Maastricht University

UM Research Data Management Code of Conduct

Research Data Management Code of Conduct

Date approved	28/05/2024
Version	1.14
Author	Dennie Hebels
Document owner	Chief Open Science and Open Science Officer at Maastricht University Library

Table of contents

Introduction

The paragraphs below constitute Maastricht University's (hereinafter: UM) Research Data Management (RDM) Code of Conduct, which outlines the guidelines and best practices for RDM[1]. This code applies to all research staff and students at Maastricht University, encompassing all disciplines and research activities. It provides UM's academics with essential principles and standards to ensure the responsible handling, preservation, and sharing of research data.

Research data are valuable to UM. They play an essential role in the scientific process and must be managed with care and integrity to ensure future reuse and verification of research data for academic research and educational purposes. RDM is indispensable to this process and includes all operations that deal with the organisation, storage, preservation, and sharing of research data, any associated metadata (descriptive information about the research data), as well as data governance and regulatory activities related to the collection, usage, and dissemination of research data within the framework of faculty compliance procedures. Many RDM best practices promote higher quality research, enrich teaching and learning resources, are time-saving, protect sensitive data, improve the visibility of research output, and contribute to recognition and rewards. UM academics therefore have a lot to gain by practicing good RDM.

There is a large variation in the type and format of research data that benefit from RDM. Research data can be either quantitative or qualitative, and they can include text, images, video, audio, spreadsheets, databases, statistical data, geographical data, clinical trial data, etc. Moreover, depending on the research methods used, some data can be easily reproduced, while other data are determined by time and place.

The FAIR principles of Findability, Accessibility, Interoperability, and Reusability[2] form an indispensable guideline in the RDM process (paragraph 2). Inherent security measures[3], privacy legislation[4] and determining the necessary intellectual property rights[5] play an important role too, in addition to the information security concepts of Confidentiality, Integrity and Availability (the CIA triad[6]). The purpose of RDM is therefore to safeguard the FAIRness of research data while protecting it against theft, misuse, damage or loss. Moreover, RDM is an essential aspect of Open Science, as it promotes the core values of impact and transparency in research and strengthens the teaching and learning engagements. By safeguarding the FAIRness of research data (transparency), academics can ensure that their findings can be replicated and built upon by other academics, leading to the advancement of knowledge in both academia and society (impact).

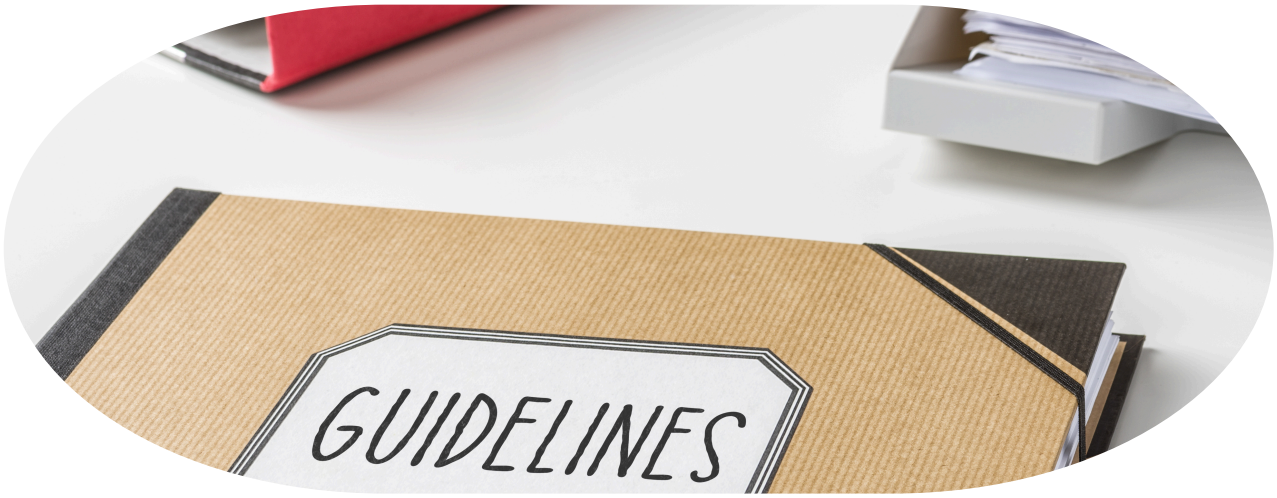
Open and accessible research data facilitate collaboration among academics at Maastricht University and other national or international institutions and/or companies, enabling them to work together on common research goals. This collaborative approach also helps to avoid duplication of effort and enhances the quality of research outcomes.

In addition, the use of appropriate infrastructural provisions to manage research data, such as data repositories, enhances the findability and accessibility of research data. This helps to ensure that research data are preserved over time and remain available for future generations of academics to use and build upon.

[1] Should any of the links in the footnotes no longer work, please send an email to the UM Open Science Officer or Chief Open Science https://www.maastrichtuniversity.nl/research/open-science
[2] More on the FAIR principles https://doi.org/10.1038/sdata.2016.18
[3] Please refer to the Information Security and Acceptable Use policies on the UM website https://www.maastrichtuniversity.nl/cybersecurity
[4] The academic must ensure that the processing of Personal Data is allowed. A guide has been developed to help academics determine what they should pay attention to under the General Data Protection Regulation (GDPR) and who to contact for assistance. https://umployee.maastrichtuniversity.nl/en/research/research-support-um-wide/the-gdpr-dos-and-don-ts-of-personal-data-in-scientific-research
[5] Please refer to paragraph 10 and 11
[6] More on the CIA triad https://en.wikipedia.org/wiki/Information_security

1. Compliance and monitoring

Adherence to the RDM guidelines and privacy legislation, as outlined in this Code of Conduct and any additional faculty guidelines, is essential for all academics. Faculty Deans play a key role in supporting this process, through monitoring and facilitating regular check-ins to promote alignment with these guidelines.



2. The FAIR principles

The FAIR principles aim to enhance the usability and value of data for both humans and machines. UM's academics are expected to follow the FAIR principles in their RDM activities. The principles cover the following:

- **Findability:**

Findability emphasises the need for research data to be easily discovered and located by both humans and machines. To achieve this, data should be accompanied by comprehensive metadata that describe the content, context, and provenance, (meta)data should have persistent and unique identifiers, such as DOIs (digital object identifiers), and (meta)data should be registered or indexed in a searchable resource (for example, in a trusted public data repository such as DataverseNL[7]).

- **Accessibility:**

Accessibility refers to ensuring that research data can be accessed by humans and machines under specific conditions or restrictions where appropriate. The principle of 'as open as possible, as closed as necessary' that is central to UM's Open Science Policy[8] also applies to the availability of data. (Meta)data should be openly available, or at least accessible with clear conditions and permissions. This involves the use of standardized access protocols and authentication mechanisms, ensuring data can be retrieved and used by anyone interested. Persistent and unique identifiers should be assigned by which data can be retrieved and the metadata should always be accessible, even if the data are not.

- **Interoperability:**

Interoperability enables seamless integration and combination of diverse research datasets by both humans as well as machines. To achieve interoperability, data should be structured using widely accepted and community-endorsed open standards and formats and relevant metadata standards. Community agreed schemas, controlled vocabularies, keywords, thesauri or ontologies should also be used where possible. This facilitates data integration, analysis, and exchange across different platforms, tools, and disciplines.

- **Reusability:**

Reusability emphasises the need for data to be reusable for future research and future processing, making it self-evident that findings can be replicated and that new research effectively builds on already acquired, previous results. This requires clear and explicit licenses, terms of use, and documentation. Additionally, data should be well-documented with rich metadata, enabling others to understand and build upon it effectively.

The FAIR principles apply equally well to research software/code and academics should ensure that data reliant on data processing scripts or automated workflows (i.e., software) are reproducible and adhere to FAIR principles. The preservation, versioning, and synchronisation of data and scripts are essential to ensure replicability. In the rest of this Code of Conduct, the term “research data” is also meant to include research software/code.

By adhering to the FAIR principles, research data become more valuable, fostering collaboration, reproducibility, and innovation across the scientific community and beyond. Moreover, it forms an integral part of UM’s Open Science policy[8] and harmonises research and education at UM. Practising Open Science, while adhering to the FAIR principles for RDM, ensures the optimal conditions for sharing and reusing research data and software for academic purposes thereby maximising their potential in both research and education. Academics should document how each of the FAIR principles is applied in their research by filling out a Data Management Plan, as described in the next paragraph.

[7] More on DataverseNL: https://library.maastrichtuniversity.nl/research/rdm/services-tools-training/dataverse/

[8] Please refer to the UM Open Science policy document: https://www.maastrichtuniversity.nl/file/um-open-science-policy-update-2022-v13pdf

3. Data Management Plans

Data management works best when it is planned in the early stages of the research process, i.e., during the design and writing phase of a research proposal. This can be achieved with a Data Management Plan (DMP). DMPs are essential components of scientific research that include details on data collection, storage, preservation (including data retention period, see paragraph 8), and sharing strategies. DMPs must also address issues of data sensitivity, including plans for anonymisation and handling of confidential information, in compliance with privacy legislation (see paragraphs 5 and 10). For research software, it also outlines aspects such as language choice, version control, documentation, and repository integration. A well-crafted DMP helps ensure that research data are properly managed throughout the research lifecycle and that they are in compliance with relevant legislation, regulations, and ethical standards.

The FAIR principles form the basis of every DMP and it typically includes information on data types, formats, and standards, data storage and backup, data sharing and access policies, data preservation, and data security and confidentiality. By providing a clear roadmap for managing research data, DMPs help to ensure the quality, integrity, and transparency of scientific research and thereby contribute to the core values of Open Science. Of course, drawing up a DMP does not guarantee that these goals are met and the academic is always responsible for monitoring its implementation and adjusting it when necessary during the course of a research project.

Publishers increasingly require academics to make their research data publicly available in FAIR-compliant data repositories. Moreover, most national and European subsidy providers, as well as several UM faculties, require a DMP to be drawn up as part of the grant approval process. These requirements reflect the growing recognition of the importance of RDM in ensuring the reproducibility and sustainability of scientific research. However, even in the absence of such requirements, writing a DMP is always advisable. UM has made tools available[9] to assist academics in drawing up their own DMPs and faculty Data Stewards[10] are available for any assistance.

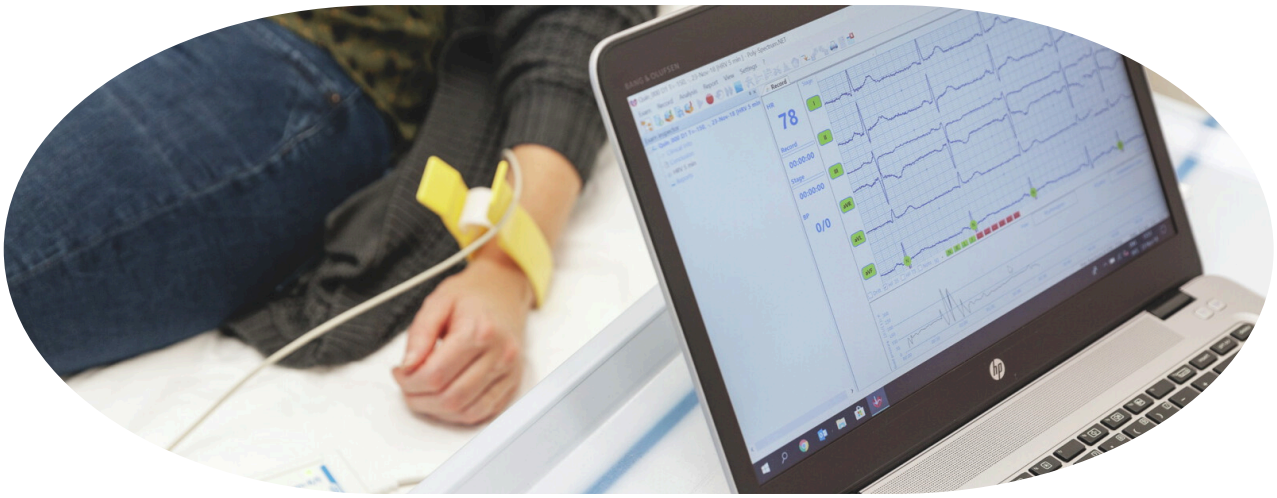
[9] Please refer to the information on DMPs: https://library.maastrichtuniversity.nl/research/rdm/research-data-management/data-management-planning/

[10] Please refer to the RDM faculty contacts: https://library.maastrichtuniversity.nl/research/rdm/faculties/

4. Ethical approval

Research performed at UM that involves human participants or personally identifiable data may be subject to an ethical review before the research is allowed to commence. Academics may also wish to have their research reviewed because journals, publishers or funders require it. Ethical review of scientific research involving either human participants or personally identifiable data is done by several ethical review committees within the university. For studies that fall under the Medical Research Involving Human Subjects Act (in Dutch, WMO), review by the accredited review committee METC (in Dutch, Medisch Ethische Toetsingscommissie) is always mandatory. For research that does not fall under the WMO, the ethical committees involved in approving the research differ per faculty[11] and for some review may be mandatory as well (e.g., FHML). Since research involving human subjects usually involves collecting Personal Data, compliance with the General Data Protection Regulation is always mandatory, regardless of the requirement for ethical approval (see paragraph 5). For studies involving Personal Data, additional documentation detailing data protection measures should therefore be included in the ethical review submissions.

Likewise, ethical review of scientific research involving animals also requires prior approval. The UM Animal Ethics Committee (in Dutch, DEC-UM) reviews animal research proposals on an ethical and scientific basis. After review, the DEC-UM submits its final advice to the Central Dutch Authority for Scientific Procedures on Animals (CCD). The CCD will subsequently decide to grant the license for the project proposal[12].



[11] Please refer to the rules on Ethics review per faculty: https://www.maastrichtuniversity.nl/research/integrity-ethics/ethics-review

[12] Please refer to the DEC-UM regulations: https://www.maastrichtuniversity.nl/about-um/faculties/health-medicine-and-life-sciences/facilities/maastricht-university-animal-ethics

5. Privacy, security, and confidentiality: General Data Protection Regulation

Privacy and confidentiality of research data are of utmost importance to UM. When carrying out research that involves human subjects, academics must know and comply with the rules established by the General Data Protection Regulation (GDPR[13]) and Maastricht University Policy on the Processing of Personal Data[14], here in after the Data Protection Rules. Personal Data are any information relating to an identified or identifiable natural person and can include amongst others:

- Biographical information or data on current living situation, including dates of birth, Social Security numbers, phone numbers, email addresses, etc.
- Looks, gender, appearance and behaviour, including eye colour, weight, character traits, etc.
- Workplace data and information about education, including salary, tax information, student numbers, etc.
- Private and subjective data, including religion, political opinions, geo-tracking data, etc.
- Health, sickness, and genetics, including medical history, genetic data, information about sick leave, etc.

The GDPR has additional requirements for the processing of Special Categories of Personal Data, which could be used to discriminate groups of people. These include, amongst others, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. These Special Categories of Personal Data have extra safeguards and require explicit consent from participating subjects.

[13] Please refer to the UM privacy regulations: https://www.maastrichtuniversity.nl/about-um/um-general-privacy-statement/privacy-regulations and the corresponding Dutch Implementation Act of the GDPR: https://wetten.overheid.nl/BWBR0040940/2021-07-01

[14] Please refer to the UM Policy on the Processing of Personal Data: https://www.maastrichtuniversity.nl/file/um-beleid-verwerking-persoonsgegeven091019enpdf

In accordance with the Data Protection Rules, UM academics are committed to handling research data in a secure and responsible manner, respecting the rights and privacy of individuals involved[15]. This means that academics should comply with the GDPR principles. The academic needs to:

- maintain a record of processing activities under its responsibility in relation to each research project in which Personal Data will be processed and therefore is subject to the principles of the GDPR. The record will be part of the more generic record of processing activities held by the related faculty (the faculty's Information Manager and dedicated Data Steward can be contacted for assistance[16]);
- document his/her RDM activities and be able to evidence them upon request, e.g., by a data subject, a competent supervisory authority, or in case of internal inspection by the Data Protection Officer (accountability principle);
- define the appropriate legal basis to process Personal Data, e.g., obtain the informed consent and provide the participants with the required information about the research (lawfulness, transparency and fairness);
- define the appropriate legal basis to share Personal Data with third parties, if applicable;
- protect the Personal Data against unauthorised access, by complying with the UM Information Security Policy[17] and following existing faculty regulations (integrity and confidentiality);
- only collect and process data that are necessary for the specific research purpose (data minimisation and purpose limitation);
- retain the said data only as long as they are needed to achieve the specific research purpose or as long as legal obligations mandate (storage limitation, see also paragraph 8) and
- process research data that are truthful (accuracy).

[15] The academic must ensure that the processing of Personal Data is allowed. A guide has been developed to help academics determine what they
should pay attention to under the GDPR and who to contact for assistance:
https://umployee.maastrichtuniversity.nl/en/research/research-support-um-wide/the-gdpr-dos-and-don-ts-of-personal-data-in-scientific-research
[16] Please refer to the RDM faculty contacts: https://library.maastrichtuniversity.nl/research/rdm/faculties/
[17] Please refer to the UM Information Security Policy: https://www.maastrichtuniversity.nl/file/policy-um-v30-2020-enpdf

UM recognises the importance of conducting research within the boundaries of the GDPR, which promotes transparency, fairness, and accountability in data processing. UM academics are responsible for ensuring compliance with the Data Protection Rules in their research activities, and they should work closely with their (local) privacy/GDPR team, faculty's Information Manager and Data Steward[16] to maintain the highest standards of privacy and confidentiality in handling research data. After registering a research project that will process Personal Data, the (local) privacy team will also inform the academic if additional GDPR procedures or specific faculty regulations need to be followed, such as the preparation of a Data Protection Impact Assessment.

6. External collaborations and knowledge security

In consortium research projects with (inter)national external partners, the responsibilities of all partners are articulated in the consortium agreement, which should normally be drawn up in the first months of the project. For data management, the DMP can be included as an annexe to the consortium agreement. Since organisations in a consortium might have diverse data storage and architectural solutions, FAIR data practices need to be ensured that emphasise data compatibility and format standardisation. Intellectual property rights and security measures, including data access controls, should also be clearly defined in the consortium agreement. Each consortium partner must consult their own (local) privacy team and/or legal advisor[16] regarding potential secondary agreements such as Data Transfer/Processing Agreements or Joint Controller Agreements, similar to Non-Disclosure Agreements.

Although international collaborations are one of the pillars of academic research, there are also risks associated with such partnerships that pose a serious threat to our knowledge security. In this context, knowledge and innovation are increasingly seen as strategic instruments of power. In particular, if sensitive knowledge and technology fall into the wrong hands it can have negative consequences for our national security and innovativeness. Knowledge security is about protecting sensitive knowledge and technology from unwanted access, influence, and other misuse. In many cases, it requires practical, organisational precautions and a degree of vigilance on the part of our academics[18].

[16] Please refer to the Information Security and Acceptable Use policies on the UM website: https://www.maastrichtuniversity.nl/cybersecurity

[18] More on how to maintain knowledge security: https://umployee.maastrichtuniversity.nl/en/research/research-support-um-wide/knowledge-security-yes-unless%E2%80%A6

7. Information security

To comply with all regulations and be sure that data can be relied upon, careful handling of research data is an important factor in RDM. Within UM, we have all the facilities academics need to work safely. If UM infrastructure is used and the guidelines of our Information Security Acceptable Use policies are followed, then research data should be "information secure"[19]. If deviation from our standard data research infrastructure is needed, make sure that data is processed compliant and secure by discussing this first with the faculty Information Manager[20].

[19] Please refer to the Information Security and Acceptable Use policies on the UM website: https://www.maastrichtuniversity.nl/cybersecurity

[20] Please refer to the RDM faculty contacts: https://library.maastrichtuniversity.nl/research/rdm/faculties/

8. Data storage and retention

Both during and after a research project, academics are expected to store all research data responsibly within the UM data infrastructure (i.e., UM-approved cloud services or physical servers, observing the respective terms of use of these facilities[19]). During the research process, there are three points of protection to consider:

- Protection against data loss: periodic data backups to an independent storage device (e.g., a UM-approved server) are essential to prevent accidental data loss.
- Protection against data leakage: a careful assessment of all used storage places and their access points needs to be performed to ensure minimisation of data leakage. Data encryption can also be a useful tool here, provided it is combined with good password management. Sensitive data must always be stored in encrypted formats with access controls.
- Protection of data integrity: version control tools and synchronisation management are key to maintaining the integrity of research data.

If an academic stops working on a UM research project or resigns from UM altogether, a proper data handover procedure needs to be followed in which a new UM data responsible person is assigned who carries the responsibility for the continued protection of the research data from the departing academic. This means that the data are either securely transferred to the person responsible or the person responsible is informed about the location of the data within the UM data infrastructure, and the person responsible is given any necessary access rights to the data.

At the end of the research project (or earlier depending on need, relevant faculty guidelines or other applicable rules), research data must be archived in the infrastructure facilities made available by UM. These facilities can differ between faculties but should always provide a secure internal long-term storage solution for research data. The Maastricht Data Repository (MDR[21]) or secure internal UM network drive storage are suitable archiving options. The choice between these two options is determined by the project's collaborative nature, faculty-specific guidelines, and data volume. However, specific determinations might arise, and it's advisable to consult with a Data Steward or Information Manager.

[19] Please refer to the Information Security and Acceptable Use policies on the UM website: https://www.maastrichtuniversity.nl/cybersecurity

[21] Please refer to MDR: https://mumc.atlassian.net/wiki/spaces/IN/overview

In accordance with the Netherlands Code of Conduct for Research Integrity[22], all data, software codes and research materials, published or unpublished, are managed and securely stored for a period appropriate to the discipline(s) and methodology. For medical research, subject to the WMO, this concerns legally binding retention periods of up to 30 years, depending on the type of research[23]. For non-WMO research, data retention conditions put forward by the funder take precedence. For example, NWO-funded research is subject to a retention period of 10 years, unless legal provisions or discipline-specific guidelines dictate otherwise. If the funder does not have a data retention policy or if research is funded through other means, a retention period of 10 years is often used.

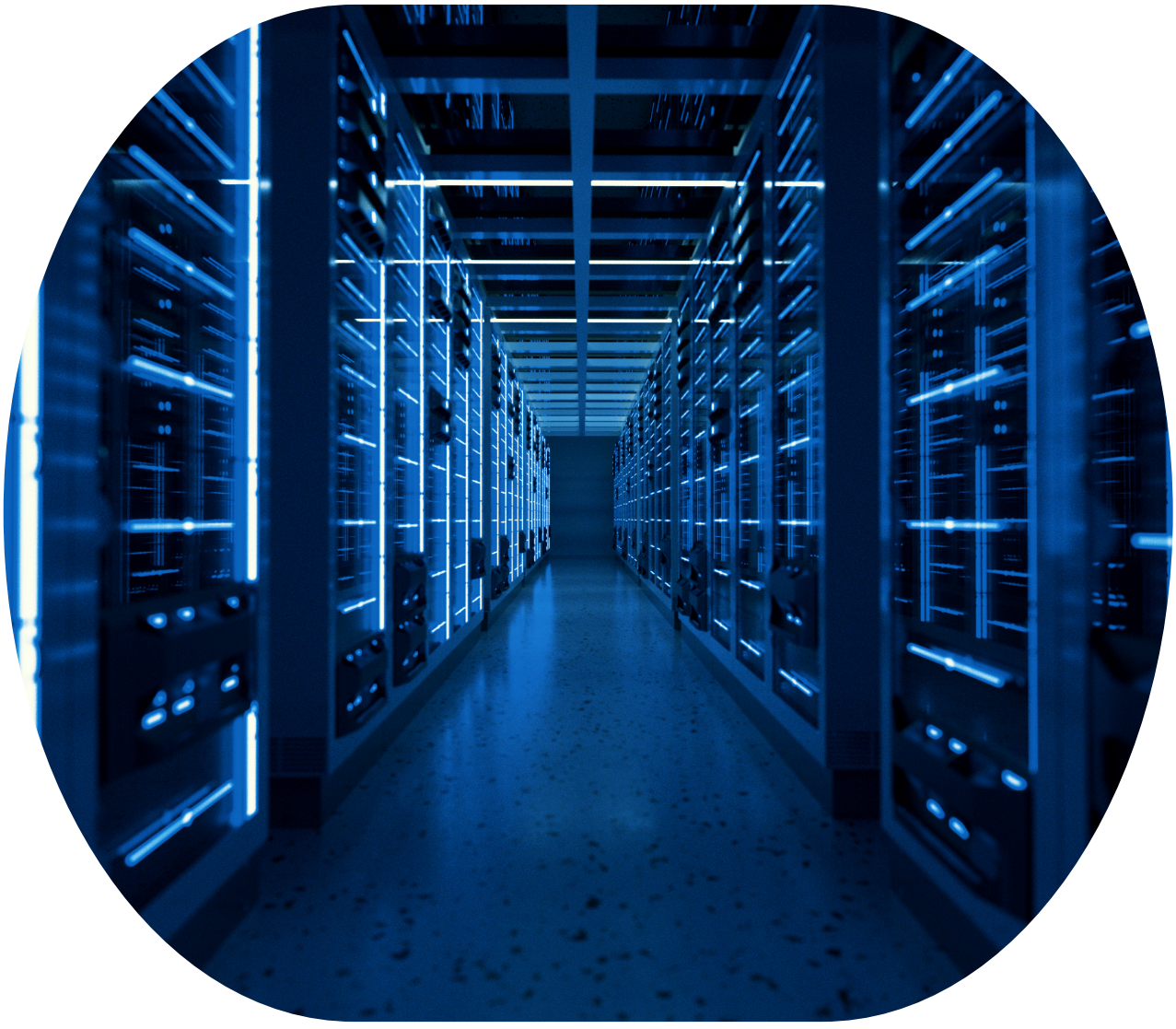
The data archival strategy used by faculties (or even specific research departments) should follow the following general guidelines:

- Before starting a new research project, a Data Management Plan should be prepared that contains, among others, details on data storage and data retention periods[22],[23] (see paragraph 3).
- Decide which data needs to be preserved, keeping the maximisation of reuse of the data at a later point, in relation to the safety of the participants (where applicable), as the main goal.
- If the research data are part of an external collection managed elsewhere by a third party, the UM academic should adequately refer to this and arrange with the owners that they store the data for the minimum period applicable. Alternatively, a local copy can be arranged to be stored within UM's infrastructure.
- Add sufficient documentation to the data, thereby creating a data package, in order to make the data comprehensible to other academics. In doing so, all documentation and data (raw or possibly analysed) that enable research replication are contained together.
- Ensure that preserved data are protected against intended or unintended modification by others, such as editing, overwriting or deleting content.
- Ensure that data are protected against data loss at both the software level (future interoperability) and hardware level (backups).

[22] Please refer to the Netherlands Code of Conduct for Research Integrity: https://www.universiteitenvannederland.nl/files/publications/Netherlands%20Code%20of%20Conduct%20for%20Research%20Integrity%202018.pdf

[23] More on the data retention periods for medical research: https://english.ccmo.nl/investigators/data-retention-periods-for-medical-research and https://www.nationaalarchief.nl/archiveren/kennisbank/selectielijst-universiteiten-en-universitair-medische-centra-2020

- Outline the criteria for granting access to research data, including the individuals eligible for access, the circumstances under which access is permitted, and the corresponding privileges granted to each person involved based on various foreseeable scenarios.
- Assign roles and responsibilities in an archival policy, making clear who is responsible for doing what with the data in the long term. This ensures that data are protected and available for verification purposes after a research project has finished and/or when the academic involved leaves UM.
- If any, follow faculty guidelines on the retention period of non-digital data formats (e.g., paper questionnaires, informed consent forms, etc.).



9. Property

Research data (including software) generated by an academic on behalf of UM in the context of employment, internship or secondment remain the principal property and the proprietary information of UM, unless otherwise agreed in a separate contract with a third party. The academic must ensure that the data remains available for inspection and use by UM at all times during the acquisition and retention period. In joint research projects, data ownership must be agreed upon in a written agreement between all parties at the project's inception. In such cases, a clear delineation of data ownership and rights to future use must be outlined in the research agreement.

10. Retrieval

The academic is responsible for ensuring that all research data contain the necessary metadata, as formulated in the FAIR principles, to understand the data and maximise their potential reuse. Academics must also ensure that data retrieval mechanisms are in place, allowing data access for verification and replication purposes. A protocol for data retrieval should be included in case of emergencies or data loss, detailing steps for recovery and any responsible personnel (see also paragraph 8).

In the event of research where Personal Data is collected, it is recommended, whenever possible, to anonymise the data (the irreversible process of rendering Personal Data non-personal). Details on when data will be anonymised also need to be included in the informed consent form (a binding obligation) that is signed by study participants. Following anonymisation, the research data are no longer subject to GDPR legislation. If anonymisation is not (yet) possible, Personal Data should be pseudonymised by replacing identifying information with random codes or by encryption. In such cases, the Personal Data can still be recovered by using the key-code or the encryption key and the data are therefore still subject to GDPR legislation. The key should always be stored separately from the pseudonymised data in facilities provided by UM or trusted third parties. This must be done at the end of the research project (or earlier depending on the relevant faculty guidelines or other applicable rules).

11. Data sharing and licenses

In line with UM's 2022-2026 Open Science policy and the grant conditions of many national and European funders (e.g., NWO, ZonMw, EU), academics are expected to share their research data in online FAIR-based data repositories, barring any potential conflicts with sensitive data, including, but not limited to, data to which intellectual property, contract or privacy legislation apply. The sharing of research data often takes place in concert with publishing a research paper Open Access[24] or making it available for educational purposes. In cases where intellectual property applies, academics must ensure that UM and/or third parties retain all intellectual property rights by filing a patent application prior to publishing their research or sharing their research data[25]. With regards to privacy legislation, UM academics are expected to handle their research data in a secure and responsible manner compliant with the Data Protection Rules, as explained in more detail in paragraphs 5 and 10. In those cases where intellectual property or privacy legislation prevents the sharing of research data, academics should embrace making the metadata associated with their studies publicly available.

UM encourages the use of FAIR-based repositories for (meta)data sharing. There are many data repositories available to publicly share research data, both general-purpose repositories as well as research field or data type-specific repositories. Regarding the selection of an appropriate general-purpose FAIR-based data repository, DataverseNL[26] is a very suitable candidate for many types of academic research data and it is curated by the UM Library. Regarding data where the GDPR applies, DataverseNL uniquely offers the possibility to deposit pseudonymised data under access request. Any requests for access to the data will then first need to be reviewed by the researchers in charge of the data and subsequently followed up with a Data Transfer Agreement.

It is recommended that academics use the DataverseNL repository to either share the research data or, if another data repository is more suitable for the research data in question or if intellectual property or privacy legislation prevents sharing of the research data, to store at least the metadata and refer to the location of the research data.

[24] Please refer to the Open Access guide: https://library.maastrichtuniversity.nl/research/sharing-output/open-access-guide/
[25] Please refer to the Valorisation guideline for UM/MUMC+ researchers regarding patent application: https://www.brightlands.com/sites/default/files/2020-03/BL_MHC_Valorisation%20guideline.pdf
[26] Please refer to DataverseNL: https://library.maastrichtuniversity.nl/research/rdm/services-tools-training/dataverse/

For those looking for another (field-specific) data repository, FAIR-based repositories should be selected that score high on the following reliability indicators:

- **Stability & Longevity:**

A repository that guarantees long-term data deposition that meets the prescribed retention periods (paragraph 8) and has solid funding and support available.

- **Relevance & Acceptance:**

A repository that is recognised and frequently used within the academic's research community or field.

- **Accreditation & Compliance:**

A repository that possesses a recognised certification like the Core Trust Seal or an equivalent.

- **Data Protection & Access Control:**

A repository that offers clear data access controls, rights management, and security mechanisms to protect sensitive data.

The faculty Data Stewards can be contacted to assist with identifying a reliable FAIR-based repository in case DataverseNL is not suitable.

Any (meta)data shared in a repository should be accompanied by clear usage licenses. When publicly sharing research data or software, by default, it should be deposited with an open mindset, meaning that academics conscientiously opt for a public license type based on the intended use and accessibility of the data, unless prohibited by any of the legal or policy concerns mentioned above. For shared research data, such as non-personal and/or anonymised data deposited in DataverseNL, a Creative Commons (CC) license[27] is required that is as open as possible, while for research software a Berkeley Source Distribution (BSD[28]) or GNU General Public License (GPL[29]) license is prescribed unless a tailored Terms of Use for data or software needs to be drafted in order to comply with research collaborations or legal frameworks. Please consult with a legal advisor if needed.

Sharing data not only supports the (re)use of data in the research field. It also generates opportunities for creating (semi) open educational resources and instigates an attitude shift towards actively considering research data to be used for teaching and learning within UM.

[27] More on Creative Commons licenses: https://creativecommons.org/share-your-work/cclicenses/
[28] Please refer to BSD license information: https://opensource.org/license/bsd-3-clause/
[29] Please refer to GPL license information: https://www.gnu.org/licenses/gpl-3.0.html

12. Use of non-public research data by other academics

If an academic from UM or another institution or company wishes to access specific research data that are not openly available in public repositories under a Creative Commons license (e.g., pseudonymised data under access request or data sets where only metadata are available), the UM academic (or their representative) has the authority to approve or decline the request. Approvals should always be made while taking into account any potential conflicts with intellectual property, privacy legislation or other limiting factors and, if the request is approved, a Data Transfer Agreement should be drawn up describing the type of data, the permitted use, and the protection of the data[30],[31]. Depending on the situation, a Confidentiality Agreement may also be necessary. The (local) privacy team or the faculty Information Managers[32] can be contacted for assistance with drawing up such agreements and they should be signed by the faculty Dean.

13. Inspection of research data by a non-mainstream third party

Should a non-mainstream third party wish to inspect UM research data, the Dean of the faculty in which the involved UM academic(s) are/were appointed is authorised to grant permission. The Dean will, to the best of his/her ability, consult with the academic(s) involved and/or the current data assignee before granting permission, with the interests of the academic(s) in mind. The Dean may set additional conditions to this request procedure.

14. Additional faculty guidelines

The faculty Dean reserves the right to implement additional faculty guidelines governing RDM. Such guidelines should be in line with the UM Open Science policy. Depending on the topic(s) on which the faculty Dean wants to expand, contact will have to be made with relevant specialists to discuss the possibilities and conditions for expansion.

[30] Please refer to the Valorisation guideline for UM/MUMC+ researchers regarding a DTA in terms of IP: https://www.brightlands.com/sites/default/files/2020-03/BL_MHC_Valorisation%20guideline.pdf
[31] Please refer to the UM Policy on the Processing of Personal Data regarding a DTA in terms of privacy law: https://www.maastrichtuniversity.nl/file/um-beleid-verwerking-persoonsgegeven091019enpdf
[32] Please refer to the RDM faculty contacts to find each faculty's Information Manager: https://library.maastrichtuniversity.nl/research/rdm/faculties/

15. Questions

In the paragraphs above, contacts or links with additional information are mentioned for the most important aspects of RDM. However, if those contacts or links are not sufficient to answer certain questions, academics can always contact the UM Open Science Officer or Chief Open Science[33].

This code of conduct has been approved by the UM Executive Board on 28 May 2024

[33] Please refer to the UM Open Science Officer or Chief Open Science contacts here: https://www.maastrichtuniversity.nl/research/open-science

Maastricht University

Contact:

Maastricht University Library

Chief Open Science:

marielle.prevoo@maastrichtuniversity.nl

Open Science Officer:

d.hebels@maastrichtuniversity.nl