

HERTIE SCHOOL RESEARCH DATA MANAGEMENT POLICY

PREAMBLE AND STATEMENT OF PRINCIPLES

This policy sets the research data strategy that helps guide researchers and units within the Hertie School in how to best manage, analyse, safeguard and act upon their collected research data, to help inform decision-making and foster best data practices. This Research Data Management Policy serves as a tool for the benefit of Open Science, in accordance with the recognised principles of good research and best practices. Research data management must be effective, safe, and consistent, and, whenever possible, be in accordance with the FAIR principles: findable, accessible, interoperable, and reusable.

The aim of this policy is to:

1. Provide sufficiently detailed but feasible guidance on research data management
2. Inform on how to safeguard and protect data that has been collected and processed
3. Provide for a well-defined procedure for managing data
4. Provide details of different units involved in the data management process
5. Demonstrate a link to the research ethics policy and review mechanism
6. Emphasise our commitment to Open Science and Open Access

All researchers at the Hertie School are committed to the secure storage, processing, preservation, sharing and publication of their research data. Each researcher is responsible for complying with the Hertie School's Code of Conduct and the Hertie School Research Ethics Review Policy, which integrate and make binding good ethics research principles and conduct, in line with the German Research Foundation's (Deutsche Forschungsgemeinschaft) Guidelines for Safeguarding Good Scientific Practice, national and international legislation, and any other relevant regulations, principles, and practices. Special care should be taken to comply with the EU General Data Protection Regulation 2016/679 (GDPR).

I. RESEARCH PROJECTS AND RESEARCH DATA

- a. For the purposes of this policy, a "research project" is any activity that involves (1) collecting new data, (2) acquiring and using secondary data, or (3) implementing experiments for research purposes.
- b. Research data means all data that was created, collected or processed in the course of a research project, or data which results from a research project. The data may involve a range of media, aggregation levels and formats.

II. RESEARCH DATA COLLECTION

- a. For collecting, processing, using, and storing personal data, researchers are responsible for obtaining and documenting the freely given informed consent of participants, in accordance with the international and national guidelines.
- b. Researchers should aim to obtain participants' written consent. Where written consent is not possible, approval for alternative ways of obtaining consent must be gained in accordance with the Hertie School Research Ethics Review Policy.
- c. Points a and b also apply to the collection of data on social media, online forums, apps, websites, and other publicly accessible online locations. When collecting data from online locations,

researchers must adhere to their specific terms, conditions, and legal disclaimers, as well as to the current legislation concerning data protection. Online research should follow the same duty of care and integrity principles as any type of research conducted at the Hertie School.

- d. If a researcher uses personal data collected by previous research projects or other sources (i.e., secondary data), there is nonetheless the requirement to document informed consent applicable in the current research project.

III. RESEARCH DATA PROCESSING

- a. Researchers should familiarise themselves with, and fill in, data management plan (DMP) templates.
- b. DMPs are documents required by research funders at the beginning, mid-point and end of research projects. Researchers who are required to submit a data management plan can contact the Hertie School Library for assistance.
- c. Researchers using third party software/servers for the collection, processing, storage and/or transfer of personal or sensitive data must be aware of the software/servers' specific policies on data privacy and obtain consent from all human subjects for the use of such software/servers.

IV. RESEARCH DATA STORAGE

- a. Researchers should determine the safest way to store their data, while allowing access whenever possible to ensure reproducibility of the research.
- b. All research data must be stored appropriately, and whenever necessary, protected against unauthorised access.
- c. It is the responsibility of the researchers to take technical and organisational measures to prevent any unauthorised access and establish clear access rules.
- d. There should be no access to the data for any third party unless they meet the data protection requirements and provide assurances to that effect.
- e. The researchers can contact the Hertie IT Department for assistance.

V. RESEARCH DATA ARCHIVING AND DELETION

- a. Research data should be archived for the long term and published in an appropriate data archive or repository, whenever possible.
- b. The researcher should ensure the retrievability of the research data.
- c. Data shall be kept for the period that is required by the research project, in accordance with the GDPR and other laws and regulations. If the data is fully anonymous, GDPR allows the retention of data without deadlines. The data can be kept for archiving and scientific research purposes.
- d. All research data containing personal data must be deleted in accordance with the GDPR.

VI. RESEARCH DATA SHARING AND TRANSFER

- a. 'Data transfer' includes the communication, disclosure or otherwise making the data available to a third party.
- b. All parties of the data transfer must have adequate safeguards for the protection of personal data in place.
- c. Researchers should pay special attention to any transfer of personal data to a third party, in accordance with GDPR.

- d. Researchers should pay special attention to any transfer of data to a non-EU country, in accordance with GDPR. Special precautions need to be taken when personal data is transferred to third parties outside the EU/EEA that do not provide for EU-standard data protection.
- e. Accessing data at another facility:
 - i. When a researcher requires access to data held by a third party, they may require data management assurances.
 - ii. If a formal statement of assurances is needed and for assistance with access applications, the researcher should contact the Hertie IT Department and the Research Ethics Officer.
- f. Giving data access to a third party:
 - i. When a third party or a partner to a research project requests access to data, it is the responsibility of the researcher to ensure that data is only shared when all legal, technical, and practical safeguards are in place.
 - ii. The researcher should request a formal statement of assurances from the third party or the project partner.
 - iii. For advice and support, the researcher should contact the Hertie IT Department and the Research Ethics Officer.

VII. PUBLICATION OF RESEARCH DATA

- a. Research data should be open to the fullest possible extent unless covered by overriding commercial, contractual, legal, or ethical obligations.
- b. Research data as well as scholarly publications should be made publicly available in a timely manner. Protection of personal data, copyrights, and the legitimate interests of third parties must also be ensured.
- c. It is recommended that all datasets and metadata collected by Hertie researchers, and all software programmed by Hertie researchers shall be made publicly available (Open Access) along with the source code, using external generalist or subject-specific public data archives and repositories. Datasets can also be attached to research publications if they are repositored to the Hertie School Research Repository (OPUS).

VIII. SUPPORT AT THE HERTIE SCHOOL

- a. All members of the Hertie School are advised to attend and complete training on data management and protection. Necessary resources shall be made available through the Library and IT Services.
- b. The Hertie Library will support researchers in meeting the requirements of this policy by:
 - i. Serving as the focal point for research data management and providing advice to researchers involved with data management planning.
 - ii. Offering guidance to researchers with the management of research data.
 - iii. Supporting researchers in finding data archives or repositories for the adequate preservation and storage of data, including support in applying appropriate licenses to data.
 - iv. Providing advice on Open Science and Open Access.
- c. The Hertie IT Department will support researchers in meeting the requirements of this policy by:
 - i. Offering guidance to researchers how to set up and maintain a secure IT work environment (e.g. hard drive encryption).
 - ii. Supporting researchers in finding, setting up and maintaining a secure data storage environment.
- d. The Research Ethics Officer will support researchers in meeting the requirements of this policy by:

- i. Serving as the primary contact for all matters related to research ethics and the ethical issues of data collection.
 - ii. Coordinating and advising when a formal ethics review and approval is required.
 - iii. Advising on ethics-related questions regarding the application of the GDPR.
- e. The Legal Officer will support researchers in meeting the requirements of this policy by:
 - i. Advising on non-research related matters of data protection and the GDPR.
 - ii. Examining data protection compliance issues, and when required, involving the consultant DPO.
 - iii. The consultant DPO shall only be consulted in exceptional situations after a referral by the Legal Officer.
 - iv. The consultant DPO assesses data management practices and provides guidance where needed. If a high risk to personal information is identified, the DPO can undertake a Data Protection Impact Assessment (DPIA).

IX. PROCESS FOR REVIEW OF DATA MANAGEMENT IN RESEARCH PROJECTS

- a. As the first step, the Research Ethics Self-Assessment checklist should be completed for every new project and funding proposal that includes research with human subjects and/or identifiable human subject data.
- b. If a review or formal approval is needed for a research project and its data management plan and practices, an application for research ethics review should be submitted, as set out in the Hertie School Policy for Research Ethics Review.
- c. Where the extent, complexity, subject matter, methodology or data ethics of the project requires a full research ethics review, or where the funder, partner, or publisher requires a formal ethics review or statement, the Research Ethics Committee shall review the application.
 - i. Examples of projects that require full review include but are not limited to: projects involving vulnerable participants, where the researcher is unable to gain full and informed consent of the participants; covert research; use of deception; manipulations of social processes; and processing of sensitive personal data.

After approval and acknowledgment by the Academic Senate in mutual agreement with the School's Management with prior comment of the Academic Council of the Board of Trustees, this policy took effect as of 15 March 2023.