Data Privacy Declaration for Users of HPC Systems of the NHR@ZIB

Gender neutral people names:
In the text below, gender-specific differentiation (for example, scientist, user, applicant) is omitted for reasons of easier readability in people names. Insofar as only one of the gender-specific variants is mentioned, this should in principle apply to both sexes in the sense of equal treatment.

Preamble

The NHR Alliance bundle the resources and competencies of university high-performance computing and make them available to scientists at German universities free of charge. As one of the nine NHR centers in Germany, NHR@ZIB offers HPC resources as well as domain-specific consultation as scientific service. In preparation phase, during and after the use of the scientific and technical services, personal data required for the provision of the services will be collected, processed and stored. **Therefore, please read this Privacy Policy carefully, especially your rights to use your personal information in Section 7**.

Below we inform you about the nature, scope and purpose of the collection and use of personal data.

The personal data collected by NHR@ZIB are stored and processed on servers at the operational site

Zuse Institute Berlin (ZIB), Takustraße 7, D-14195 Berlin

- in the following referred to as “provider”.

For the provider, the processing of personal data is subject to the applicable data protection regulations, in particular the EU General Data Protection Regulation (GDPR), the Federal Data Protection Law (BDSG), the Berlin Data Protection Law (BlnDSG), and the German Telecommunication Telemedia Data Protection Law (TTDSG).

This “Data Protection Declaration for Users of the NHR@ZIB Systems” can be downloaded at any time at

https://nhr.zib.de/en/data-privacy-declaration-for-system.

1. Processed Personal Data

Master Data and Project Data

For the usage of the scientific services offered by NHR@ZIB you communicate to us personal information (master data):

- user account
- given name, family name
- federal state of your scientific institution (university, research institute)
- address of your scientific institution and division
- scientific area
- business phone number
- business email address
- nationality and passport number, if you belong to an embargo country (see the current list of the relevant nationalities in the application form)
- statement regarding the intended use of computing systems

Usually, you use the services in the context of a project reviewed by the Scientific Council (WA). For this, you communicate to us the following additional data (project master data) during the application process for using the resources:

- project title
- name of the principal investigator
- extensive description of the planned scientific project
- a summary of the project description
- the amount of required resources (e.g. computing time, storage requirements for permanent and scratch data)

These data are stored in a project database for the content and administrative project management. This includes the preparation and execution of the review of the project proposal by the WA, the provision of the resources granted by the WA, as well as the compilation and accounting of the used resources.
By sending the project proposal the applicant agrees to the publication of the summary of the project description together with information about the executing institution on the NHR@ZIB websites and project reports. The project description can be enriched by multi-media material (images, videos) for publication.

Protocol Data of Usage

On access to resources and usage of NHR@ZIB services certain data are automatically captured in logfiles on the servers.

Data captured on access of web pages of the NHR@ZIB websites are explained on the webpage at

https://nhr.zib.de/en/data-privacy-declaration-for-website.

Protocol data of users contain among others the following information:

- connection data:
  - IP addresses and/or hostnames of the access hosts
  - date and time (time stamp) of the access
- usage data:
  - account, kind and duration of the resource usage (system monitoring)
  - account in data of system activities and state in case of errors (system dumps)
- project-related data:
  - personal data that you agree to communicate to us in web forms
  - type of the used web browser and operating system (if communicated by the web browser)

The providers do not match connection and usage data with other compiled data, so no backtracking to a person is possible.

2. Legal Basis and Usage of the Data

The processing of the data described in section 1 is necessary for the operation of NHR@ZIB according to Art. 6 (1) lit. b and c GDPR.

Account, given and family names, phone numbers and email addresses are needed for contact and for the scientific and technical support enabling a save and optimal usage of the resources (HPC consultancy). These personal data serve to record and process your resource usage, e.g., used computing time (system monitoring, accounting).

Master data and project master data are stored beyond the end of project for comparison with other project proposals (continuation proposals, avoidance of multiple proposals etc.), for resource-usage statistics, and to implement access policies during restauration of old research data of a user (see also section 5.). For this, only resources at the provider site are used. Parts of the project data including the project ID are published at https://nhr.zib.de/en/nhr-projects.
The agreement to the publication of these data is part of the application process and has been granted by the applicant.

The connection data including the account serve as access control to and monitoring of the resources.

NHR@ZIB operates a ticket system by which users can report problems to the Support Team. The ticket system joins your master data for display in the web browser.

The nationality is required to check the access rights in the context of legal and contractual regulations for using high-performance computers within the NHR.

3. Security Measures

The provider of the NHR@ZIB resources strive to protect resources and their users against unauthorized access to or unauthorized modification, transfer or damage of data. To assure this we have implemented the following technical and organizational measures:

- Access to the resources is SSL-encoded, only.
- Connection to the NHR@ZIB Service Portal is SSL-encoded, only.
- The provider of the resources regularly checks his systems regarding the implemented practices for collecting, storing and processing user data, including physical security measures against unauthorized access to systems.
- The provider restricts access to personal data to a narrowly-defined circle of employees of the provider and the NHR bodies. These persons compellingly need to know these data for processing and are subject to confidentiality obligations.

4. Offices in Charge of Data Privacy

Office in charge according to Art 13. GDPR "Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person" is:

Zuse-Institute Berlin (ZIB)
Takustraße 7
D-14195 Berlin

The Data Protection Officer at the provider institution cares for the compliance with the principles of data privacy. Questions about data privacy should be directed to the Data Protection Officer of the provider:

z. Hd. **Datenschutzbeauftragter**
Zuse-Institute Berlin
Takustraße 7
D-14195 Berlin
E-Mail: datenschutz@zib.de

5. Differentiation to User-Managed Data – Research Data with Personal Information

The provider of the NHR@ZIB resources is only responsible for protecting the operational data. Operational data are the user's master data, project data, connection data, and resource-usage data. **Data that the user stores on NHR@ZIB resources for his research purposes (so-called payload data or research data) are subject to his individual responsibility. The provider expressly notes that storing and processing of research data with personal information on NHR@ZIB resources is prohibited.**

We absolutely recommend considering working with anonymized personal information. Should storing and processing of personal information be part of a planned research project, please contact the NHR@ZIB Account Administration (see Section 9. "Information") at least 6 months in advance by postal letter, as in this case a German Data Processing Agreement (German AVV) has to be concluded with the ZIB.

6. Transfer, Storing, and Deletion of Personal Data

Your personal data are collected, processed and used solely to ensure the operation of resources.

For the review process by the Scientific Council (WA) personal data (given name, family name, business phone number and email address, address of your institution, scientific area) are transferred to external reviewers of the WA. The list of members of the WA can be found at

https://nhr.zib.de/en/boards-and-the-scientific-board.

For the period of time for storing personal data the following statements apply:

- All user data (master data) and project master data are stored for the duration of operating resources at NHR@ZIB.
- Users can communicate arising problems to the Support Team via the NHR@ZIB ticket system. Data in the ticket system are stored similar to a shared email folder for the duration of NHR@ZIB operation.
- User account, federal state, scientific area and project membership are stored for the collection of statistical data about the differentiated resource consumption (accounting) and for the purpose of reporting to NHR bodies and funding agencies for the service life of a system (typical 5-6 years).
- Connection data is anonymized after a year for later analysis of attacks on the IT infrastructure of the NHR@ZIB, and for statistical purposes.
- Hostnames of target hosts for the communication from servers to the outside are managed by the user.

For users from so-called embargo countries (see section 1) the communication of personal data (usually first and family names, nationality, passport number) to the manufacturer of the system is required according Art. 49 (1) lit. c GDPR.
Personal data are communicated to governmental institutions and authorities only in the context of mandatory national legislation or where disclosure is required by law enforcement in the event of attacks on the providers' IT infrastructure.

7. Your Rights as a user of NHR@ZIB

According to the EU GDPR each person affected, i.e., you as a user of NHR@ZIB, has

- **the right to information (Art. 15),**
- **the right to correction (Art. 16),**
- **the right to deletion (Art. 17),**

- **the right to restriction of processing (Art. 18),**
- **the right to data transfer (Art. 20) and**
- **the right of appeal to the competent supervisory authority (Art. 77).**

Should you want to make use of your right to block, delete or correct incorrect data or should you want information about personal data stored at NHR@ZIB, please contact NHR@ZIB User Administration (see Section 8 "Information") by postal letter.

After activation of your user account by the administration you can view and modify your data at the NHR@ZIB Service Portal (https://portal.nhr.zib.de).

8. Information

c/o NHR@ZIB Nutzerverwaltung
Zuse Institute Berlin
Takustraße 7
D-14195 Berlin

9. Change of Our Data Privacy Policy

This data privacy policy is valid from February 1st, 2024 and replaces all prior declarations. NHR@ZIB reserves the right to adapt this declaration to developments and legal requests. We recommend that you revisit the latest privacy policy if necessary.

The applicant will be informed and, if necessary, asked for permission, if NHR@ZIB plans to process collected data for other purposes.

Version: January 2024