public)
- Measurements of material parameters
- Microscopy images
- Quantitative interview/survey data
- Data visualisation script
- Analysis scripts (such as .py, .f90, .c, .m)
- Simulation model code
- Physical samples (such as rocks, human tissue)

- *Personally Identifiable Information* (personal data processed for administrative purposes, such as communication with participants, obtaining informed consent, or information related to distributing renumeration):

- Names and/or emails of participants
- Informed consent forms
- Key document to assign unique identifiers to participants for pseudonymisation

- *Personally Identifiable Research Data* (personal data processed for research purposes) such as:

- IP addresses and/or online user names
- Demographic information about the participants (such as gender, date of birth and/or age)

How will the data/code be collected/generated?

Specify the methodology (such as online surveys, field observations, output of machine learning algorithms) and the tools or applications (for example, MS Forms, QGIS, Python script) used to collect/generate the data/code. Before processing personal data or other confidential data using third-party software, be aware of how data are shared with the software provider and if this complies with security and privacy regulations. Please also note that some survey providers collect information such as IP addresses and location; it is important to disable these features. For more information and privacy/security recommendations for some tools, please see the Software Finder.

Are you using any experimental devices in interaction with humans? Please indicate the devices and whether or not they are CE certified. For more information and support, contact

the relevant Health, Safety, and Environment adviser.

If you receive or re-use data/code from someone else, specify the source and the terms of re-use. The terms of re-use will be specified by one of the following: (1) a licence (for example, for open source data/code), (2) terms of use (these are sometimes included on websites sharing data if no licence is specified), or (3) an agreement with the data owner (for example a data sharing agreement or Non-Disclosure Agreement (NDA)). If you have questions or concerns about copyright and/or licences of re-used materials (such as multimedia, data, and software), consult the Copyright Information Point.

Purpose of processing
Briefly explain the purpose for processing or generating the data/code: why do you need to collect/generate the data/code; how does this data/code help answer your research question(s)?

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

Data stored on Project Data 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 Bitwarden or Dashlane to avoid file access issues due to forgotten passwords. TU Delft ICT offers manuals for full disk encryption of TUD computers (not the Project Data Storage) (BitLocker for Windows users and FileVault for Mac users). When needed, you can request support from security@tudelft.nl.

Who will have access to the data/code?
Please explain who will have access to the data and code.

For personal data or other types of confidential data, access should be restricted as much as possible, based on the 'need to have' principle. Please keep in mind that using third-party service providers such as cloud storage providers or survey platforms may give those providers access to the data/code access as well: therefore, use of these should be carefully considered, especially for personal data and other types of confidential data. If parties outside of your research team (including third-party service providers) will have access to personal 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.

II. Storage and backup during the research process

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

- > 5 TB
- 250 GB – 5 TB
- < 250 GB

Guidance:

The Principal Investigator (PI) can request a dedicated Project Data Storage drive through the self-service portal: Project Data Storage at TU Delft. Requests for more than 5TB of Project

Data Storage have to be approved by the Faculty IT Manager.

5. Where will the data/code be stored and backed-up during the project lifetime? (Select all that apply.)

- GitHub/other version control repository (external) – please explain below
- Project Data Storage (U:) drive at TU Delft
- TU Delft OneDrive
- SURFdrive
- Git(lab)/subversion repository at TU Delft
- Another storage system – please explain below, including provided security measures

Guidance:

See the Storage Finder for an overview of the storage solutions offered by TU Delft.

Storage options explained:

Project Data Storage (U:) drive:
The Project Data Storage (U: or staff-umbrella) drive is the TU Delft provided storage facility with backup for research projects. It is only accessible to project members added to the drive. This is the recommended solution for storing all research data, particularly personal and other types of confidential data. If you process highly confidential data, take additional measures such as encryption (see the 'Sharing and collaborating' Sharepoint page).

It is possible to give access to the Project Data Storage drive to external collaborators (external members can be added). Please note that the access rights apply to the whole storage drive instead of individual folders/files.

Project Data Storage can be requested through Top Desk. To make changes (such as adjusting storage size or giving access to others), contact the Service Desk of your faculty or make use of UMRA (manual link).

OneDrive:
TU Delft provides OneDrive to researchers with up to 1TB of cloud storage space. OneDrive can only be used as temporary storage, as access to data is lost upon researcher's departure from TU Delft. 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 one-by-one by specifying users' email addresses.

SURFdrive:
SURFdrive provides researchers with up to 1TB of cloud storage space. SURFdrive can only be used as temporary storage, as access to the data will be lost upon researcher's departure from TU Delft. 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:
SURFfilesender is an external service for sharing large files (up to 1TB). If sending highly confidential data, make sure to encrypt the data and send the password through another channel.

GitLab at TU Delft:

TU Delft-provided version control system with backup facility. The TU DelftGitLab instance should be used when it is necessary to restrict access to the research code, for instance due to confidential content. By default, the GitLab is only accessible to TU Delft staff and students, and you can choose to further restrict access to private repositories to specific users. Access to external collaborators can also be granted on a case-by-case basis. More information and a form to request access for external users can be found at Top Desk.

GitHub and other externally hosted version control systems:
For some projects, access restrictions are not necessary or not desirable, in which case hosting code on an external service such as GitHub or GitLab is possible. These solutions are more suitable for collaboration with external collaborators. For a comparison between GitLab (TU Delft version) or other open-source repository managers based on Git, check here.

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

Additional guidance:
The data/code should be stored safely ensuring backup and transfer of responsibility, if needed. In addition, data needs to be stored securely, with access control and, for highly confidential data, with encryption. Our advice is to use the Project Data Storage at TU Delft. Your local drive, as well as external hard drives and other external storage media, should not be primary data storage or backup locations. It is also not recommended to use the Staff Group Data (M:) drive for research data, particularly not for confidential data/code, as access restrictions within the group are not enforced (all group members can see all files).

In case you use TU Delft OneDrive or SURFdrive, please make sure to have a backup (using Project Data Storage). OneDrive or SURFdrive only offer 30 days of back up and access rights expire upon termination of your contract.

Project Data Storage can also be used after the project ends. Please make sure to make necessary arrangements for extended access rights, and, if relevant, transfer of ownership.

For privacy/security reasons, do not use free online solutions for storage of research data (such as DropBox, your personal Google Drive/Hotmail or similar).

For GitLab/subversion repositories (especially external ones like GitHub), you must make sure appropriate procedures are in place to enable another staff member to take over the responsibility of administering the repository in your absence.

III. Data/code documentation

6. What documentation will accompany data/code? (Select all that apply.)

- Data – Methodology of data collection
- Data – Codebook describing the contents, structure, layout, and variable definitions of the data
- Data – Data dictionary explaining the variables used
- Procedure – A description of data processing procedure(s) (such as laboratory setup, simulation workflows).
- Procedure – Documentation of research method in an Electronic Lab Notebook
- Metadata – I will adhere to the metadata standards used by the data repository where the data will be shared (see section V)
- Metadata – I will adhere to disciplinary metadata standards - please explain below which standards are used

- Software – Usage documentation (README file, docstrings, and in-line comments)
- Software – Developer/API documentation (GitHub wiki, readthedocs)
- Other – please explain below
- Data – README file or other documentation explaining how data are organised

Guidance:

Documentation for data/code should include any information that is necessary to be able to validate, reproduce or reuse the data/code, and is paramount when making data/code available to others - during the project, or afterwards. Therefore, it is recommended that you start documenting your data/code as early as possible.

Re-using data and research software (from simple scripts to full libraries) is difficult if you don't know what they are about and how they were created. Therefore, it is important to have appropriate documentation including metadata about the data and software of your project, as well as to keep track of changes (version control).

Methodology of data collection:
A description of the data collection process that enables other researchers to replicate the study. This can be a qualitative description of a particular process or it may be a more formal description of the procedure using a service like protocols.io.

Codebooks and data dictionaries:
Some researchers, especially in the social sciences, create a codebook which explains the dataset and provide information such as code, field and label descriptions. They are usually text documents (.docx, PDF, or .txt format.), and are frequently – but not exclusively – used for survey and interview data. See useful guides to codebooks by ATLAS.ti, the Data Documentation Initiative or by ICPSR.

Data dictionaries are similar to codebooks in their content, but used in a wider range of contexts than codebooks. They are typically frequently formatted as a data table or spreadsheet: see 'How to make a data dictionary' by OSF.

Data organisation / README files:
When uploading datasets to a repository, you should include a README file that contains a description of the data, and any necessary information about its use. 4TU.ResearchData offers useful guidance on how to create README files for datasets.

Protocols and data processing procedures:
A comprehensive description of the research procedures such that an experiment, simulation, or manufacturing process can be independently repeated by other researchers. These are used in fields that have complex hardware/software workflows, or require precise calibration of parameters/samples for replication.

For example, in engineering, a common simulation workflow might include a hierarchical structure where material model parameters are used as input to simulate the overall behavior of a complex system. This workflow can also include specifics of the system configurations such as initial and boundary conditions, for all models involved in the simulation framework. Following this, there might be also post-processing procedures for the analysis.

Services such as protocols.io provide users a way to formalise the description of a research process in a FAIR and citable way.

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 headers with metadata with information about the data.
- NetCDF and HDF5 files – These files are often used for handling geospatial data and large datasets in high-performance computing environments, containing metadata about the structure and context of the 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. Data repositories usually adhere to metadata standards. For example, 4TU.ResearchData uses DataCite metadata and 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.

Software – Usage documentation:
Research software should be published with sufficient documentation for others to be able to set it up and run it. This requirement can be met by providing a README file alongside your code that describes the intended functionality, instructions on how to install and run the software, and links to any further reading or related publications. When developing code or software, it is good practice to include descriptions of variables, functions, and program logic within the scripts themselves using docstrings and in-line comments. Many integrated development environments (IDEs) include functionality to automatically insert template docstrings, or to generate basic descriptions of functions (for example, the autoDocstring plugin for Python code in Visual Studio Code). For an example README file and example software repository structure, see the DCC's faircode repository.

Software – Developer / API documentation:
Some software projects may benefit from more extensive documentation, such as when dealing with a large codebase, when the codebase contains many configurable options, or the project is widely used in the community. This documentation may be in the form of a compiled pdf document, set of linked markdown (text) documents, or static webpage (Readthedocs, GitHub wiki). For more information on making your software FAIR, see the DCC's FAIR software checklist.

IV. Legal and ethical requirements, code of conducts

7. Does your research involve human subjects or third-party datasets collected from human participants?

If you are working with a human subject(s), you will need to obtain the HREC approval for your

research project.

- Yes – please provide details in the additional information box below
- Not sure
- No

Guidance:

If your research project involves human subjects or third party datasets collected from human participants, you are required to submit an application to the Human Research Ethics Committee (HREC). For more guidance on the HREC application procedure, please consult the information and documents available on the HREC website.

If you have already applied for and/or received HREC approval, provide more information in the 'Additional Information' box.

If you have consulted the HREC but they advised that your research does not require ethical approval, state this under 'Additional Information'.

Example Answer:

If yes, intending to apply for ethical approval:
I intend to apply for ethical approval from the Human Research Ethics Committee, but have not yet done so.

If yes, having already applied for (and received) ethical approval:
I have applied for (and received) ethical approval from the Human Research Ethics Committee on [date] with HREC application number [#12345].

8. Will you work with personal data? (This is information about an identified or identifiable natural person, either for research or project administration purposes.)

- No
- Yes

Guidance:

Personal data – all information about an identified or identifiable natural person (the data subject). A person is considered identifiable if they can be identified directly or indirectly based on one or more items of personal data, for example, name, address or geographic location, date of birth or IP-address, but also factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. 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 them uniquely from other persons.

9. Will you work with any other types of confidential or classified data or code as listed below? (Select all that apply and provide additional details below.)

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

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

Guidance:

For questions on data that falls under export control regulations, please contact the TU Delft Knowledge Security team at adviesteam.kennisveiligheid@tudelft.nl.

10. 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.

Example Answer:

In case of collaboration with external parties:

- The intellectual property rights are framed by a consortium agreement between Delft University of Technology and [Insert names of key partners in the project involved in the steps described here].
- The intellectual property rights are framed by a collaboration agreement between Delft University of Technology and [Insert names of key partners in the project involved in the steps described here]. A specific Non-disclosure agreement was signed by the TUD and [name of Company], for the management of company data issued by [name of Company].
- *(for MSc students)* The intellectual property rights are framed by a graduation agreement between Delft University of Technology, myself and [insert the name of the company].

In case of internal project (if no other parties involved):

- *(for MSc students)* This project is an internal TUD MSc thesis project, in the context of the ongoing research project [Name of the project].
- *(for MSc students)* This is an internal TUD MSc thesis project.
- This is an internal TUD research project.

Guidance:

Explain who will be the data controller, meaning who will have the rights to control access. Consider:

- Access to data for multi-partner projects and multiple data owners should be outlined in the Consortium Agreement, or Collaboration Agreement.
- Explain what access conditions will apply to the data during the project? Will the data be openly accessible, or will there be access restrictions after the project? In the latter case, which? Consider the use of data access and re-use licences.
- Indicate whether Intellectual Property Rights are affected. If so, explain which and how will they be dealt with. 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 and the TU Delft Research Software Policy expect 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 or code of others:
If you want to re-use data or code/software of third parties, first check if there is a data or software licence. The licence should inform you what you can and cannot do with the data/code*: you can read more about data and software licencing in* 'the Turing Way'. If you have questions or concerns about licences, copyright, and/or terms of use of re-used materials (such as multimedia, data, and software), consult the Copyright Information Point. In case of doubts, contact your Faculty Data Steward.

Students:
Data generated by students largely belongs to the student in question, because they are not employed by TU Delft: this is in contrast to data generated by TU Delft employees. However, establishing ownership and Intellectual Property Rights becomes more complicated when a student's data are generated within the context of a university research group that the student is participating in, or as part of an internship at a company. Therefore, questions of IPR should be addressed before the thesis/graduation project begins. For more information, see the 'Intellectual Property Rights of Students' webpage and Intellectual Property Rights Flowchart, and **discuss with your supervisor.**

11. Which personal data or data from human participants do you work with? (Select all that apply.)

- Gender
- Free text fields (for instance, in questionnaires) in which participants could unintentionally share personal data
- Proof of consent (such as signed consent materials which contain name and signature)
- Special categories of personal data (specify which): race, ethnicity, criminal offence data, political opinion, union membership, religious or philosophical beliefs, sex life and/or sexual orientation, health data, biometric or genetic data – please provide details in the additional information box below
- Names as contact details for administrative purposes
- Names and/or geolocation information as part of research data
- Date of birth and/or age
- IP addresses or other online identifiers – please provide details in the additional information box below
- Financial information, such as bank account numbers
- Citizen Service Number (BSN)
- Copies of passports or other identity documents
- Photographs
- Video materials
- Performance appraisals
- Student results
- Other types of personal data or other data from human participants – please provide details below
- Telephone number, email addresses and/or other addresses as contact details for administrative purposes
- Access or identification details, such as personnel number, student number
- Audio recordings

Guidance:

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

12. Please list the categories of data subjects and their geographical location.

Guidance:

Examples of categories of data subjects are: (healthy) adults, customers, consumers, (school) children, (hospital) patients, mentally or physically handicapped individuals, 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.

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

Example Answer:

Survey participants are residents in urban areas in [country X], specifically in [location A] and [location B].

13. Will you be receiving personal data from or transferring personal data to third parties (groups of individuals or organisations)?

- No
- Yes – please provide details about the data and third party(ies) below

Guidance:

The transfer of personally identifiable information between different entities must be governed by specific agreements which lay out the responsibilities of all parties with respect to data subjects. Indicate here if you will be receiving personal data (such as names and email addresses) or sending such data to third parties (such as a private company, university, NGO). When you want to share personal data with a third party, you have to make contractual arrangements with that party. Please check the privacy website for more information and contact the Privacy team (privacy-tud@tudelft.nl) for support.

Note that data transfer to or from third parties also include data transfer after the completion of the project and the data has been archived, whether in open access or restricted access.

14. Which countries will you be receiving personal data from or transferring personal data to? (Select all that apply.)

- EEA country other than the Netherlands – please check the link in the guidance, and indicate which country in the additional information box
- Netherlands
- Other – please indicate which in the box below

Guidance:

TU Delft has to maintain the record of transfers of personal data to recipients outside the EEA (see EEA countries here). 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 from what countries personal data are received and to what countries personal data are transferred will enable TU Delft to put appropriate measures in place. If you require assistance with answering this question, please get in touch with the Privacy team: privacy-tud@tudelft.nl.

15. What advice did the Privacy team give regarding data transfer? Record below their advice, the data transfer mechanism used, and any agreed security measures.

Guidance:

If you have not already done so, please contact the Privacy team (privacy-tud@tudelft.nl) for advice on data transfer: include a draft of your DMP when contacting the Privacy team.

Please indicate what type of agreement will frame the data transfer and the minimum requirements of the type of the agreement.

16. What are the legal grounds for personal data processing?

- Other – please see guidance and explain below
- Informed consent

Guidance:

In order to process personal data, you need to comply with the GDPR principle of legal basis. The preferred basis for personal data processing at TU Delft is informed consent**,** but in some cases another legal basis may be required. Please consult the privacy team (privacy-tud@tudelft.nl) for more information.

Informed consent
Informed consent consists of an agreement between the researcher and the participants about what participants will do for the research, what the researcher will do to ensure participants' physical, emotional and reputational security, how long personal data will be stored, and whether data will be anonymised or pseudonymised and made available in a data repository for use in further research. The Human Research Ethics Committee at TU Delft provides a guide and templates for informed consent materials. You can find more information on the informed consent processes here: Research Design 3: Communicating and managing risk.

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, and, therefore, it might be necessary to explore other legal grounds for data processing. In this case, please contact the Privacy team: 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.

17. Please describe the informed consent procedure you will follow below.

Guidance:

The Human Research Ethics Committee (HREC) at TU Delft provides a guide and templates for informed consent materials. If you have any questions about the template or your plans for ensuring that your participants can provide you with informed consent for study participation and data processing, please consult the online documentation of the HREC.

If you need help answering this question, contact your Faculty Data Steward.

Example Answer:

Example 1 for written informed consent:
The researcher will inform the potential participants about the goals and procedures of the research project. The researcher will also inform them about the personal data that are being processed and for what purpose. This information will be provided to the potential

participants as follows: [please specify, for example, if a digital copy of the information will be emailed to participants before the interview/experiment]. All participants will be asked for their consent for taking part in the study and for data processing by signing a [physical/digital] informed consent form before the start of the interview/experiment.

Example 2 for verbal informed consent:
All participants will be asked for their consent to take part in the study and for data processing before the start of the interview/experiment. Consent is obtained verbally, whereby the participant positively affirms their participation in the study and their understanding of what the Participation Information Sheet states, and expressly agrees to the conditions of the data collection and processing. The consent will be recorded as follows: [please specify, for example, if a video/audio recording of the consent will be made, or if the verbal consent will be recorded using a witness].

Example 3 for consent for participating in an anonymous online survey:
At the start of the anonymous online survey an Opening Statement will be used to inform participants about the goals and procedures of the research project, as well as the type of information that is requested in the survey. Participants' agreement with the terms and conditions of the research are signified by clicking through to the survey.

18. Where will you store the physical/digital signed consent forms or other types of proof of consent (such as recording of verbal consent)?

Example Answer:

The proof of consent (digital copy of signed document) will be preserved on the TU Delft Project Data Storage (U:) drive.

Guidance:

If you collect hard copy consent forms, store them in a secure location (for example, a locked cabinet, and/or a locked office space). Alternatively, if signed consent forms are digital, or can be digitised, they should be stored securely, and separately from the research data, so that the consent forms cannot be used to re-identify participants. This can be achieved by encrypting the signed consent forms separately from the research data.

Note that even if you anonymise the data and do not process personal data anymore, you will be required to store the signed informed consent forms for validation.

If you need help answering this question, contact your Faculty Data Steward.

19. Does the processing of the personal data result in a high risk to the data subjects? (Select all that apply.)

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 in your research project.

If any category applies, please provide additional information in the box below. Likewise, if you collect other type of potentially sensitive data, or if you have any additional comments, include these in the box below.

If one or more options listed below apply, 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.

- None of the above apply
- Processing which 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
- Matching or combining datasets about individuals
- Data processed on a large scale about individuals
- Special category of personal data
- Sensitive personal data
- Systematic monitoring of activities of individuals
- Automated decision-making with legal or similar significant effect
- Evaluation or scoring of people or personal performance

Guidance:

If you process personal data in a way that could result in high risk for your participants, this requires you to approach the Privacy Team for an assessment regarding the potential necessity of a Data Protection Impact Assessment (DPIA). Consider carefully if you process personal data through any of the following ways:

Evaluation or scoring of people, or personal performance:
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 include research on the movement of students and employees through the campus areas, or research on migrant's movements in cities/countries, with the aim to have a predicting function.

Automated decision-making with legal or similar significant effect:
Processing that aims to make decisions on data subjects without human intervention, producing legal, or similarly significant, effects concerning the natural person, thereby potentially leading to the exclusion of or discrimination against individuals.

Systematic monitoring of activities of individuals :
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:
Some types of personal data are sensitive because they can have a high impact on the privacy of the data subject if other persons have access to these data. For example, financial data, location data, data relating to children or other vulnerable groups. Whether personal data must be considered sensitive also depends on the circumstances. Please note that photo and video materials of research participants are also considered sensitive personal data. For more examples of personal data that are considered sensitive at TU Delft, click here. For the processing of these sensitive personal data, it is important to provide additional safeguards to ensure that they are processed in accordance with the GDPR, equivalent to the safeguards for special categories of personal data.

Special category of personal data:
In addition to ordinary personal data, the GDPR also defines a stricter regime for special categories of personal data. As a rule, the processing of such data is prohibited. However, these data may be processed in certain cases if an exception for this is included in the GDPR or the GDPR (Implementation) Act. If you have questions regarding whether you process such personal data, contact the Privacy team: privacy-tud@tudelft.nl.
Special categories of personal data are data about a person’s religion, race, health, sexual life, political preference, trade union membership as well as genetic and biometric data. In the GDPR, the processing of personal data relating to criminal convictions and offenses and the Processing of a person’s Citizen Service Number (in Dutch: Burger Service Nummer,

BSN) is also subject to a separate regime.

Data processed on a large scale about individuals:
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 about individuals:
Processing that includes two or more data processing operations (datasets) performed for different purposes, beyond the research of the current project.

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, elderly, or patients.

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

Processing which prevents data subjects from exercising a right or using a service or a contract:
Processing that includes operations aiming 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 to decide whether to offer them a loan.

20. Did the Privacy team advise you to perform a DPIA?

- No – please provide details in the additional information box below
- Yes – please provide details in the additional information box below

Guidance:

If you have selected one or more of the answer options for Question 19, indicating that you process personal data in a way that could result in high risk to participants, you need to contact the Privacy team (privacy-tud@tudelft.nl). After the Privacy team provides their assessment on whether or not a DPIA is necessary, you can answer Question 20.

21. Please detail the outcome of the DPIA below, describing the measures taken.

Guidance:

If you have not yet consulted the Privacy team, or if you are unsure how to answer this question, contact the Privacy team as soon as possible: privacy-tud@tudelft.nl.

22. Where will you store the DPIA report (documents on data processing features and 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 Data Storage.

If you need help answering this question, contact your Faculty Data Steward.

23. What will happen with the personal data used in the research after the end of the research project?

- Other – please explain below
- Anonymised or aggregated data will be shared with others
- Personal data will be shared with others – please explain below which personal (pseudonymised) data will be shared, with whom, for what purpose, 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.

Pseudonymisation of personal data is the process of replacing personally identifiable information in data with artificial identifiers. This can be done by assigning a unique participant number to each participant on a key document and using this unique participant number for all data processing activities (such as collection, storage, analysis, sharing). Please note that this is not anonymisation, since it is possible to trace each unique participant number to the corresponding participant. Therefore, pseudonymised data are also considered personal data.

Anonymisation of personal data is the process of removing personally identifiable information from data in an irreversible way. Anonymisation means that there is no remaining personal data that can be used to re-identify participants, and that there is no other risk of re-identification of the participant. Unlike pseudonymised data, anonymised data are no longer considered personal data under the GDPR. However, please be aware that full anonymisation is often difficult to achieve: even if direct identifiers are removed, if there is still a possibility to identify specific individuals through indirect identifiers (such as gender, birth date, geographic location, occupation, or other descriptors) or using with other available information, the data are not anonymous.

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 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. 4TU.ResearchData offers both open (public) access and restricted access. You can contact researchdata@4tu.nl for advice.

In the informed consent form, you can ask the participants for their consent for anonymising their personal data with the purpose of publicly sharing the anonymised data. Datasets that cannot be anonymised cannot be shared with others unconditionally.

- If you intend to share a dataset that cannot be anonymised, it is advised to restrict access to this dataset. You also have to ask the participants to give consent for sharing their non-anonymised personal data with specified recipients and for specified purpose(s).
- Whenever data are intended to be shared publicly in a non-anonymised manner, a separate and explicit consent is required for this. We advise that you carefully discuss this with the Faculty Data Steward as well as Privacy team, if needed.

Note that even if you anonymise the data and do not process personal data anymore, you will be required to store the signed informed consent forms for validation.

If you need help answering this question, contact your Faculty Data Steward.

24. For how long will personal research data (including pseudonymised data) be stored?

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

- Personal data will be deleted at the end of the research project

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 anonymisation. Destroying the personal data also means that you do not have to take responsibility for their privacy and security anymore.

However, if you need the personal data for validation, reproduction or re-use purposes, you can keep the personal data if the participants agree to it in the informed consent form. As with any personal data, be transparent about the following in the informed consent form and ask your participants' consent for these activities: what personal data you are collecting; where the personal data will 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 during and after the project.

Note that even if you anonymise the data and do not process personal data anymore, you will be required to store the signed informed consent forms for validation.

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

- Other – please explain below (see guidance for additional options)
- In the informed consent form: participants are asked to give their explicit consent for sharing their (pseudonymised) personal data with restricted access with specific recipients for specific purpose(s)
- In the informed consent form: participants are informed that their personal data will be anonymised and that the anonymised dataset is shared publicly

Guidance:

If a participant does not give explicit consent for sharing their non-anonymised personal data, this participant has to be deleted from the dataset before data are shared. Even if you are planning to fully anonymise the data, it is always important and ethical to ask your study participants for their consent for data sharing.

In some cases, it may be acceptable to identify participants by name in the research output (such as specific expert interviews). In such cases, you need to obtain their explicit consent for the publication, and have a clear plan for the preservation of the consent material.

V. Data sharing and long term preservation

26. What data/code will be publicly shared?

Please provide a list of data/code you are going to share under 'Additional Information'.

- Not all data/code can be publicly shared – please explain below which data/code and the reason why public sharing is not possible
- All data/code produced in the project
- All data/code underlying published articles/reports/theses
- No data/code can be publicly shared – please explain below why data/code cannot be publicly shared
- Other – please explain below

Guidance:

The TU Delft Research Data Framework Policy expects researchers to:

- Ensure that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a 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 data repository, ensure that the relevant metadata is discoverable and any research publications resulting from the project have a statement explaining: what additional datasets/materials exist, why access is restricted, who can use the data and under what circumstances.

See also the TU Delft Research Software Policy.

Additionally, the funders of your project may have specific requirements - NWO and ZonMW require you to archive all data underpinning your results in a FAIR manner. Similarly, Horizon Europe projects often include Open Science requirements.

27. Apart from personal data mentioned in question 23, will any other data be publicly shared?

Please provide a list of data/code you are going to share under 'Additional Information'.

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

Guidance:

The TU Delft Research Data Framework Policy expects researchers to:

- Ensure that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a 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 data repository, ensure that the relevant metadata is discoverable and any research publications resulting from the project have a statement explaining: what additional datasets/materials exist, why access is restricted, who can use the data and under what circumstances.

See also the TU Delft Research Software Policy.

Additionally, the funders of your project may have specific requirements - NWO and ZonMW require you to archive all data underpinning your results in a FAIR manner. Similarly, Horizon Europe projects often include Open Science requirements.

28. How will you share your research data/code?

- All data/code will be uploaded to 4TU.ResearchData
- I will share the code via git(lab)/subversion and also create a snapshot in a data repository
- I am a Bachelor's/Master's student at TU Delft and I will share the data/code in the body and/or appendices of my thesis/report in the Education Repository

- I will will upload the data/code to another data repository – please provide details below regarding the availability of a persistent identifier (such as a DOI), licensing and preservation period of the data
- The data/code can't be shared in a data repository, but the metadata will be registered in 4TU.ResearchData with a persistent identifier (a DOI), and all research publications resulting from the project have a statement explaining: what additional datasets/materials exist, why access is restricted, who can use the data and under what circumstances
- The data/code will be shared in a different way – please provide details below regarding the availability of a persistent identifier (such as a DOI), licensing, and preservation period of the data

Guidance:

The TU Delft Research Data Framework Policy expects researchers to:

- Ensure that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a 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 data repository and any research publications resulting from the project have a statement explaining: what additional datasets/materials exist, why access is restricted, who can use the data and under what circumstances.

Additionally, the funders of your project may have specific requirements - NWO and ZonMW require you to archive all data underpinning your results in a FAIR manner. Similarly, Horizon Europe projects often include Open Science requirements.

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

Bachelor's and Master's students have the possibility, but are not required to share their data in a data repository (such as 4TU.ResearchData), unless their research constitutes part of a project of a university research group: see previous question 10 in the DMP.

For sharing code/software, see the TU Delft Research Software Policy and check the TU Delft Guidelines on Research Software.

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

29. How will you share research data/code, including those mentioned in question 23?

- All anonymised or aggregated data, and/or all other non-personal data/code will be uploaded to 4TU.ResearchData with public access
- All pseudonymised data will be uploaded to 4TU.ResearchData with restricted access
- I will share the code via git(lab)/subversion and also create a snapshot in a data repository
- The data/code can't be shared in a data repository, but the metadata will be registered in 4TU.ResearchData with a persistent identifier (a DOI), and all research publications resulting from the project have a statement explaining: what additional datasets/materials exist, why access is restricted, who can use the data and under what circumstances
- I will upload the data/code to another data repository – please provide details below

regarding the availability of a persistent identifier (such as a DOI), licensing, and preservation period of the data
- The data/code will be shared in a different way – please provide details below regarding the availability of a persistent identifier (such as a DOI), licensing and preservation period of the data
- I am a Bachelor's/Master's student at TU Delft and I will share the data/code in the body and/or appendices of my thesis/report in the Education Repository

Guidance:

The TU Delft Research Data Framework Policy expects researchers to:

- Ensure that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a 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 data repository and any research publications resulting from the project have a statement explaining: what additional datasets/materials exist, why access is restricted, who can use the data and under what circumstances.

Additionally, the funders of your project may have specific requirements - NWO and ZonMW require you to archive all data underpinning your results in a FAIR manner. Similarly, Horizon Europe projects often include Open Science requirements.

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

Bachelor's and Master's students have the possibility, but are not required to share their data in a data repository (such as 4TU.ResearchData), unless their research constitutes part of a project of a university research group: see previous question 10 in the DMP.

For sharing code/software, see the TU Delft Research Software Policy and check the TU Delft Guidelines on Research Software.

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

30. How much of your data/code 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/code per year free of charge.

31. When will the data/code be shared?

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

Guidance:

If research data support 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(s) will the data/code be released?

- Other – please explain below
- AGPL-3.0
- LGPL-3.0
- GPL-3.0+
- GPL-2.0
- EUPL-1.2
- Apache
- BSD
- MIT Licence
- Restricted (access) licence (such as EULA) – please explain below
- CC BY-NC-ND
- CC BY-NC-SA
- CC BY-NC
- CC BY-ND
- CC BY-SA
- CC BY
- CC0

Guidance:

A licence is a formal arrangement between the data/code sharer and the end-user, specifying what users can do with the data/code. All the licences starting with CC (Creative Commons) are commonly used for data. The other licences listed are used for code/software and are in accordance with the TU Delft Research Software Policy. TU Delft Data Stewards recommend CC-BY for open data (which requires citation when data are re-used) and MIT for open source software (a short and simple permissive software licence). CC-BY is also the top pick for most NWO and ZonMW projects. If you are working with third-party data/code, note that the licence of that data/code may restrict how you can share your derivative data/code. Visit the 4TU.ResearchData page on Licensing for more detailed information, use the CC licence chooser for data, or choose a licence for software. You can also check the TU Delft Guidelines on Research Software for detailed guidance about and compatibility of open software licences.

Students' theses:
All theses/reports in the Education repository are automatically placed under copyright: if you are happy with this, please select “Other” and mention the copyrighted thesis under ‘Additional Information’. Note that you can apply another licence (such as CC-BY) to your thesis, but this must be indicated separately within the thesis/report when depositing it in the Education repository.

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

VI. Data management responsibilities and resources

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

Guidance:

Please provide the functional details, name, surname and an email address of the person who is going to be responsible for the data/code resulting from this project. For a MSc/PhD project, this would be your supervisor. If you are a Principal Investigator, this could be the head of

your department.

For Master's students and doctoral candidates:
Please make sure that you share your plan with your supervisor in the ‘Share’ tab, or by sharing the PDF which you can download in the ‘Download’ tab.

Example Answer:

My supervisor [insert name, surname, role, department], with email address [insert email address].

34. 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)?

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, may need 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:
Increasingly, 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.

Your Faculty Data Steward can provide guidance on sources for data management costs, such as the costs of personnel, hardware, infrastructure, software or publishing.

Hardware and infrastructure costs:
Costs might apply to using 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 at least 5TB of storage for free to every researcher. If you need to store more than 5TB of data, speak with your Faculty ICT Manager about the possibilities.

Software costs:
Purchase of licences for software to support good data management, such as Electronic Lab Notebooks, transcription software to use for interviews, project management software (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.

Example Answer:

4TU.ResearchData is able to archive 1TB of data/code 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.