GDPR Data Processing Agreement

between the Licensee
Data Controller or its service provider,

hereinafter referred to as ***"Client"***

and iTernity GmbH, Heinrich-von-Stephan-Straße 21, 79100 Freiburg
Data (Sub-)Processor,

hereinafter referred to as "***iTernity***" or ***"Contractor"***

Agreement version: August 01, 2024

iTernity GmbH

Heinrich-von-Stephan-Str. 21
D-79100 Freiburg
Germany

Amtsgericht Freiburg i.Br.
HRB 701332

Steuernummer 06435/43554
Finanzamt Freiburg-Stadt
USt-Id Nr.: DE242664311

Geschäftsführer:
Ralf Steinemann

Bankverbindung:
Commerzbank AG
IBAN: DE37 680800300450056800
BIC: DRES DE FF 680

Tel +49 / (0)761 / 59034 -810
Fax +49 / (0)761 / 59034 -859

www.iternity.com
sales@iternity.com

1. Contractual structure, begin and term of the mandate

(1) This GDPR Data Processing Agreement (**"Agreement"**) may be concluded with the Data Controller (direct iTernity B2B Customer). In this case, the Data Controller is the Client and iTernity as Contractor is its Data Processor.

(2) The Agreement may also be concluded with a service provider (system provider, ISV, Hoster or Reseller) mandated by the Data Controller. In this case, the service provider is the Client and iTernity as Contractor is the Sub-Processor of the service provider. The client concludes the GDPR Data Processing Agreement with the joint customers on its own responsibility.

(3) Rights granted in this Agreement to the Client, are also granted to the Data Controller, if different to the Client.

(4) This Agreement applies as soon as and as long as the Client uses at least one service from iTernity, e.g., proof of concept or analysis of defects within the scope of a maintenance agreement.

(5) This Agreement also applies to the provision of future services, as soon as these services are explicitly mandated. In this case, iTernity will provide the Client with a corresponding Schedule to the respective service.

2. Subject of data processing as Processor / Sub-Processor Categories of data subjects affected and categories of personal data

(1) iTernity provides various, in part combinable, products and services (**"Services"**) for all aspects of data storage. At present, these are the Services iCAS and iCAS FS. The difference between these products is from a data protection perspective the data processing location and the responsibility for the operation.

Product	Data processing location	Operated by
iCAS	at the Client	the Client
iCAS FS	at the Client	iTernity

(2) iTernity has, in any case, only the obligation to support the Client with the Client's processing (e.g., in the case of iCAS with data migration), or to ensure the operation of the IT-Systems (in the case of iCAS FS), if applicable.

(3) As far as the content is concerned, selection, recording, correction or erasure of stored contents is not the subject matter of processing by iTernity. Without an explicit individual mandate, iTernity is prohibited from manipulating any data content.

(4) Depending on the contracted Services, the subject matter of processing by iTernity as a Processor or Sub-Processor is different (as well as the associated technical and organizational measures, see below). The specific subject matter of processing is specified in the corresponding Schedule to the respective Service.

(5) The Data Controller may store any data of any persons. The Data Controller lists the categories of data subjects and categories of associated personal data in its records of processing activities. iTernity has, in general, no knowledge of which data the Data Controller stores and whether/how the Data Controller protects these data before these data are written into the storage system.

3. Technical and organizational measures at iTernity

(1) The processes and measures of the Services provided by iTernity are designed in such a manner that they are, from iTernity's perspective, generally appropriate and adequate for the storage of special categories of personal data.

(2) The Client is responsible to review i.e., clarify with the Data Controller, whether the measures described here are sufficient for the specific case of application and the resulting risk for the rights and liberties of the affected data subjects.

This applies, in particular, if data of vulnerable natural persons are processed or special categories of personal data are stored or if personal data is stored for the long-term.

(3) iTernity has internally designated individuals who are responsible for IT security and data protection. iTernity routinely involves external experts for these subjects.

(4) The iTernity IT department has implemented IT security rules and procedures. The internal iTernity IT systems are protected against unauthorized access, manipulation, data loss and malware in accordance with the current state of technology. Use of the internal IT systems is monitored, to the extent required and permitted from a data protection point of view.

(5) All iTernity employees are routinely trained in IT security and data protection matters. Within the scope of the Agreement, iTernity will only use employees that are obligated to confidentiality and that are familiar with the relevant data protection provisions.

(6) If the Client is subject to special confidentiality obligations (professional secrecy holder, telecommunications secrecy, social secrecy):

iTernity instructs all employees to maintain confidentiality with regard to the knowledge obtained. For this purpose, all iTernity employees receive an "Instruction on the Confidential Handling of Personal Data".

The instruction informs them that they must maintain confidentiality with regard to the knowledge they have obtained in the course of their work for a professional secrecy holder. It explains the penalties in the event of non-compliance, including in the event that third parties commissioned by iTernity violate this confidentiality.

iTernity GmbH

Heinrich-von-Stephan-Str. 21
D-79100 Freiburg
Germany

Amtsgericht Freiburg i.Br.
HRB 701332

Steuernummer 06435/43554
Finanzamt Freiburg-Stadt
USt-Id Nr.: DE242664311

Geschäftsführer:
Ralf Steinemann

Bankverbindung:
Commerzbank AG
IBAN: DE37 680800300450056800
BIC: DRES DE FF 680

Tel +49 / (0)761 / 59034 -810
Fax +49 / (0)761 / 59034 -859

www.iternity.com
sales@iternity.com

iTernity GmbH

Heinrich-von-Stephan-Str. 21
D-79100 Freiburg
Germany

Amtsgericht Freiburg i.Br.
HRB 701332

Steuernummer 06435/43554
Finanzamt Freiburg-Stadt
USt-Id Nr.: DE242664311

Geschäftsführer:
Ralf Steinemann

Bankverbindung:
Commerzbank AG
IBAN: DE37 680800300450056800
BIC: DRES DE FF 680

Tel +49 / (0)761 / 59034 -810
Fax +49 / (0)761 / 59034 -859

www.iternity.com
sales@iternity.com

The instruction contains the reference that a right to refuse to testify and a prohibition of seizure exist if iTernity processes data of a professional secrecy holder as a professional assistant with the Client deciding on this.

(7) There are instructions and training courses on the secure handling and operating of IT systems. Observance of instructions, as well as adequacy and effectiveness of the measures as a whole are routinely questioned and improved if needed.

(8) The specific technical and organizational measures are described in the Schedule to the respective Service.

(9) Software, used for remote maintenance or access to remote systems, transfers all data encrypted in accordance with the current state of technology.

(10) Remote maintenance sessions can be recorded to document the proper performance of the work and/or to be in a position to defend against any claims / actions of the Client.

4. Substantiation of iTernity's statutory obligations

(1) iTernity appointed a data protection officer. The data protection officer's contact data are provided at https://iternity.com/en/privacy/.

(2) iTernity has guidelines and controls implemented to ensure that employees process data in accordance with the mandate. Statutory obligations of iTernity remain unaffected.

(3) iTernity ensures compliance with data protection provisions and the committed measures as well as their documentation and verification.

(4) iTernity ensures that identified violations of this Agreement are reported to the Client without undue delay. The Client must ensure that the Data Controller, if different, is informed without undue delay.

(5) Insofar personal data processing by iTernity as a (Sub-)Processor is concerned, iTernity will support the Client in meeting the rights of data subjects, as well as in the Client's reporting of an incident in the case of a data protection violation.

(6) In those cases where a data protection impact assessment (DPIA) is conducted and personal data processing by iTernity as a (Sub-)Processor is concerned, iTernity will support the DPIA.

In those cases where a high risk remains, in spite of the measures taken, iTernity will support the Client or, if different, the Data Controller in the consultation of the data protection authority.

5. Subcontracting relationships

(1) Support for all products and services can be provided by the following service providers (Subcontractor):

ALSO Enterprise Services GmbH
Wegedornstr. 36, 12524 Berlin

ALSO Enterprise Services may connect to the system as part of its support activities, but only after consultation with the Licensee, in the Licensee's presence and after activation by the Licensee.

ALSO Enterprise Services GmbH has been imposed the duties and obligations arising from this agreement and may not engage any subcontractors.

(2) External suppliers / service providers may provide intermediate input for individual services. These "additional subcontractors" (of iTernity) are described in the Schedule to the respective Service, if applicable.

(3) The outsourcing of partial Services to additional subcontractors and/or the exchange of such subcontractors is permitted, if iTernity imposes upon the additional subcontractors all duties under this Agreement and informs the Client of such outsourcing in writing with reasonable advance notice.

(4) If the Client objects for good cause against the involvement of a certain subcontractor, iTernity cannot continue with the provision of the affected Service. In this case, a separate contractual arrangement must be agreed.

6. Control rights of the Client

(1) The Client has the right, in consultation with iTernity, to satisfy itself of the compliance with this Agreement in the course of business operations by way of random controls, which shall generally be notified in due time. The Client must designate the auditors in the individual case.

(2) iTernity ensures that the Client has the option to satisfy itself of iTernity's compliance with the measures. iTernity undertakes to provide the Client, at the Client's request, with the necessary information and furnishes proof of the implementation of the measures.

(3) Intermediate input provided by third parties can generally only be validated by iTernity. iTernity ensures to conduct routine controls of the required measures to achieving the data protection and IT security objectives within the scope of intermediate input.

(4) The Contractor undertakes to provide valid proof of data protection-compliant processing upon request. If the Client nevertheless insists on further or its own random controls, iTernity may demand remuneration in the event of considerable additional expense.

7. The Client's authority to give instructions

(1) The Client has the right to give explicit instructions for data processing. In those cases where an instruction exceeds the agreed scope of Service, the Client is obligated to pay for this additional service.

(2) Instructions may result from the contracted Service itself or may be given in the form of a ticket or by email of the operator or orally within the scope of a support meeting.

(3) For mutual documentation purposes, instructions are given in the form of support tickets or by email. Orally given instructions that have a significant impact on processing, will be promptly confirmed by email.

(4) iTernity informs the Client without undue delay, if from iTernity's perspective an instruction violates data protection provisions. iTernity has the right to suspend performance of such instructions until they have been confirmed or changed by the Client.

8. Copies and erasure of personal data from storage systems

(1) Beyond the subject matter of this Agreement, iTernity may only copy data to systems outside of the storage system based on the Client's explicit instruction.

iTernity GmbH

Heinrich-von-Stephan-Str. 21
D-79100 Freiburg
Germany

Amtsgericht Freiburg i.Br.
HRB 701332

Steuernummer 06435/43554
Finanzamt Freiburg-Stadt
USt-Id Nr.: DE242664311

Geschäftsführer:
Ralf Steinemann

Bankverbindung:
Commerzbank AG
IBAN: DE37 680800300450056800
BIC: DRES DE FF 680

Tel +49 / (0)761 / 59034 -810
Fax +49 / (0)761 / 59034 -859

www.iternity.com
sales@iternity.com

This may be the case for example, if the Client opens a support ticket that requests the recovery of data, because this form of troubleshooting is not performed on the live system.

(2) As a rule, iTernity does not erase any data, because the availability of these data is the essential feature of the Services. Exceptions from this rule are described in the Schedule to the respective Service.

(3) In those cases where user data have been copied onto iTernity systems for analysis within the scope of support cases, such data must be erased if the Client requests erasure or if they are no longer required. iTernity ensures that iTernity can furnish proof of erasure if requested.

(4) iTernity has the right to retain data and documents, required to document data processing as ordered and in due form to the Client, as long as this is necessary for the defense of legal claims. These data do not contain any stored data and contain personal data of the Client only to a marginal extent.

iTernity GmbH

Heinrich-von-Stephan-Str. 21
D-79100 Freiburg
Germany

Amtsgericht Freiburg i.Br.
HRB 701332

Steuernummer 06435/43554
Finanzamt Freiburg-Stadt
USt-Id Nr.: DE242664311

Geschäftsführer:
Ralf Steinemann

Bankverbindung:
Commerzbank AG
IBAN: DE37 680800300450056800
BIC: DRES DE FF 680

Tel +49 / (0)761 / 59034 -810
Fax +49 / (0)761 / 59034 -859

www.iternity.com
sales@iternity.com

GDPR Data Processing Agreement
Schedule to the service "iCAS" (Middleware)

Agreement version: August 12, 2024

iTernity GmbH

Heinrich-von-Stephan-Str. 21
D-79100 Freiburg
Germany

Amtsgericht Freiburg i.Br.
HRB 701332

Steuernummer 06435/43554
Finanzamt Freiburg-Stadt
USt-Id Nr.: DE242664311

Geschäftsführer:
Ralf Steinemann

Bankverbindung:
Commerzbank AG
IBAN: DE37 680800300450056800
BIC: DRES DE FF 680

Tel +49 / (0)761 / 59034 -810
Fax +49 / (0)761 / 59034 -859

www.iternity.com
sales@iternity.com

1. Service specific subject of data processing

(1) The service "iCAS" (Middleware) includes the license for the installation of the software on servers of the Data Controller or a service provider engaged by the Data Controller, as well as the support of the administrators by iTernity.

(2) These servers are located at the premises and the network of the Data Controller or its service provider. The servers are operated by their administrators. The Data Controller / its service provider is the "Operator".

(3) The subject of the data processing as a Processor or Sub-Processor is the support of the administrators

- In the case of data migration during the start up or taking out of service
- Optimization, analysis of defects and troubleshooting (Fix) during operations
- for specific requests, such as targeted erasure of many data records

2. Service specific instructions of the Client to iTernity

(1) Specific instructions must be mandated by the Client in writing. This includes, for example, the request to erase data designated by the Client or the Operator prior to the expiry of their retention period ("Special Delete Tool").

3. Service specific technical and organizational measures

(1) Unless explicitly requested by and agreed with the Operator, iTernity has access to the archive system only after activation in the individual case.

(2) In general, iTernity does not have direct access to the archive system. Rather, the Operator's administrator allows the iTernity employee to access the Operator's PC by remote maintenance and the Operator's administrator establishes a connection to the archive system.

(3) Either the Operator's administrator operates the archive system himself or the Operator leaves the control to the iTernity employee and observes the activities of the iTernity employee. In both cases, the Operator's administrator has full control.

(4) In the case of a defect iCAS object header, it may be necessary to analyze the object at iTernity. For this purpose, defect objects are transferred to iTernity. If the contained data can be recovered, the object is re-transferred and erased at iTernity. Objects that cannot be read, remain with iTernity for further analysis of the defect causing errors.

4. Service specific Subcontractor relationships

(1) Except for ALSO Enterprise Services GmbH, iTernity does not engage any additional service provider.

5. Service specific erasure of personal data

(1) iTernity has in general no access to the archive system and for this reason iTernity cannot – and does not have to – erase any data (e.g., at the end of the Agreement).

iTernity GmbH

Heinrich-von-Stephan-Str. 21
D-79100 Freiburg
Germany

Amtsgericht Freiburg i.Br.
HRB 701332

Steuernummer 06435/43554
Finanzamt Freiburg-Stadt
USt-Id Nr.: DE242664311

Geschäftsführer:
Ralf Steinemann

Bankverbindung:
Commerzbank AG
IBAN: DE37 680800300450056800
BIC: DRES DE FF 680

Tel +49 / (0)761 / 59034 -810
Fax +49 / (0)761 / 59034 -859

www.iternity.com
sales@iternity.com

GDPR Data Processing Agreement
Schedule to the service "iCAS FS" (Scale-Out Platform)

Agreement version: July 07, 2023

iTernity GmbH

Heinrich-von-Stephan-Str. 21
D-79100 Freiburg
Germany

Amtsgericht Freiburg i.Br.
HRB 701332

Steuernummer 06435/43554
Finanzamt Freiburg-Stadt
USt-Id Nr.: DE242664311

Geschäftsführer:
Ralf Steinemann

Bankverbindung:
Commerzbank AG
IBAN: DE37 680800300450056800
BIC: DRES DE FF 680

Tel +49 / (0)761 / 59034 -810
Fax +49 / (0)761 / 59034 -859

www.iternity.com
sales@iternity.com

1. Service specific subject of data processing

(1) The service "iCAS FS" (Scale-Out Platform) includes the license for the installation of the software on one or several servers, as well as installation and operation on servers provided by the Client including their maintenance.

In order to be able to ensure function and availability, the Client has no access to the operating system level as long as iCAS FS is in operation.

(2) The subject of the data processing as a Processor or Sub-Processor is the comprehensive technical operation:

- Installation and administration of the operating system
- Configuration during start-up of service; as option including data migration
- Monitoring, optimization, analysis of defects and troubleshooting (Fix) during ongoing operations
- Special instructions such as the deletion of certain data records

2. Service specific instructions of the Client to iTernity

(1) During standard operations instructions are not necessary. iTernity monitors availability and functionality of the data storage system and optimizes these, if necessary, by means of security and function updates. If problems arise, iTernity analyzes and fixes the causes. If necessary, the Client is informed of measures taken or required decisions.

3. Service specific technical and organizational measures

(1) Login credentials and generated encryption keys are stored in encrypted password databases. Access to them requires personal login and multifactor authentication and exists only for Level 3 support staff.

(2) The Client-specific password database is protected with a 20-character support password. The support password is known only to Level 3 support staff. It is stored in a password database that is secured via multifactor authentication.

(3) If the Client provides a Raid Encryption Licence, content or usage data will be stored in the data carriers of the system in encrypted form. For this purpose, Client-specific encryption keys are generated and stored in the Client-specific password database.

(4) iTernity only accesses the system if the Client requests a change (Service Request) or if the monitoring gives reason to do so (Alert). Access takes place according to the Client's specifications, usually via VPN with password. Data access itself always takes place via an encrypted connection, usually via SSH with function-related user names and an associated password.

(5) To achieve full performance (monitoring, proactive acting), iTernity must have permanent access to the operating system level. If requested by the Client, access can instead only take place on a case-by-case basis after consultation.

(6) Level 1 and 2 support only have access to a tool for standard tasks (e.g. creating a new share). These staff members never have access to any data stored in the system, but only to the system configuration.

(7) Only Level 3 support can have access to content or user data of the system. It only accesses user data if this is absolutely necessary for the task (e.g. for troubleshooting).

(8) Level 3 support only uses company-owned laptops and an infrastructure centrally administrated by iTernity to access the system. Only software required for support tasks is installed on these laptops. The hard drives/SSDs are encrypted, malware protection is active. Software and malware detection patterns are updated automatically.

(9) Access to the system and changes to it are logged: Time, user name, action (e.g. changes to logon data, authorisations, network setup or deletion processes). The access logs are limited in size and are overwritten cyclically.

4. Service specific Subcontractor relationships

(1) Level 3 support is provided exclusively by iTernity staff. Subcontractors take over tasks in Level 1 and Level 2 support.

5. Service specific erasure of personal data

(1) iTernity erases data only if explicitly mandated. At the end of the Agreement, the Client may itself erase its data carriers. The Client should block the network access and instruct iTernity to erase the access data.

iTernity GmbH

Heinrich-von-Stephan-Str. 21
D-79100 Freiburg
Germany

Amtsgericht Freiburg i.Br.
HRB 701332

Steuernummer 06435/43554
Finanzamt Freiburg-Stadt
USt-Id Nr.: DE242664311

Geschäftsführer:
Ralf Steinemann

Bankverbindung:
Commerzbank AG
IBAN: DE37 680800300450056800
BIC: DRES DE FF 680

Tel +49 / (0)761 / 59034 -810
Fax +49 / (0)761 / 59034 -859

www.iternity.com
sales@iternity.com