ISiS's Policy for Research Data Management

Approved in December 2024 by the director of ISiS Prof. H. de Regt and the ISiS Board.

Written by: Riyan van den Born & Rob Lenders, Data Stewards ISiS from 2023-2024

RDM at ISIS at a glance

- **Contact the data steward** at isisdatasteward@science.ru.nl with any questions regarding research data management.

Before research

- Write a **data management plan.** This can be done at the beginning of a research project, or if required by the funder, upon submission of a project.

- If processing **personal data**:
  - Follow the GDPR throughout the entirety of the research process.
  - Contact the local privacy officer before the data collection has started to fill out a **pre-DPIA** (Data Protection Impact Assessment) if processing personal data.

- Check https://www.ru.nl/en/about-us/organisation/faculties/science/research/ethics-committee to see if the research proposal needs to be reviewed.

- Check the Digital Competence Center on gROW to see what **RDM courses** are relevant for you.

During research

- **Store and share** research data using the Radboud Data Repository / Microsoft 365 Team / workgroup folder / SURFdrive.

After research

- **Archive or publish** research data in the Radboud Data Repository for a minimum of ten years accompanied by sufficient metadata and documentation.

- Use **CC0 licence** when publishing the research data unless there are legal or ethical constraints.

- **Register the archived or published dataset** in Radboud University's Research Information Services (RIS) here, unless it was archived with public metadata or published in the Radboud Data Repository, in which case this happens automatically.

- **Store other forms of research-related data,** that are not suited for archiving in a repository (e.g. consent forms and encrypted keyfiles), in a workgroup folder.

Table of Contents

Definitions

For whom this policy is intended

The ISiS's Policy for Research Data Management applies to anyone who performs research at ISiS (hereafter referred to as researcher). This means that this policy is not intended for external collaborators from other institutes or universities, however it does apply to external PhDs and emeritus professors.

This policy does not replace, but rather expands upon the **Radboud University Guidelines for Research Data Management** (hereafter referred to as Guidelines for RDM) and the Netherlands Code of Conduct for Research Integrity.

Roles and responsibilities

The roles and responsibilities for good research data management are outlined in the Guidelines for RDM. This responsibility is shared between the Director of Research, the data steward, and the researcher.

The **Director of Research** is responsible for the development, implementation, and compliance of this policy.

The tasks of the **data steward** are outlined in Appendix 2 of the Guidelines for RDM. The data steward assists in the compliance with the RDM Policy within the institute and monitors this compliance within the institute on a regular basis.

All **researchers** are responsible for effective and accurate data management and must therefore familiarise themselves and adhere to this policy. **PhD candidates** must additionally adhere to the Radboud University Doctorate regulations and are responsible for the data they collect for their dissertation, together with their supervisors. PhD students whose research does not concern personal data, are also expected to make a DMP as part of the procedure in Hora Finita, but can indicate that they don't have personal data and that many sections are then 'not applicable' to their research.

Compliance with policy

PhD supervisors are responsible for monitoring compliance with the ISiS's Policy for RDM by checking whether data management plans are filled in; repositories are used for archiving and publishing, etc. In case of non-compliance the supervisor or data steward informs the ISiS's Director of Research. Together they can decide which actions are necessary to address this non-compliance.

ISiS will review the ISiS's Policy for RDM and revise it in consultation with the Radboud University Digital Competence Centre every two years.

Control of research data

In general, as outlined in the Radboud University Guidelines on control of research data, research data generated by employees is controlled by Radboud University. This means that Radboud University is authorised to exercise their rights to this research data. When research data is generated in collaboration with other institutions or externally funded, other arrangements may exist. If it is not clear to the researcher who controls the research data or if the researcher has any questions, they should contact Administration & Legal Affairs.

Research data

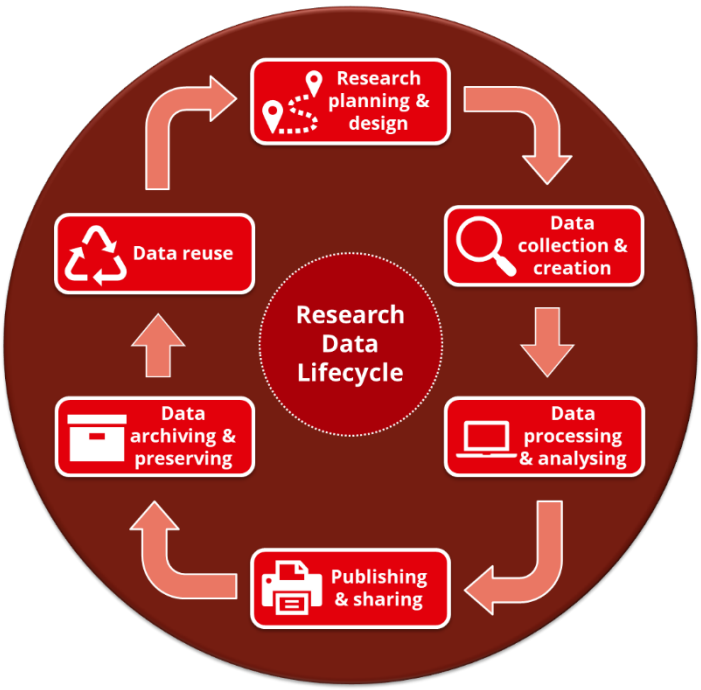
The definition of research data includes:

All information, digital and non-digital, that was generated during the research process and used to form scientific conclusions. This encompasses information that is used for forming and testing hypotheses as well as information upon which conclusions are based. If the information contributed to results in a scientific report, it is research data[1]. At ISiS, typical data takes the form of (but is not limited to) interview data, focus group data, survey data, or participatory observations.

Research software falls out of/within scope of this policy and is not addressed here.

Research data management

As the name indicates, research data management (RDM) is the management of research data along the research life cycle (see Appendix). RDM includes a variety of activities such as planning, collecting, processing, analysing, archiving, and publishing.



Having good RDM has **many advantages**. It allows the researcher to make informed decisions about the research data and helps to keep the research project organised. This means that the researcher can keep the data safe, prevent unauthorised access, and avoid data loss. Moreover, the researcher can save time, conform to standards of scientific integrity, adhere to open science principles, and encourage the reuse of data.

Open Science

Open Science[2], is a movement in which academic outputs such as data and publications are made available as openly as possible, encouraging reuse. Open Science is becoming more prominent in research. By practicing Open Science, research becomes more reliable and transparent. In addition to this, research becomes more impactful as reuse of data is encouraged. Good RDM can contribute to Open Science and make data as open as possible by encouraging researchers to follow associated practices from an early stage in the research data lifecycle. Additionally, researchers can make use of already existing and available data instead of, or in addition to, collecting new research data.

Data Management Plan (DMP)

A data management plan (DMP) includes information about the whole research life cycle, allowing the researcher to make informed decisions about all aspects of their RDM. Writing a DMP helps the researcher to plan how research data will be handled during each phase of the research life cycle. The benefits of writing a DMP are therefore in line with good RDM as mentioned above; keeping research data safe by preventing unauthorised access and data loss, saving time by being organised, and enabling open science.

[1] The definition of research data was inspired by the definition provided in the Radboud Data Repository.
[2] For more information on Open Science in the Netherlands, see NWO's website.

Many funders require a DMP or data management paragraph. Here at ISiS, we recommend that if required, researchers write a DMP. This can be done at the beginning of a research project, or if required by the funder, upon submission of a project. DMPs **must** be created by logging in to Research Information Services (see Guidance) and using the ISiS's template. All researchers are additionally **required** to request feedback of the data steward on their DMP. DMPs are living documents that **must** be adapted by the researcher whenever plans change. If a DMP is updated substantially, it receives additional feedback.

Storing and sharing

This section describes where the researcher can **safely** store and share the data **during their research**. In contrast, the next section on archiving and publishing explains where to archive the research data for the long-term (e.g., after the research is complete or published in an academic publication).

Storing and sharing options

At ISiS the researcher can safely store their data on the Radboud Data Repository. During research, when still working with the data, the researcher can use using the following options:, Teams, an ISiS workgroupfolder, SURFfilesender, or in consultation with data steward at other locations. Each option is outlined in more detail below. When sharing data or collaborating, researchers should follow data minimisation and **access control** practices, meaning that they should manage who has access to what, and who has viewing or editing rights.

1. **Radboud Data Repository**: ISiS uses the Radboud Data Repository (RDR). The researcher is to store research data in their original form[3] in a Data Acquisition Collection and the documentation and research data which is created from the moment of acquisition to publication in a Research Documentation Collection (see Guidance)[4]. The RDR can be used to safely share with fellow researchers (and students) at Radboud University as well as with external researchers. The RDR is not to be used for work-in-progress when multiple people access the same files simultaneously.

2. **Microsoft 365 Teams**: A researcher at ISiS can use a Microsoft 365 Team (see Guidance) to store their data during their research as well as collaborate with internal and external individuals. When creating and using a Microsoft 365 Team, the researcher **must** use their Radboud account, and **not** a personal account. Further, the researcher is **required** to disable the synchronisation setting in a Microsoft 365 Team. Be aware that Microsoft 365 Teams and OneDrive are not the same. OneDrive is not an option for storing and sharing, since it is for personal documents, and not research data.

3. **Workgroup folder**: Researchers at ISiS can use a Radboud University network drive – workgroup folder – to store their data during their research and collaborate with internal researchers (and students) (see Guidance).

4. **SURFfilesender**: If the researcher is looking to share files in a safe manner, they can use SURFfilesender. Personal data **must** be encrypted when shared via SURFfilesender (see Guidance).

In case none of these solutions meet the researcher's needs, for example if the researcher is collaborating with colleagues at institutes who use different storage locations, the data steward should be contacted. Together with the researcher the data steward will investigate the best solutions that fit the researcher's needs.

[3] The original form is the version of the data that has not yet been manipulated.
[4] The definitions here are inspired by the RDR.

Prohibited options for storing and sharing

Storing and sharing research data using the following means is **not allowed**[5]:

- **Personal commercial cloud drives** such as *Google Drive* and *Dropbox*. Commercial cloud services may be situated outside of the European Union and therefore other regulations and laws may apply to them. Further, cloud services may claim rights to the data that they store.
- **Commercial services** such as *WeTransfer*. These are not allowed for the same reasons as given for commercial cloud services above.
- **External drives** such as *USB drives, SD-cards,* and *external hard drives*. These are discouraged since they can easily be lost. If a researcher needs to use an external hard drive, SD-card or USB drive, they **must** make sure that:
    - they are encrypted[6].
    - the amount of time that data is stored on these devices is limited.
    - the data are backed up in a recommended storage location as soon as possible.
- **Mobile phones** should be avoided (e.g., as recording devices) for storage or sharing since oftentimes they are connected to a cloud and therefore not recommended for the same reasons as given for commercial cloud services.

Non-digital data

Any non-digital (research) data (e.g., hand taken notes, consent forms) **must be digitised** as soon as possible (inspired by the DIV and Archive Management Guidelines). When digitising documents, the paper originals need to be securely stored in a locked cabinet for six months, after which they can be (confidentially) disposed of. These six months give the researcher time to fix any issues, such as skewed, missing, or unreadable pages that may be present in the digitalised version. If it is not possible to digitise the paper documents, or artifacts from fieldwork, then the researcher **must** store these in a locked cabinet where only authorised personnel can access them. The one exception to these substitution guidelines is consent forms from WMO obligated research, for which the non-digital forms **must** be preserved for 15 years (25 years in case of clinical trials).

Archiving and publishing

Archiving and publishing are relevant throughout a research project, whenever research data needs to be preserved for the long-term. In line with the requirements of the Guidelines for RDM, ISiS sees to it that upon archiving and publishing research data, pertaining to scientific publications are **findable** and **accessible** as outlined by the **FAIR principles**[7] [8] [9]. Having the data be findable and accessible ensures:

- the integrity and reproducibility of research
- the potential of research data reuse
- the recognition and accountability of the involved researchers

Furthermore, ISiS encourages researchers to ensure that their research data is additionally both interoperable and reusable. By archiving or publishing your data in one of the ISiS's approved repositories, you will be able to abide by the findability and accessibility principles in FAIR.

[5] See "Sharing and storing files safely" where "Unsafe storage locations" are specified for sensitive data.

[6] For advice with regard to encryption and digital security researchers can contact the ICT Helpdesk.

[7] See the Radboud University Guidelines for Research Data Management (2023): "In the case of scientific publications that are based on research data, of which one or more Radboud University researchers are authors, it should be evident how the corresponding data can be found and the access management should be well-organised."

[8] See GO-FAIR and Wilkinson et al. (2016) for a full overview of these principles.

[9] As is stated in the Radboud University Guidelines for Research Data Management (2023): "Findability means that research data can be found in a simple, unambiguous and sustainable manner, both within and outside the organisation, also by persons other than the researcher him or herself... Accessibility is not about making research data accessible to everyone at all times, but about the proper regulation and registration of the conditions under which it is possible to access the data and how this can be done..."

For the sake of **transparency**[10] and **scientific integrity** it is vital that research data can be independently verified to exist and is described in sufficient detail to enable replication of the data collection and analysis. All newly generated research data that underpins a scientific publication at ISiS must therefore be archived or published for a **minimum of 10 years** in a trusted repository, such as the RDR.[11] in a manner that allows continued understandability of the data over time. It is recommended that the researcher uses a persistent identifier such as an ORCiD when archiving and publishing the data. This ensures that all the researcher's output is connected to them with a single identifier, enabling FAIR practices.

This repository must be used for the data in their original form[12] and the documentation and data which is created from the moment of acquisition to publication. Archived or published research data **must** always be supplemented with sufficient **metadata**[13] and other **documentation** so that the entirety of the research process – from data acquisition to publication – is sufficiently contextualised.

Furthermore, whenever existing (secondary) research data are used, these **must** be properly referenced with a persistent identifier, such as a DOI, that refers to the location where the research data can be found. Researchers should be aware that if they archive or publish research data with the publishers of their academic publications, this may give publishers exclusive ownership of the data. For this reason, archiving or publishing research data with the publishers of an academic publications is not recommended.

Archiving and publishing options

The **required** archiving and publishing location for research data at ISIS is the **Radboud Data Repository (RDR)**. The researcher **must** archive the research data in their original form[14] in a Data Acquisition Collection and / or the research data that is created from the moment of acquisition to publication in a Research Documentation Collection (see Guidance)[15]. The data that are made available for reuse or replication studies **must** be placed in a Data Sharing Collection (DSC).

If the researcher wishes to archive or publish the research data in a different repository, they **must** first discuss whether this is possible with the data steward. Before the researcher can proceed to archive or publish the research data at this repository, the data steward will assess if it guarantees long-term preservation, provides adequate security, and adheres to the FAIR principles.

Prohibited archiving and publishing options

Archiving research data using the following means is **not allowed**:

- **Cloud drives** such as *Microsoft Teams, OneDrive, Google Drive* and *Dropbox*.
- **External drives** such as *USB drives, SD-cards,* and *external hard drives*.
- **Local servers** such as workgroup folders.

These options do not conform with the FAIR principles, impeding the findability and accessibility of data. They also do not guarantee the minimal retention period of data and some of them create risks for data loss or data breaches.

[10] The Netherlands Code of Conduct for Research Integrity (2018) mentions how transparency means, among other things, ensuring that it is clear to others what data the research was based on, how the data were obtained, what and how results were achieved and what role was played by external stakeholders.
[11] A trusted digital repository has been defined in Trusted Digital Repositories: Attributes and Responsibilities (2002), as a repository whose "...mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future." A researcher can recognize if a repository is trustworthy by having the following attributes: i.e., having online policies and a preservation plan, being approved by ISiS, or by being certified
[12] The original form is the version of the data that has not been manipulated.
[13] Metadata refers to documentation and/or other information concerning research data, which is required to find and understand the content and context of the data.
[14] The original form is the version of the data that has not been manipulated.
[15] The definitions here are inspired by the RDR.

Retention period

Following the Guidelines for RDM research data generated at ISIS that support a publication must be archived or published for a minimum of ten years after publication[16]. There can be exceptions to this rule, for example when data are not owned by the Radboud University, in case of specific agreements with third parties, or when privacy regulations make compliance with this rule impossible. This term starts from the first moment of publication of research based on the research data.

Access levels and licenses

In accordance with the Guidelines for RDM, the default for publishing research data at ISiS is to make the data publicly available, **as open access as possible, as closed as necessary**[17] [18]. This means that, as long as there are no legal, ethical, or contractual constraints, research data **must** be published under a CC0 license. Publishing research data as open access introduces the fewest barriers and thus maximises the potential for reuse of the research data.

While there can be valid reasons to deviate from this default of open access, these exceptions are limited to ethical concerns, privacy limitations, security issues, contractual agreements, and other serious grounds. In these cases other access levels might be required:

- **Registered access:** If the research data are potentially identifiable or pseudonymised[19].
- **Restricted access:** If the research data are directly identifiable or sensitive[20].
- **Closed access:** If the research data cannot be shared because there is no permission, or if the data are too sensitive.
- **Embargo:** If the research data are being used for a patent or another publication then there could be an embargo until all intended publications based on these data are published.

In the case that the data cannot be shared open access, it may still be possible to share the metadata openly. Whenever this is possible, it is encouraged, since doing so helps to make the data FAIR.

Whether data can be published and what the most appropriate access level is should be determined in conversation with research participants, supervisors, research collaborators, and the data steward before data collection begins. This allows the research participants to make an informed decision about their participation.

Registration

Once a dataset is archived or published, it should also be **registered** in Radboud University's Research Information Services (RIS). If the dataset is archived in the RDR this happens automatically when the metadata is made public or when a dataset is published. Registering datasets gives exposure to the research and links the research data with related scientific output such as publications or presentations. At ISiS this registration is done by the researcher (see Guidance).

Research-related data

There are **other forms of research-related data** that are not suited for archiving or publishing in a repository but must be stored regardless. These research-related data include but are not limited to: administrative personal data that the researcher collects and cannot dispose of during the course of their research, data

[16] See the Radboud University Guidelines for Research Data Management (2023): "The minimum retention period for research data that is required for checking or verifying scientific publications is ten years from the time that the scientific publication is available."
[17] See the Radboud University Guidelines for Research Data Management (2023): "Research data should be archived as open as possible, as closed as necessary. The starting point is that research data should be made publicly available."
[18] According to https://www.openaccess.nl, open access is a broad international movement that seeks to grant free and open online access to academic information, such as publications and data. A publication is defined 'open access' when there are no financial, legal or technical barriers to accessing it - that is to say when anyone can read, download, copy, distribute, print, search for and search within the information, or use it in education or in any other way within the legal agreements.
[19] See section below on Personal data.
[20] See section below on Personal data.

related to the informed consent process, and encrypted keyfiles that must be preserved for pseudonymous datasets. These other forms of research-related data must be stored in an ISiS workgroup folder, in line with the following requirements: preferably in the folder on the ISiS drive that is created for the specific project, for instance in the running projects or the PHD project file.

Personal data

In the process of doing research at ISiS, it is common that researchers collect, analyse, or otherwise process[21] **personal data**. This refers to information that can either directly identify a living individual or which, when combined with other information, can be traced back to a living individual[22]. Personal data can be present within the research data itself, but also in administrative data or in the information related to the informed consent process. Whenever this is the case, the personal data in the research becomes subject to the General Data Protection Regulation (GDPR). The researcher, in their role as controller[23], joint controller, or processor[24] of this personal data, must be able to demonstrate compliance with this regulation. In order to comply with the GDPR, researchers **must** familiarise themselves with the GDPR, e.g. through courses, information provided by the Radboud University (on privacy or on RDM), or via the GDPR itself. The researcher is expected to take into account the consequences that this regulation has for their research throughout the entirety of the research process, from research planning to data acquisition to data publication.

This means, among other things, that data containing personal data can only ever be collected, analysed, or otherwise processed when a clearly defined legal basis exists, such as informed consent, public interest, or legitimate interest. Furthermore, participants must be made aware of their privacy rights, in particular the right to be informed[25] and the right to be forgotten[26]. Finally, when sharing data or collaborating, researchers should also follow **data minimisation** practices, meaning that they should only store and share personal data that is required for the research project.

Anonymisation

Researchers are encouraged to anonymise the personal data in their research project **as much and as soon as possible**, as this effectively removes the personal data from the dataset and significantly reduces the privacy risks. If the researcher chooses to anonymise research data then this should be detailed in the informed consent. A dataset is considered anonymous if it is no longer possible to identify any of the participants in any way[27]. To be considered anonymous, a dataset must not contain any direct identifiers[28] that can be linked to participants in the data, metadata[29], or documentation. Furthermore, the risk of

[21] The General Data Protection Regulation (2018) describes processing as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
[22] According to the General Data Protection Regulation (2018), 'personal data' means any information relating to an identified or identifiable living natural person.
[23] The General Data Protection Regulation (2018) defines the controller as a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. When there are two or more controllers the GDPR speaks of joint controllers and arrangements must be made to share responsibility for GDPR compliance.
[24] The General Data Protection Regulation (2018) defines the processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. A processor thus carries out specific processing instructions and activities for the controller.
[25] More information on the right to be informed can be found here.
[26] More information on the right to be forgotten can be found here.
[27] The General Data Protection Regulation (2018) advises that, to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. Using these means it may be possible to identify someone, for example through the singling out of individuals, the linking of records or the inference of information.
[28] According to the General Data Protection Regulation (2018), an individual is directly identifiable if you can identify them using nothing but the information you possess. This would for example be a name, photo, video or audio recording.
[29] See footnote 8.

identification via combinations of indirect identifiers[30] or via combinations of different datasets must be sufficiently reduced in order to make re-identification effectively impossible. When a dataset is anonymised it is not considered personal data and is, therefore, not subject to the requirements of the GDPR.

Pseudonymisation

Pseudonymisation[31], while not removing the personal data, is an alternative to anonymisation by which the privacy risks of a data breach can be reduced. Researchers should be aware, however that pseudonymisation keeps the link between personal data and the participant intact, meaning that pseudonymised data are still considered personal data and thus subject to the requirements of the GDPR.

Whenever it is impossible to effectively anonymise or pseudonymise a dataset, for example when this would result in excessive loss of relevant information, the identifiable research data **must** be archived or published under the conditions specified in the informed consent. Researchers must therefore plan under which conditions they intend to archive or publish the data prior to acquiring informed consent, so that they can inform their participants about the data archiving and publication strategy.

Ethics and informed consent

There are certain circumstances that require ISiS researchers to submit their research proposal for review to the Research Ethics Committee (REC)[32]. The researcher **must** consult the ethics committee website to know if they need to send their research proposal in for review before they start with the data collection for their research. Further, the researcher must consult the ethics committee website for information on informed consent – when it is needed and how to properly accomplish this.

Support and training

Contact information

The ISiS's data steward can be contacted at **isisdatasteward@science.ru.nl** if there are any questions about ISiS's Policy for Research Data Management or any other questions related to research data management.

Training

The Radboud University provides a range of training opportunities to help researchers comply with this Policy and develop skills with research data management. The Radboud University Digital Competence Centre provides a **variety of workshops**. Participation in these workshops is encouraged for all researchers. Upon request the Radboud University Digital Competence Centre can also offer **tailor-made workshops**.

[30] According to the General Data Protection Regulation (2018), an individual is indirectly identifiable when you are able to identify a person by using other information you hold or information you can reasonably access from another source. Research data can be archived or published under the conditions specified in the informed consent. Researchers must therefore plan under which conditions they intend to archive or publish the data prior to acquiring informed consent, so that they can inform and obtain consent from their participants about data archiving and publication.

[31] The General Data Protection Regulation (2018) describes pseudonymisation as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

[32] See https://www.ru.nl/en/about-us/organisation/faculties/science/research/ethics-committee. Researches can also contact the REC's secretary: secretarisrec@science.ru.nl.

Appendices

Appendix: Sources

- Bestuurlijke en Juridische Zaken & Bureau Documentaire Informatievoorziening / Archief (DIV). (2016). *Handboek Substitutie. Verantwoorde opslag en beheer van digitale en gedigitaliseerde archiefdocumenten.* Radboud University. https://www.radboudnet.nl/publish/pages/533842/handboek_substitutie.pdf

- EU General Data Protection Regulation (GDPR): *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

- GO FAIR initiative. (2017). *FAIR Principles - GO FAIR*. GO FAIR. https://www.go-fair.org/fair-principles

- KNAW; NFU; NWO; TO2-federatie; Vereniging Hogescholen; VSNU (2018): *Netherlands Code of Conduct for Research Integrity*. DANS. https://doi.org/10.17026/dans-2cj-nvwu

- Radboud University (2016). *Guidelines on control of research data.* https://www.ru.nl/en/about-us/policies-and-regulations/research-data-management/guidelines-for-control-of-research-data

- Radboud University (2024). *Radboud Data Repository User Manual.* https://data.ru.nl/doc/help/helppages/user-manual.html

- Radboud University. (2023). *Guidelines for Research Data Management*. https://www.ru.nl/en/about-us/policies-and-regulations/research-data-management/guidelines-for-research-data-management

- Radboud University. (2024). *Doctorate regulations 2024.* https://www.ru.nl/en/regulations/doctorate-regulations

- Radboud University. (2024). *Manuals Research Information Services.* https://www.ru.nl/research-information-services/manuals-ris

- Research Libraries Group. (2002). *Trusted Digital Repositories: Attributes and Responsibilities*. https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

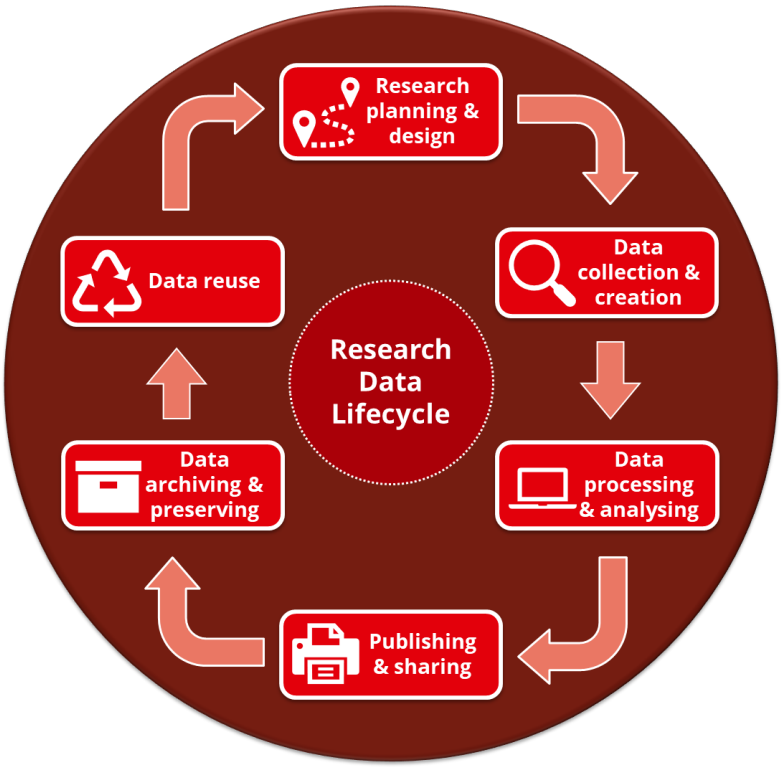
- The working party on the protection of individuals with regard to the processing of personal data (2014). *Opinion 05/2014 on Anonymisation Techniques.* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

- Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J., Da Silva Santos, L. O. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T. W., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., . . . Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, 3(1). https://doi.org/10.1038/sdata.2016.18

Appendix: The research data life cycle

Research planning and design

In this phase, researchers specify the data to be collected in order to answer their research inquiry and devise a plan for managing the data throughout its life cycle. During this phase researchers tend to finish the study design, write a data management plan, and complete an ethics review.



Data collection and creation

This phase involves conducting experiments, making observations, doing interviews, conducting surveys, and acquiring secondary materials. Documentation of data collection, instruments and methods, along with information essential for data interpretation, is crucial during this phase.

Data processing and analysing

Data analysis is the phase where research materials are examined to generate insights that result in the research findings. The instruments, methods, code, or visualizations used for analysis should be documented and might need preservation for support of written or published research outputs.

Publishing and sharing

During this phase, publications based on data should include a statement indicating where and under what terms the data can be accessed.

Data archiving and preserving

Towards the conclusion of the research process, it is essential to preserve data that substantiates the research findings. Proper archiving of data in a data repository is the key to improved integrity and reproducibility of research and the re-usability of research data, now and in the future.

Data re-use

Data available for discovery and access can be re-used by other researchers, either to validate original findings or to generate new insights. At this phase, the data may serve as raw materials for a new research cycle. There may also be applications for research data in policymaking, commercial product and service development, and teaching.