Fabasoft®

Fabasphere

Performance Characteristics Data Center Operation Public and Government Cloud

Valid from January 1st, 2026

Public

1 Data Locations

A data location is a self-sufficient system operated by the contractor in a specific country. These data locations are currently implemented in Germany, Austria and Switzerland.

At each data location, the Service Package operates in two Data Centers located at a geographical distance of several kilometers from one another in terms of linear distance. This makes it possible to implement disaster-resistant operation measures, e.g. high protection against natural disasters. The Data Centers are designed based on the Tier-III-specifications of the Uptime Institute.

1.1 Security

The Data Centers implement the following minimum-security measures:

- Electromagnetic access system
- Separation system or turnstile
- Video monitoring system
- Around-the-clock (24/7) monitoring of Data Center areas

1.2 Fire protection

The Data Centers implement the following minimum fire safety measures:

- Comprehensive fire alarm system
- Very early smoke detection
- Automatic gas extinguishing system

1.3 Power supply

The Data Centers implement the following minimum measures for power supply:

- Redundant UPS systems
- Redundant diesel aggregates
- Redundant feeds
- Redundant transformers

1.4 Cooling

The Data Centers implement the following minimum measures for air-conditioning:

- Redundant cooling systems

1.5 Connection between Data Centers

The connection between the Data Centers at each data location is established via Ethernet point-to-point networks. The network hardware is designed with redundancy. The connection provides for redundant paths, which are fed into each building at two different points.

The connection between the Data Centers is ensured by the individual Data Center operators. A designated Layer 2 transparent connection is available.

1.6 Hardware and software environment used

The contractor retains its independence. The service package is based on Fabasoft AI Core. Other software products required to operate the service package are open source products wherever possible.

Fabasphere AI Core is operated on the basis of a high-availability hardware environment. The hardware components used are divided into primary components and secondary components.

The Fabasphere AI Core Services are provided on the primary hardware components. The primary hardware components are located redundantly in both data centres.

Data backup is performed on the secondary hardware components. The secondary hardware components are located in a separate fire compartment in one of the data centres.

2 Service levels

2.1 High availability

The Data Centers generally operate 24 hours per day, 7 days per week, 52 weeks per year. The following parameters are provided for each data location and service package within the scope of availability:

- Availability of 99.9% for each observation period (quarter)

Availability is measured by two dedicated external measuring points connected to the internet via independent internet lines. A Service Package is considered available when at least one measurement point is able to gain access.

The calculation is made using the following formula:

$$\text{Uptime} = \text{Possible Available Time} - \text{Maintenance Downtime} - \text{Unexpected Downtime}$$

$$\text{Availability} = \frac{\text{Uptime}}{(\text{Possible Available Time} - \text{Maintenance Downtime})}$$

The calculation process therefore excludes the availability during planned maintenance (Maintenance Downtime).

The following times are reserved for maintenance windows:

- Saturday from 12 a.m. to Monday at 7 a.m. CET/CEST.
- In urgent cases and with prior notice

These reserved windows will only be used for maintenance work as required. Should maintenance work be required, prior notice and documentation will be provided the CSA Information Sheet under "Additional Helpful Links", "Cloud Services/System Status".

An availability report will be generated per calendar month and provided electronically to the Customer at the end of each month at the website listed in the CSA Information Sheet under "Additional Helpful Links", "Cloud Services/System Status".

2.2 Resilience / Response times

The response times of all incoming requests are measured directly at the load balancer of the Fabasoft Cloud Service using Fabasoft app.telemetry. An HTTP, CalDAV or WebDAV request received at the load balancer is considered a request.

The following parameters are provided for each data location and service in terms of response time behaviour:

- Average response time of all requests of less than one second per observation period (quarter)

A report on response times is generated per calendar month and made available to the Customer electronically at the end of the month at the website listed in the CSA Information Sheet under "Additional Helpful Links", "Cloud Services/System Status".

Since a request at the web browser can initiate multiple requests against the load balancer, the response times at the web browser are also documented in this report for transparency reasons.

2.3 Data security

2.3.1 Service Package

Metadata, structured data and content/documents are stored in the scope of the operation of the Service Package. This data is stored redundantly on the primary hardware components for each location.

The metadata and structured data are stored in relational database systems and synchronously mirrored to distributed database servers on the primary hardware components. At least once a day, a full backup of the metadata and structured data is performed in the scope of database backups to dedicated backup systems on the secondary hardware components. In addition, transaction logs are also backed up to these backup systems on an ongoing basis.

The content/documents in the file system are stored in parallel on at least three file servers (two on the primary hardware components, one file server on the secondary hardware components). At least once a day, the contents/documents are fully synchronised with additional backup systems on the secondary hardware components at a data location.

The content/documents are regularly checked for malware by an automated malware scanning service. Any findings are reported to the administrators of the affected Fabasphere organisation by email. The Customer is responsible for cleaning up the infected files, as the Contractor has no access to them. An audit of files uploaded in the last 31 days is performed once a week. In addition, all files are checked once per month.

The following parameters are provided in the scope of data security:

- Recovery Point Objective (RPO): The maximum time period for which data is lost in the event of a disaster recovery is 30 minutes.

- Recovery Time Objective (RTO): In the event of a disaster recovery, the maximum time for restoring services, from the availability of the network, hardware and software infrastructure, is 48 hours.
- Retention Time: Each backup is retained for a minimum period of 4 months up to a maximum of 6 months.