Arnold-
Bergstraesser-
Institut

ABI Research Data Management Policy

March 2025

Contents

This Policy and Guideline document has been developed by Dr. Martin Adelmann (ABI Data Protection Officer, Executive Manager) and Dr. Franzisca Zanker (ABI Deputy Director) in March 2025. It serves as a binding reference framework for ABI staff.

Arnold-Bergstraesser-Institut e. V. Freiburg
Windausstraße 16, 79110 Freiburg im Breisgau
Homepage: www.arnold-bergstraesser.de

Arnold-
Bergstraesser-
Institut

About Research Data Management (RDM) at the ABI

The Arnold Bergstraesser Institute is committed to the responsible handling of research data throughout the entire research process. This includes research planning, data collection, data storage, data processing, publication and archiving of data.

Researchers at the ABI are committed to adhering to established standards in the field of RDM. This includes in particular the *DFG Guidelines for Safeguarding Good Research Practice* (implemented through the *Satzung des ABI zur Sicherung guter wissenschaftlicher Praxis und zum Umgang mit Verdachtsfällen wissenschaftlichen Fehlverhaltens)* and the *DFG Checklist of Handling of Research Data.* Moreover, researchers must comply with the statutory data protection provisions in accordance with the German *Bundesdatenschutzgesetz* (BDSG) and European General Data Protection Regulation (GDPR). The FAIR principles, see also below, serve as additional guidelines.

ABI Data Protection Officer: Dr Martin Adelmann

Contact: martin.adelmann@abi.uni-freiburg.de

RDM Structure and Procedure at the ABI

The responsibility for RDM lies with the respective researchers. The project leader is responsible for the RDM of their research team. Researchers are advised and supported by the ABI Data Protection Manager (hereafter DPO). In addition, the ABI provides information and resources for needs based training on RDM.

At the beginning of each project, ABI researchers are required to complete a research data management plan. The plan will be reviewed by the DPO, amended if necessary, and then stored by the DPO. Staff are strongly encouraged to revisit the data management plan regularly during the project period, to ensure that data-protection measures stay up to date with technological developments, legal requirements and ethical considerations.

Arnold-
Bergstraesser-
Institut

Data Management Plans may differ in form, depending on the requirements of respective funding organisations and nature of the project. Notwithstanding this, each Data Management Plan should give basic information about the project title, funding agency, responsible researcher including contact information, date of first version, and date of last modification.

The following guidelines serve as an overview of the core requirements and most important questions that all researchers should address in their Data Management Plan.

Data Management Plan Guiding Questions

Part 1: Data Overview

In order to assess how to make data accessible (see Part 2 below) and how to collect and store it securely (see Part 3 below) it is necessary to get an overview of the planned data. Researchers need to consider the following questions for each project:

1) What is the purpose of data collection?
2) What is the utility of the data (i.e. to whom may it be of interest)?
3) What is the expected data that will be collected? Include information on the origin (e.g. what method and research participants), data type, format (.docx, .txt, .pdf, .jpg, .png, .avi, .mp4, .mov, .wav or .mp3), and expected size of the data. It is possible to summarise this information in a table.
4) What are the costs of data management and how will these costs be covered (e.g. project funds, institutional resources).

Part 2: FAIR Data Collection

Data collection should follow the principles of **FAIR** – making data **f**indable, **a**ccessible, **i**nteroperable and **r**eusable. The idea is to make data available as a benefit to science and society in general, following the idea that data must be "as open as possible, as closed as necessary". In other words, particularly sensitive data – including, for example, on political and religious beliefs – does not have to be made available and the decision to share data openly should be carefully assessed to ensure that it aligns with legal and ethical regulations and does not compromise anonymity of research participants.

Taking this into account, and considering all the types of different data collected for a research project:

5) How are the data made **findable**, including provisions for metadata?
    a. What are the metadata features (standard and additional descriptive data) and how will these be documented?
    b. What are the naming conventions for data documents generated throughout the project (e.g. do they comply with the standards of Dublin Core Metadata Initiative or the Data Documentation Initiative)?
    c. How is the findability of internal documentation ensured? (Such as through name, date format, versioning etc.)
    d. Where is the naming conventions for data that is openly accessible documented (e.g. codebooks)? Relatedly, how will the application of a unique and persistent identifier (e.g. DOI) to each datset be ensured?

6) How are data made openly **accessible**, e.g. in a repository or similar?
    a. How can the data be accessed (i.e. are relevant tools/ methods provided)?
    b. If data is not made accessible, what are the reasons for this?

7) How **interoperable** are the data, e.g. what kinds of standard/ field-specific vocabulary methods are used?

8) How **reusable** are the data, e.g. when (e.g. prior or after publication) and how long will the data be made available for?
    a. What kind of provisions are there to licence the data? (e.g. a CC BY-NC license, ensuring non-commercial reuse with attribution)
    b. What will be the terms of use for your data, with whom will they be shared?
    c. What are the quality assurance procedures for the data (e.g. training, monitoring, field reports)?

Part 3: Data Security

It is vital that data remains secure, during collection, transfer and long-term storage. It is important to remember the principles of 'data minimisation' to ensure that no unnecessary data is collected as well as to what degree the collection of sensitive data according to art. 9 of the General Data Protection Regulation 2016/679, is strictly necessary. Measures related to informed consent, pseudonymisation and anonymity are further discussed in the ABI Ethical Review Form Section 6.

9) What local data protection regulations are applicable to the project and what measures need to be drawn from this?
10) What kind of measures are taken to make sure everyone in the research team follows the correct procedures for data management during the collection process (e.g. training)?
11) How is unauthorised access to personal data and other sensitive data prevented (e.g. names and phone numbers)?
12) How will data be stored during the collection period and transferred and what measures are made to keep it secure? Are there any measures for encryption?
13) How long will data be stored and backed up during the research process?

Part 4: Data Archive

Research data should be archived in a way that they are save and easily accessible for at least 10 years after the end of the research.

14) How long and where will data be achieved (e.g. on a secure server, hard drive, data repository)?
15) Who will have access to the archived data?

Sources

For further information, please consult also the following documents:

- Deutsche Forschungsgemeinschaft, Hrsg., „Handling of research data. Checklist for planning and description of handling of research data in research projects", 21. Dezember 2021, https://www.dfg.de/download/pdf/foerderung/grundlagen_dfg_foerderung/forschungsdaten/forschungsdaten_checkliste_en.pdf.
- Deutsche Forschungsgemeinschaft, „Guidelines for Safeguarding Good Research Practice". https://wissenschaftliche-integritaet.de/en/code-of-conduct/. July 2019.
- Bundesministerium der Justiz: Bundesdatenschutzgesetz (BSDG). 25.05.2018. https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html
- „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 (General Data Protection Regulation) (Text with EEA relevance)" (2016),
- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.
- Mark D. Wilkinson u. a., „The FAIR Guiding Principles for Scientific Data Management and Stewardship", Scientific Data 3, Nr. 1 (Dezember 2016): 160018 https://doi.org/10.1038/sdata.2016.18.
- Data Protection Africa Website. https://dataprotection.africa/