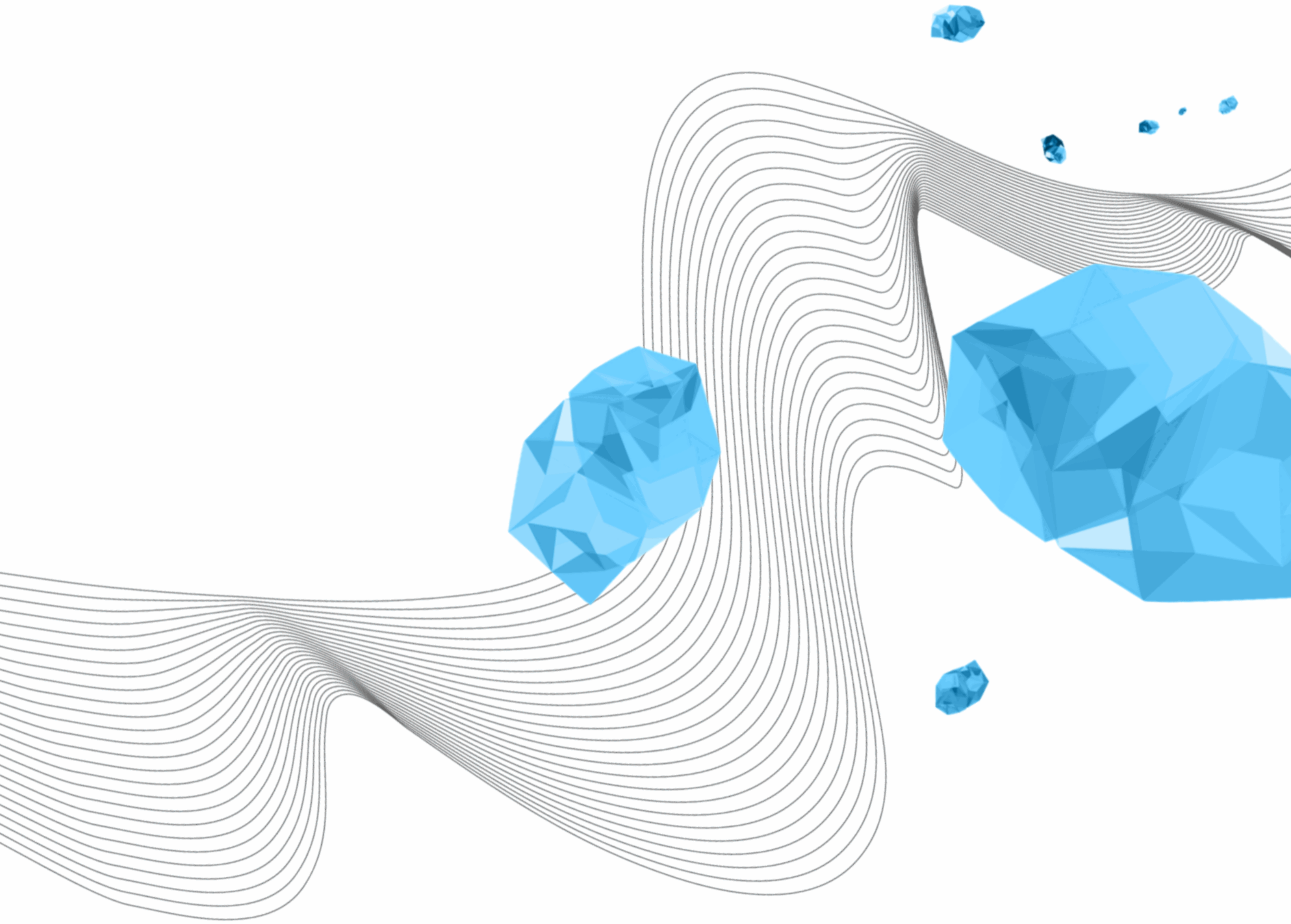
FACULTY OF ENGINEERING TECHNOLOGY

RESEARCH DATA MANAGEMENT POLICY DEPARTMENT OF DESIGN, PRODUCTION AND MANAGEMENT (DPM)

Version:

04-04-2024



UNIVERSITY OF TWENTE.

TABLE OF CONTENTS

1 Introduction ... 3
2 Department-specific roles and responsibilities ... 3
3 Data management plan (DMP) ... 3
4 Privacy regulations ... 4
5 Data storage and transfer ... 4
6 Data documentation ... 5
7 Data sharing ... 5
8 Data archiving ... 6
9 Data registration ... 6
Appendix A ... 7

Document management:

Version	Author(s)	Reviewer(s)	Description
2.2	F. van Slooten	V.R.J.R Wanningen	Updated based on the latest RDM developments at the UT/ET

Introduction

Regulations regarding research data management (RDM) are specified at various levels: UT level, faculty level, department level, research chair level, and individual researcher level. This document is intended as an addendum to the ET faculty RDM regulations (ET.23.19925, 05-05-2023), with the purpose of defining department-level guidelines or regulations for the department of Design, Production and Management (DPM). All content in this document are DPM department-specific. All content from higher-level regulations applies to this document, unless specifically indicated otherwise.

1 DEPARTMENT-SPECIFIC ROLES AND RESPONSIBILITIES

General roles and responsibilities are described in the UT RDM policy and ET RDM policy.

The chair holders are responsible for the department-specific rules and guidelines, and for their chairs' specific guidelines. Researchers are responsible for the execution of their own data management plan (DMP) during the project (including archiving at the end of the project). Daily supervisors will assure that a DMP is written in compliance with UT, ET, DPM and chair specific rules, and will supervise the execution.

Within DPM the following people can assist with data management:

- Fjodor van Slooten, as general IT contact person can advise and provide general help with software & licensing, hardware, access control and so on.
- System administration & support is the responsibility of LISA support staff (currently Milan Westerhof, T315), managed by Peter Lasker.

Contact the secretaries for additional information, current contact information is available at the DPM website.

All PhD candidates are obliged to follow the TGS course Data Management Bootcamp. Every employee can find most of the contents of the course on Canvas. Questions about the Bootcamp, Canvas course, DMPs, and data management can be directed to the ET Faculty Data Steward.

2 DATA MANAGEMENT PLAN (DMP)

General rules regarding DMPs are described in the UT RDM policy and ET RDM policy.

DPM WORKING RULE
For each research project, a DMP should be written and used during the project, preferably using the UT DMP-tool. DMPs of a chair are stored in a location which is accessible to the chair holder and all researchers within the chair, see Appendix A for the specific location that is used for each research chair.

A DMP must refer to the latest version of this document, with which it has to comply.

A DMP, as well as the actual data management resulting from it, must be updated if the DMP would no longer comply with regulations due to policy changes on any level. During the execution of the research project, it is advised to check for this on a regular basis, for instance once a year.

3 PRIVACY REGULATIONS

This part of the policy is about privacy-sensitive research data, and only applies to research that deals with personal data (e.g. using human participants).

General rules regarding privacy-sensitive data are described in the UT RDM policy and ET RDM policy.

DPM WORKING RULE

During the research, informed consent forms are stored in a safe way (e.g. a locked cabinet). A digital copy of these forms is only available to the researchers who are involved in the experiments, daily supervisor and chair holder. The original (paper) informed consent forms should be archived at the UT (ET) archive, as described in the ET RDM policy.

Pseudonymization key files that link participants' names with subject identification numbers/codes are stored in a separate folder than the pseudonymized data. This folder is only accessible to the researchers who are involved in the experiments, (daily) supervisor and chair holder.

4 DATA STORAGE AND TRANSFER

General rules regarding data storage and transfer are described in the UT RDM policy and ET RDM policy.

DPM WORKING RULE

Chosen storage options for the different research chairs are described in Appendix A. The Storage Decision Tree tool shows various options for storing and sharing data that are offered by the University of Twente.

At least the chair holder, and if applicable the daily supervisor, have access to the data of a researcher. The chair holder shares his/her research data with at least one other permanent staff member of choice. Data on the M-drive is not accessible to anyone else, therefore, the M-drive should not be used for storing research data.

In case of portable devices (external hard drive, usb stick), data is stored as short term as possible and backed up regularly, preferably on non-portable storage. If portable devices have to be used for confidential data (including privacy-sensitive data), devices have to be encrypted. (Confidential) Data on portable devices is deleted as soon as possible and no later than ending the research task for which the data is needed.

If portable devices are really the only option for storing large amounts of data, it should be ensured that at least a copy is available on another portable device which is kept at another place, and that all the research data is also available to the (daily) supervisor.

If the raw data set is large, a well-documented first processing of the data may be used to reduce the size. Data reduction/deletion always has to be discussed before with the chair holder/daily supervisor related to the research project.

Data from third parties is stored and documented in the same way as other data, unless there are restrictions (e.g. legal).

5 DATA DOCUMENTATION

General rules regarding data documentation are described in the UT RDM policy and ET RDM policy.

DPM WORKING RULE
When archiving project data, the project folder contains a file (.txt or .pdf) that describes the underlying directory structure and naming convention. It includes a section on the original author, ownership and confidentiality of the data.

Where data is stored, documentation is added to understand experimental procedures and simulations, and to be able to re-use the data (e.g. used devices, experimental/simulation settings such as sampling rates and conversion factors, specific versions of software and code, measurement units). All necessary documentation is saved together with the data.

Before closure of a project, the documentation and archived data is assessed by the daily supervisor/chair holder for conformance with the DMP of the project and this data management policy. For each publication, it should be clearly indicated where the corresponding data can be found.

The easiest way to add documentation is by means of adding README files to the project folder(s). Templates can be found here and here.

6 DATA SHARING

General rules regarding data sharing are described in the UT RDM policy and ET RDM policy.

DPM WORKING RULE
If needed, data should always be shared in a safe and secure way with collaborators (within and outside the UT).

Data should be shared using one of the storage/sharing solutions mentioned in the UT Storage Decision Tree tool, unless the group and/or external partner has another method to share data in a safe and secure way.

Data that is collected in the projects of DPM is often obtained in relation with industrial partners and can be subject to confidentiality agreements. Publication of project results requires approval from the project partners and data should be handled equally. If confidential data is shared within the group, all group members are bound to confidentiality. In specifically sensitive cases, confidential data should only be shared with the involved project members. Confidential data should never be stored on or shared by using ‘free’ cloud services like Dropbox, Google Drive etc.

7 DATA ARCHIVING

General rules regarding data archiving are described in the UT RDM policy and ET RDM policy.

DPM WORKING RULE

In Appendix A, it is described where data should be archived at the UT for each research chair. In all cases, at least the chair holder and (daily) supervisor need to have access to the archived data and management of access rights. Access rights should be passed to another member of the group when the access holder leaves the group. In addition to proper access rights management, encryption of confidential research data (files) is also possible.

Executable versions of simulation software (commercial or not) are not archived because it would not be useful without also storing operating systems and hardware. The documentation should include reference to used software versions.

Unpublished experimental and simulation data must be archived if it could be useful (for others). It should be discussed with the daily supervisor for which data this holds.

In addition to archiving data at the UT, at least research data related to a publication is uploaded to the 4TU.ResearchData repository or another trusted repository, unless this is prohibited by other legal and contractual regulations (e.g. confidential data). If needed, datasets can be embargoed (i.e. publicly available after a specific period) or made ‘confidential’ (i.e. allowing no/restricted access to others).

Archived data may not be altered, only appended to. Access management should be set such that files cannot be modified once placed in archive. If modifications are required, a new version should be created.

Data might be deleted after expiration of its storage term (typically 10 years after project-ending), and possible other conditions. Archived data on UT storage will only be deleted by the archive manager (i.e. person who is responsible for the archived data within a research chair) after discussing this with the chair holder. The archive manager will keep track of deleted information.

8 DATA REGISTRATION

General rules regarding privacy-sensitive data are described in the UT RDM policy and ET RDM policy.

DPM WORKING RULE

Once they are (permanently) archived, all datasets that are related to a publication should be registered in the research information system of the UT (currently Pure). The research information system only contains metadata (e.g. author, title, possible link to dataset), not the datasets themselves.

APPENDIX A

Data storage:

Data is preferably stored on a chair level at the Universities ‘P’ project disk within the main DPM folder (P:\ET\DPM). So the typical location of a chairs’ data storage will be P:\ET\DPM\<chair>.

Students’ data is preferably stored within the folder created for a student's project by the supervisor of the student, within the folder for the chair that the supervisor is part of.

Further details on the folder structure and how to use that is available in the guide at P:\ET\DPM\General\GUIDE.TXT

Data archiving:

Data will be archived at the UT network drive (project and organization directory, also called P-drive) in the P:\ET\DPM folder.

Read and write permission are arranged per chair, and if needed per project, in sub-folders.

The Main ICT contact person is responsible for assigning specific read and write permissions.

The P-project disk has a centralized backup scheme executed by Library, ICT Services & Archive.