

# Privacy policy for the RWTH Compute Cluster, the JARDS-Online Portal and connected software components for the submission and review of computational time requests

IT Center @ RWTH Aachen University

August 15, 2021

## Table of contents

1	Preamble .....	4
2	Person responsible for data processing .....	4
3	Person responsible for operation .....	5
4	Data Protection Officer .....	5
5	Competent supervisory authority .....	5
6	General information on data processing .....	5
6.1	Scope of the processing of personal data .....	5
6.1.1	Legal basis for the processing of personal data .....	6
6.1.2	Data deletion and storage period .....	6
7	Use of the RWTH Compute Cluster .....	6
7.1	Description and scope of data processing .....	6
7.2	Legal basis for data processing .....	8
7.3	Purpose of data processing .....	8
7.4	Data access .....	9
7.4.1	Cluster users .....	9
7.4.2	Cluster users with project participation .....	9
7.4.3	Project manager .....	10
7.4.4	Cluster administrators .....	10
7.4.5	Rights matrix .....	10
7.5	Duration of storage .....	11
7.6	Possibility of objection and removal .....	11
7.7	Data transfer .....	11
7.8	Data transfer to third countries .....	11
8	Use of the JARDS-Online portal as well as software components connected to it for the submission and review of computing time applications .....	12
8.1	Description and scope of data processing .....	12
8.1.1	Functional data .....	12
8.1.2	Usage data .....	12
8.1.3	Diagnostic data .....	13
8.2	Legal basis for data processing .....	13
8.3	Purpose of data processing .....	14
8.4	Data access .....	14
8.4.1	Members of the awarding body .....	15
8.4.2	Coordinators of the application and review process .....	15
8.4.3	Assessing .....	15
8.4.4	PI, Person to contact (PC) .....	15

8.4.5	Administering.....	15
8.4.6	Rights matrix.....	15
8.5	Duration of storage .....	16
8.6	Possibility of objection and removal.....	16
8.7	Data transfer.....	16
8.8	Data transfer to third countries .....	16
9	Rights of the data subject.....	16
9.1	Right to information.....	17
9.2	Right to rectification .....	17
9.3	Right to restriction of processing.....	18
9.4	Right to deletion .....	18
9.4.1	Obligation to delete.....	18
9.4.2	Information to third parties.....	19
9.4.3	Exceptions.....	19
9.5	Right to information .....	20
9.6	Right to data portability.....	20
9.7	Right of objection.....	20

## 1 Preamble

The RWTH Compute Cluster (hereinafter referred to as RWTHCC) is operated by the IT Center of RWTH Aachen University. Via this service, computing time quotas are made available to all persons authorized to use it. The RWTHCC consists of the following components:

- Dialogue systems
- Compute Node
- File systems
- Workload Management System (WLM)
- Directory Services
- Monitoring systems
- Databases for managing computing time projects and hardware components

The submission of requests for computing time for HPC resources of the IT Center of RWTH Aachen University by applicants (hereinafter referred to as 'Principle Investigators', PIs), their evaluation, administration and reporting are carried out via the JARDS online portal and connected software components.

When using this service, personal data is collected only to the extent necessary for the use of the cluster, for a complete processing of computing time requests, for the implementation of the review process, for the administration of approved computing time projects, for the simplification of extension requests for subsequent computing time award procedures, for statistical purposes, and for the exclusion of multiple requests. It will not be used for any other purpose.

The personal data processed is subject to the applicable data protection regulations, in particular the EU General Data Protection Regulation (DSGVO), the Data Protection Act of North Rhine-Westphalia and the Telemedia Act.

In the following, we inform you in detail about the type, scope and purpose of the collection and use of personal data.

## 2 Person responsible for data processing

The responsible person within the meaning of the EU General Data Protection Regulation and other national data protection laws of the member states as well as other data protection regulations is:

Rector of RWTH Aachen University  
Templergraben 55  
52062 Aachen (home address)  
52056 Aachen (postal address)  
Phone: +49 241 80 1  
Fax: +49 241 80 92312  
E-mail: [rektorat@rwth-aachen.de](mailto:rektorat@rwth-aachen.de)  
Website: [www.rwth-aachen.de/rektorat](http://www.rwth-aachen.de/rektorat)

### 3 Person responsible for the operation

Availability of the person responsible for technical operations:

Prof. Matthias S. Müller  
IT Center of RWTH Aachen University  
Seffenter Weg 23  
52074 Aachen  
Phone: +49 241 80 24680  
E-mail: [servicedesk@itc.rwth-aachen.de](mailto:servicedesk@itc.rwth-aachen.de)  
Website: [www.itc.rwth-aachen.de](http://www.itc.rwth-aachen.de)

### 4 Data Protection Officer

Availability of the officially appointed data protection officer:

Data Protection Officer of RWTH Aachen University Templergraben  
55  
52062 Aachen (home address)  
52056 Aachen (postal address) Germany  
Phone: +49 241 80 93665  
Fax: +49 241 80 92678  
E-mail: [dsb@rwth-aachen.de](mailto:dsb@rwth-aachen.de)  
Website: [www.rwth-aachen.de/datenschutz](http://www.rwth-aachen.de/datenschutz)

### 5 Competent supervisory authority

Ministry of Culture and Science of the State of North Rhine-Westphalia Völklinger  
Straße 49  
40221 Dusseldorf  
Phone: +49 211 89604

### 6 General information on data processing

#### 6.1 Scope of the processing of personal data

As a matter of principle, RWTH Aachen University only processes personal data of the users of the service to the extent that this is necessary to provide a functional service as well as the contents and services. The processing of personal data of the users is regularly only carried out after the consent of the users. An exception applies in cases where it is not possible to obtain prior consent for actual reasons and the processing of the data is permitted by legal regulations.

### 6.1.1 Legal basis for the processing of personal data

Insofar as RWTH Aachen University obtains the consent of the data subject for processing operations involving personal data, Art. 6 (1) lit. a EU General Data Protection Regulation (DSGVO) serves as the legal basis.

Insofar as the processing of personal data is necessary for the performance of tasks of RWTH Aachen University that are in the public interest or are carried out in the exercise of official authority, Art. 6 (1) lit. e DSGVO serves as the legal basis.

### 6.1.2 Data deletion and storage period

The personal data of the data subject will be deleted or blocked as soon as the purpose of the storage no longer applies. The specific deletion periods are described by category of personal data (functional data, usage data, diagnostic data) in chapters 7 and 8.

Storage may also take place if this has been provided for by the European or national legislator in Union regulations, laws or other provisions to which the controller is subject. Data will also be blocked or deleted if a storage period prescribed by the aforementioned standards expires, unless there is a need for further storage of the data for the conclusion or performance of a contract.

## 7 Use of the RWTH Compute Cluster

### 7.1 Description and scope of data processing

In describing the scope of the RWTHCC's data processing, the following sub-aspects are considered: Creation of the HPC user ID, use of the dialog systems and compute nodes, and use of the workload management system (WLM). The workload management system is used to distribute the set computing time jobs to the available computing nodes.

Personal data of the following four categories are collected and processed: Functional data

- First and last name
- E-mail address
- Gender
- Institute code number (IKZ)
- Status (student, employee, guest)
- User ID
- Creation time of the HPC user ID
- Time of the last login

Usage data

- User ID
- Status (student, employee, guest)
- ID and name of the job
- Computing Time Project ID
- Institute code number (IKZ)

- DFG subject number
- E-mail address, if specified by the user for notification of the job status.
- Hiring date of the job
- AssocID of the workload management system (linkage of cluster, partition, account and user ID).
- Path to working directory (may include user ID, compute time project ID, etc.)
- Path to job output files
- List of used computational nodes in a computational time order (job)
- Start and end time of the job
- Name of and path to the job script
- Consumed and still available computing time quotas
- Job script content
- Loaded software modules

#### Diagnostic data

- Time and duration of interactive use
- IP address of the terminal device from which the user logs in

#### Work data

- Data stored and processed by the users under their responsibility

Functional data is stored in the RWTHCC directory service when the HPC user ID is created.

To protect the users' work data from loss, the contents of the home file system are backed up incrementally on a daily basis via the IT Center service "Backup".

To provide users with targeted information, their e-mail address is entered in a mail list on the central list server at RWTH Aachen University. In the event of anomalies, users can be contacted by IT Center staff via the stored e-mail address if necessary.

The diagnostic data is kept on each individual server in the local log service (Syslog) for seven days and then automatically deleted.

In addition, all login processes are logged locally in the login records and on central servers. There, they are anonymized after seven days and kept in this form for statistical purposes.

A further remote logging of the login processes takes place in a central log server of the Network Operation Center of the IT Center of RWTH Aachen University and the data is kept there according to its valid times.

Usage data will be stored in central databases within RWTHCC for the reportable period for major equipment described in Section 7.2.

The data described above is not stored together with other personal data of the user.

## 7.2 Legal basis for data processing

The processing of users' functional data is necessary for the performance of the university's tasks as a public institution. The processing of this data and the log files is based on Art. 6, Para. 1, lit. e DSGVO and §3, Para. 1 DSG NRW. The tasks of the university are defined in §3, para. 1, 3, 5 and 6 HG NRW and §2, para. 1 Grundordnung RWTH Aachen.

The processing of users' usage data is necessary for the performance of the university's tasks as a public institution. The tasks of the university are defined in

§3, para. 1, 3, 5 and 6 HG NRW and §2, para. 1 Grundordnung RWTH Aachen. The processing of this data and the log files is based on Art. 6, para. 1, lit. e DSGVO and §3, para. 1 DSG NRW. The implementation agreement to the GWK agreement on the joint funding of research buildings, large-scale equipment and national high-performance computing (NHR) at universities - Ausführungsvereinbarung Forschungsbauten, Großgeräte und Nationales Hochleistungsrechnen (AV-FGH) - dated November 26, 2018 (BAnz AT 21.12.2018 B9) form the legal basis for the reporting obligations. Articles § 6, paragraph (2) and (3), as well as § 15, paragraph (3) and § 18, paragraph (2) and (3), regulate the reporting obligations of the operators of the national HPC infrastructure. Derived from this, the IT Center of RWTH Aachen University as operator keeps the above mentioned usage data for up to 10 years after the start of the NHR procedure in order to be able to provide evidence of the appropriate use of funds and science-guided allocation of computing time and to provide evidence for subsequent applications.

The processing of diagnostic data of users is necessary for the performance of the tasks of the university as a public institution. The processing of this data and the log files is based on Art. 6, Para. 1, lit. e DSGVO and §3, Para. 1 DSG NRW. The tasks of the university are defined in §3, para. 1, 3, 5 and 6 HG NRW and §2, para. 1 Grundordnung RWTH Aachen.

The processing of users' work data is necessary for the performance of the university's tasks as a public institution. The processing of this data and the log files is based on Art. 6, Para. 1, lit. e DSGVO and §3, Para. 1 DSG NRW. The tasks of the university are defined in §3, para. 1, 3, 5 and 6 HG NRW and §2, para. 1 Grundordnung RWTH Aachen.

## 7.3 Purpose of data processing

The functional data is collected and processed to ensure operation and to determine the authorization for use (hardware and software). In addition, these are used for support purposes.

The diagnostic data is processed to ensure the operation of the systems. In addition, they are used to create an anonymized report on the utilization and usage of the systems. Furthermore, they are used for tracing and forensic analysis in the event of a security-relevant incident.



The usage data is processed for the purpose of administration, further development and maintenance of the system, technical controlling, troubleshooting of technical problems, clarification of security incidents, support, project management and reporting. In this context, the reporting data is required for reasons of public procurement law in order to substantiate conditions resulting from the type of financing of the cluster.

The resolution of the Joint Science Conference (GWK) of August 2020 and the corresponding AV-FGH specifications for the National High Performance Computing Alliance (NHR- Centers) result in the obligation to secure the usage data for the reportable period of the large-scale facilities in order to enable an allocation of the used resources to the institution. In the current funding line (programmatic-structural line in transition to NHR), this period is 10 years.

An evaluation of the data for marketing purposes does not take place.

## 7.4 Data access

In the RWTHCC there are three roles with ascending scope of rights:

1. Cluster users
2. Cluster users with project participation
3. Project Lead
4. Cluster Administrators

These have varying degrees of access to personal data in the RWTHCC. Data may only be viewed for the specified purpose, insofar as it is necessary for the fulfillment of tasks. The principle of data minimization also applies.

### 7.4.1 Cluster users

*Cluster users* are persons who have access to the RWTHCC and can therefore use the workload management system. They can view which compute time jobs have been posted to the system. This includes user ID and UNIX ID, ID and name of the job, compute time project ID, start and (predicted) end time of the job, job partition, job status, name of and path to the job script, number and host names of the compute nodes involved, and the working directory.

### 7.4.2 Cluster users with project participation

The role *Cluster users with project involvement* is assigned to cluster users who are involved in a computational time project. In addition to the information mentioned in 7.4.1, they can use the

view the used and still available computing time quotas of the own project.

### 7.4.3 Project Lead

The *Project Leaders* role is given to people who have been granted the project (PI) as well as people who have been designated as contact persons (PC). In addition to the information mentioned in 7.4.2, they can view the used computing time quotas of all project participants.

### 7.4.4 Cluster Administrators

Only employees of the IT Center of RWTH Aachen University who are entrusted with the system administration and development of the RWTHCC are granted the *Cluster Administrator* role. In principle, persons with the Cluster Administrators role see all personal data including usage data and cluster log data. Viewing takes place exclusively within the scope of official duties and in case of need. The persons to whom this role is assigned are obliged to maintain confidentiality.

### 7.4.5 Rights matrix

The following rights matrix lists which data is visible for which roles.

Table 1: Rights matrix

Data is visible for:	Cluster users	Cluster users with project participation	Project Lead	Cluster administrators
<b>Job-related usage data</b> <ul style="list-style-type: none"> <li>- User ID</li> <li>- Computing Time Project ID</li> <li>- ID and name of the job</li> <li>- Hiring date of the job</li> <li>- Path to the working directory</li> <li>- List of used computing nodes</li> <li>- Start and end time of the job</li> <li>- Name of and path to the job script</li> </ul>	✓	✓	✓	✓
<b>Project-related usage data</b> <ul style="list-style-type: none"> <li>-Usedand still available computing time contingent of the project</li> </ul>	X	✓	✓	✓
<b>Project-related usage data</b> <ul style="list-style-type: none"> <li>-Consumedcomputing time quota of the individual project participants.</li> </ul>	X	✓	✓	✓

Further usage data				
<ul style="list-style-type: none"> <li>- Institute code number (IKZ)</li> <li>- DFG subject number</li> <li>- E-mail address, if specified by the user for notification of the job status.</li> <li>- AssocID (association of cluster, partition, account and user ID)</li> <li>- Path to job output files</li> <li>- Job script content</li> <li>- Loaded software modules</li> </ul>	X	X	X	✓
Function and diagnostic data	X	X	X	✓

## 7.5 Duration of storage

The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. Functional data is retained for the duration of the account, usage data for the reportable period of 10 years specified in 7.2, and diagnostic data for seven days.

The duration of the storage of the work data is generally the responsibility of the users. The work data is deleted 14 days after the deletion of the respective local file from the IT Center Service "Backup".

When the account is deleted from the IT Center service "Identity Management", it is initially deactivated in the RWTHCC and deleted after 12 months together with all work data. For technical reasons, local backup copies of individual file systems are only completely deleted after a further six months.

## 7.6 Possibility of objection and removal

The collection of data is mandatory for the operation. Consequently, there is no possibility for users to object. The registration on the mailing list can be cancelled independently by the user.

## 7.7 Data sharing

Personal data will not be disclosed to third parties or used for purposes other than those stated here, subject to legal provisions.

## 7.8 Data transfer to third countries

A data transfer to third countries does not take place.

## 8 Use of the JARDS-Online portal as well as software components connected to it for the submission and review of computing time applications.

### 8.1 Description and scope of data processing

Data collection, processing and use is performed by the IT Center of RWTH Aachen University for the purpose of submitting and reviewing computing time requests for the use of RWTHCC resources.

The following data is collected:

#### 8.1.1 Functional data

The following functional data of PIs, their contact persons (PCs), project members (PMs), and scientific and technical assessors are collected and stored:

- Title, first name, possibly call name, last name, salutation
- Contact details (official): E-mail address, phone number
- Username in RWTH Identity Management
- Institute
- Institute code number for applications from RWTH Aachen University
- Address (official)
- State of the requesting institution

In the case of computing time requests for student work, the following personal data is collected and stored from the students involved:

- Title, first name, possibly call name, last name, salutation
- Contact details: E-mail address, phone number
- Username of the RWTH Identity Management
- University

#### 8.1.2 Usage data

The following data and information are stored:

- The computing time applications with associated project descriptions, as well as status and final reports from the applicants.
- Field(s) and expertise(ies) of applicants and scientific reviewers
- Scientific and technical opinions prepared by the assessors
- Start and end time of the project

- Overview of requested and approved computing time requests of all HPC systems of the last three years, incl.
  - o Year of application
  - o Application track
  - o HPC system
  - o Project ID
  - o Requested computing time in core-h
  - o Granted computing time in core-h
  
- Computing time project ID (for project extension)

### 8.1.3 Diagnostic data

Every access by users to this online portal is logged in server log files. These store the following data and information:

- the time of access
- the IP address of the end device
- the called URL

Cookies can be used to simplify the login process. They store a session ID in a text file on your computer, which can be used to manage the login status in the online portal.

## 8.2 Legal basis for data processing

The processing of users' functional data is necessary for the performance of the university's tasks as a public institution. The processing of this data and the log files is based on Art. 6, Para. 1, lit. e DSGVO and §3, Para. 1 DSG NRW. The tasks of the university are defined in §3, para. 1, 3, 5 and 6 HG NRW and §2, para. 1 Grundordnung RWTH Aachen.

The processing of usage data of users is necessary for the performance of the tasks of the university as a public institution. The processing of this data and the log files is based on Art. 6, Para. 1, lit. e DSGVO and §3, Para. 1 DSG NRW. The tasks of the university are defined in §3, Abs. 1, 3, 5 and 6 HG NRW as well as §2, Abs. 1 Grundordnung RWTH Aachen. The implementation agreement to the GWK agreement on the joint funding of research buildings, large-scale equipment and national high-performance computing (NHR) at universities - Ausführungsvereinbarung Forschungsbauten, Großgeräte und Nationales Hochleistungsrechnen (AV-FGH) - dated November 26, 2018 (BAnz AT 21.12.2018 B9) form the legal basis for the reporting obligations. Articles § 6, paragraph (2) and (3), as well as § 15, paragraph (3) and § 18, paragraph (2) and (3), regulate the reporting obligations of the operators of the national HPC infrastructure. Derived from this, the IT Center of RWTH Aachen University as operator keeps the above mentioned usage data for up to 10 years after the start of the NHR procedure in order to be able to provide evidence of the appropriate use of funds and science-guided allocation of computing time and to provide evidence for subsequent applications.

The processing of diagnostic data of users is necessary for the performance of the tasks of the university as a public institution. The processing of this data and the log files is based on Art. 6, Para. 1, lit. e DSGVO and §3, Para. 1 DSG NRW. The tasks of the university are defined in §3, para. 1, 3, 5 and 6 HG NRW and §2, para. 1 Grundordnung RWTH Aachen.

### 8.3 Purpose of data processing

The processing of personal data is carried out in accordance with Art. 5, Para. 1, lit. b and c DSGVO for a specific purpose and under the condition of data minimization.

The functional and usage data listed under 8.1.1 and 8.1.2 are processed for the purpose of administration, support, project application, technical and scientific project assessment, project management and reporting. Furthermore, these data are required for reasons of public procurement law and for quality assurance of the scientific review in order to substantiate requirements resulting from the type of funding of the cluster (see section 8.2).

From the data under 8.1.1 and 8.1.2, publicity reports and anonymized statistics are generated. In addition, the title, the project abstract, the PI and, in the case of theses, the student can be published on the RWTH websites.

The diagnostic data listed under 8.1.3 is processed for the purpose of administration, troubleshooting technical problems, clarifying security incidents and for support purposes.

The resolution of the Joint Science Conference (GWK) of August 2020 and the corresponding AV-FGH specifications for NHR centers result in the obligation to save the usage data for the reportable period of the large-scale facilities in order to enable an allocation of the used resources to institution and federal state. In the current funding line (programmatic-structural line in transition to NHR), this period is 10 years.

An evaluation of the data for marketing purposes does not take place in this context.

### 8.4 Data access

The following roles exist in the JARDS portal and connected systems:

1. Members of the awarding body
2. Coordinator of the application and review process
3. Assessing
4. Principle Investigator (PI), Person to contact (PC)
5. Administrating

These have varying degrees of access to the personal data collected under 8.1. Data may only be viewed for the specified purpose, insofar as this is necessary for the fulfillment of the task. The principle of data minimization also applies.

#### 8.4.1 Members of the awarding body

The *members of the awarding body* are RWTH employees or members of the NHR Association and do not have direct access to the data mentioned in 8.1. Upon request, the coordinators of the application and review process will provide them with the required data for the purpose of resource allocation.

#### 8.4.2 Coordinator of the application and review process

*Coordinators of the application and review process* come from among the RWTH staff or the NHR network and have direct access to the data mentioned in 8.1.1 and 8.1.2.

#### 8.4.3 Reviewing

*Reviewers* are given access to the personal and application data described in sections 8.1.1 and 8.1.2 for the applications relevant to them for review. For quality assurance of the scientific review, reviewers from all German teaching and research institutions (in particular from the NHR Association) can be appointed.

#### 8.4.4 PI, Person to contact (PC)

A *PI* or a *PC* have access only to the data of their own projects.

#### 8.4.5 Administrating

Only employees of the IT Center of RWTH Aachen University who are entrusted with the system administration and development of the JARDS online portal and the connected components are granted the role of *Administrator*. In principle, persons with the role of administrator see all personal data, including log data. Viewing takes place exclusively within the scope of official duties and in case of need. The persons to whom this role is assigned are obliged to maintain secrecy.

#### 8.4.6 Rights matrix

The following rights matrix lists which data is visible for which roles

Table 1: Rights matrix

Data is visible for:	Awarding body	Coordinating	Reviewing	PI, PC	Administrating
Functional data of all projects	✓ (on request)	✓	X	X	✓
Functional data of own projects	not applicable	not applicable	Not applicable	✓	not applicable

Functional data of the project to be assessed	✓ (on request)	not applicable	✓	not applicable	not applicable
Usage data of all projects	✓ (on request)	✓	X	X	✓
Usage data of own projects	not applicable	not applicable	Not applicable	✓	not applicable
Usage data of the project to be assessed	✓ (on request)	not applicable	✓	not applicable	not applicable
Diagnostic data	X	X	X	X	✓

## 8.5 Duration of storage

The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected.

The functional and usage data collected in sections 8.1.1 and 8.1.2 are stored in central databases for the period subject to reporting.

The diagnostic data collected in section 8.1.1 will be stored locally on the JARDS web server for 7 days.

## 8.6 Possibility of objection and removal

The collection of data is mandatory for the operation. Consequently, there is no possibility for users to object. The registration on the mailing list can be cancelled independently by the user.

## 8.7 Data sharing

For the purpose of scientific review, personal data will be passed on to the respective reviewers from German teaching and research institutions, members of the awarding body and coordinators of the application and review process within the NHR Association.

## 8.8 Data transfer to third countries

A data transfer to third countries does not take place.

# 9 Rights of the data subject

If users' personal data are processed, they are data subjects within the meaning of the GDPR and are entitled to the following rights vis-à-vis the controller:



## 9.1 Right to information

You may request confirmation from the controller as to whether personal data concerning you are being processed by RWTH Aachen University.

If there is such processing, data subjects may request information from the controller about the following:

- the purposes for which the personal data are processed;
- the categories of personal data which are processed;
- the recipients or categories of recipients to whom the personal data concerning them have been or will be disclosed;
- the planned duration of the storage of the personal data concerning them or, if concrete information on this is not possible, criteria for determining the storage duration;
- the existence of a right to rectification or erasure of personal data concerning them, a right to restriction of processing by the controller or a right to object to such processing;
- the existence of a right of appeal to a supervisory authority;
- any available information on the origin of the data, if the personal data are not collected from the data subject;
- the existence of automated decision-making, including profiling, pursuant to Article 22(1) and (4) of the GDPR and, at least in these cases, meaningful information about the logic involved and the scope and intended effects of such processing for the data subject.

Data subjects have the right to request information about whether personal data concerning them is transferred to a third country or to an international organization. In this context, they may request to be informed about the appropriate safeguards pursuant to Art. 46 DSGVO in connection with the transfer.

This right of access may be restricted to the extent that it is likely to render impossible or seriously impair the achievement of the research or statistical purposes and the restriction is necessary for the fulfillment of the research or statistical purposes.

## 9.2 Right to rectification

Data subjects have a right to rectification and/or completion vis-à-vis the controller if the personal data processed concerning them are inaccurate or incomplete. The controller shall carry out the rectification without undue delay.

Inventory data can only be changed in the source system upon corresponding request. The content data generated by data subjects can change or delete them independently according to their role and your rights.

All other personal data may be changed upon request to Support, provided that the claim is justified and reasonable.

### 9.3 Right to restriction of processing

Under the following conditions, data subjects may request the restriction of the processing of personal data concerning them:

- if they contest the accuracy of the personal data concerning them for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and they object to the erasure of the personal data and request instead the restriction of the use of the personal data;
- the controller no longer needs the personal data for the purposes of processing, but they need it for the assertion, exercise or defense of legal claims, or
- if you have objected to the processing pursuant to Art. 21 (1) DSGVO and it is not yet clear whether the legitimate grounds of the controller outweigh your grounds.

Where the processing of personal data relating to them has been restricted, those data may be processed, with the exception of their storage, only with their consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of substantial public interest of the Union or of a Member State.

If the restriction of processing has been restricted in accordance with the above conditions, data subjects shall be informed by the controller before the restriction is lifted.

The right to restrict processing may be limited to the extent that it is likely to render impossible or seriously impede the achievement of the research or statistical purposes and the restriction is necessary for the fulfillment of the research or statistical purposes.

### 9.4 Right to deletion

#### 9.4.1 Obligation to delete

Data subjects may request the controller to erase personal data concerning them without delay, and the controller shall be obliged to erase such data without delay, if one of the following reasons applies:

- The personal data concerning them are no longer necessary for the purposes for which they were collected or otherwise processed.

- You revoke your consent on which the processing was based pursuant to Art. 6 (1) a or Art. 9 (2) a DSGVO and there is no other legal basis for the processing.
- You object to the processing pursuant to Art. 21 (1) DSGVO and there are no overriding legitimate grounds for the processing, or you object to the processing pursuant to Art. 21 (2) DSGVO.
- The personal data concerning them have been processed unlawfully.
- The deletion of the personal data concerning them is necessary for compliance with a legal obligation under Union or Member State law to which the controller is subject.
- The personal data concerning them was collected in relation to information society services offered pursuant to Art. 8 (1) DSGVO.

#### 9.4.2 Information to third parties

If the controller has made public the personal data concerning him or her and is obliged to erase it pursuant to Article 17(1) of the GDPR, he or she shall, taking into account the available technology and the cost of implementation, implement reasonable measures, including those of a technical nature, to inform data controllers which process the personal data that the data subject has requested that they erase all links to or copies or replications of such personal data.

#### 9.4.3 Exceptions

The right to erasure does not exist insofar as the processing is necessary to

- to exercise the right to freedom of expression and information;
- for compliance with a legal obligation which requires processing under Union or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health pursuant to Art. 9(2)(h) and (i) and Art. 9(3) DSGVO;
- for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes pursuant to Article 89(1) of the GDPR, insofar as the right referred to in Section a) is likely to render impossible or seriously prejudice the achievement of the purposes of such processing, or
- for the assertion, exercise or defense of legal claims.

## 9.5 Right to information

If data subjects have asserted the right to rectification, erasure or restriction of processing against the controller, the controller shall be obliged to communicate this rectification or erasure of the data or restriction of processing to all recipients to whom the personal data concerning them have been disclosed, unless this proves impossible or involves a disproportionate effort.

The data subject has the right to be informed by the data controller about these recipients.

## 9.6 Right to data portability

Data subjects have the right to receive the personal data concerning them that they have provided to the controller in a structured, commonly used and machine-readable format. They also have the right to transmit this data to another controller without hindrance from the controller to whom the personal data was provided, provided that

- the processing is based on consent pursuant to Art. 6 (1) a DSGVO or Art. 9 (2) a DSGVO or on a contract pursuant to Art. 6 (1) b DSGVO and
- the processing is carried out with the help of automated procedures.

In exercising this right, data subjects also have the right to have the personal data concerning them transferred directly from one controller to another controller, insofar as this is technically feasible. The freedoms and rights of other persons must not be affected by this.

The right to data portability does not apply to processing of personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

## 9.7 Right of objection

Data subjects have the right to object at any time, on grounds relating to their particular situation, to the processing of personal data concerning them which is carried out on the basis of Article 6(1)(e) or (f) DSGVO; this also applies to profiling based on these provisions.

The controller shall no longer process the personal data concerning them unless it can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defense of legal claims.

If the personal data concerning them is processed for the purpose of direct marketing, data subjects shall have the right to object at any time to the processing of personal data concerning them.

personal data for the purpose of such advertising; this also applies to profiling, insofar as it is associated with such direct advertising.

If data subjects object to processing for direct marketing purposes, the personal data concerning them will no longer be processed for these purposes.

Data subjects have the possibility, in connection with the use of information society services, notwithstanding Directive 2002/58/EC, to exercise their right to object by means of automated procedures using technical specifications.

Data subjects also have the right to object, on grounds relating to their particular situation, to the processing of personal data concerning them which is carried out for scientific or historical research purposes or for statistical purposes pursuant to Article 89(1) of the GDPR.

The right to object may be restricted to the extent that it is likely to render impossible or seriously impair the achievement of the research or statistical purposes and the restriction is necessary for the fulfillment of the research or statistical purposes.