Performance Characteristics Data Security

for a Service Package on Fabasoft PROCECO

Valid from January 1st, 2025
Public

To aid readability, the third-person plural pronoun will be used
instead of gendered pronouns (e.g. they/them instead of he/him).

These plural pronouns shall be used for both
singular and plural references, encompassing all genders.

1 Introduction

The performance characteristics of data security in the Service Package are described below.

Customers can contact the Contractor via the e-mail address given in the CSA Information Sheet under “Possible Contacts”, “Data Privacy” in case of any questions regarding the processing of personal data. This contact option is also available for notification and communication in the event of security or data protection incidents.

2 Performance

2.1 Reversibility and the termination process

Subject to a term of at least four months and no more than six months after contract termination, the contractor shall be explicitly authorized to permanently delete data saved by the customer in the data locations – i.e. in such a way that the process cannot be reversed. The customer shall be informed upon signing the contract and shall receive a reminder before the termination date (see Cloud Service Agreement, Clause 4.6).

Objectives	
Period of access to user data (data retrieval period)	Upon termination of the contract, the contractor deactivates the customer's access to the service package upon termination of the contract. See Cloud Service Agreement, Clause 4.6
Period of retention of user data (data retention period)	In case of termination of the contract, the contractor is entitled to delete the user data at the earliest four months and at the latest six months after termination of this contract. See Cloud Service Agreement, Clause 4.6
Additional retention of user data (residual data retention	If requested by the Customer in a written declaration to the Contractor by email within four months after contract termination, the Contractor is prepared to transfer data specifically designated by the Customer, that the Customer had stored in accordance with this contract, on machine-readable data carriers, in exchange for a fee to be decided on an individual basis, within a period of at least four months and no more than six months after the termination of this Contract. See Cloud Service Agreement, Clause 4.6

3 Security

3.1 Authentication and authorization

Depending on the selected service package, different two-factor authentication methods are available. These are recorded in the Fabasoft Cloud's SPI.

Authentication

Teamrooms are used to authorize access to user data. Team members can be granted access rights (read access, change access, full control) for each Teamroom. The search for user data takes place in accordance with the access rights. It only displays results that the respective user is allowed to access.

A user with full control can configure a Teamroom to allow so-called “public links” in that Teamroom. A public link allows access to the Teamroom, a folder, a document or any other content in the Teamroom without prior authentication; only a knowledge of the link is required. In addition, a public link can be given a password and a validity period. These parameters are checked when the link is accessed; access is denied by the system if the validity period has expired and/or the password is not entered correctly. If there is a public link to a Teamroom or folder, the entire contents of the Teamroom or folder can be accessed via these public links.

Access to the service package with third-party applications that only support a username and password without a second factor (e.g. connecting as a network drive) must be done using specially generated passwords. A validity must be set for the passwords. These passwords for applications can be extended by the user during their validity and revoked during their validity.

3.2 Encryption

Access to the service package is only possible via HTTPS with TLS encryption.

The user data is stored on encrypted hard disks (SEDs) that at least meet the FIPS 140-2 Level 2 standard or a comparable standard, encrypted file systems or encrypted data carriers. This ensures that the data is protected even if the hardware is lost.

The Fabasoft Secomo product (including hardware security module), which has to be purchased separately, extends the service package to include end-to-end encryption for highly sensitive documents. With Fabasoft Secomo, user data is decrypted directly and exclusively at the user's workstation.

3.3 Logging and monitoring

Auditing

As part of the traceability, the auditing information is collected in accordance with the SPI of the Fabasoft Cloud. The following auditing information is collected:

Depending on the service package, users in Teamrooms with full control can access the audit log reports. Audit log entries are saved for at least 13 months. The customer has the option to export the audit log entries and store them separately. The audit log entries will be permanently deleted at the conclusion of this contract at the latest, together with the user data, after a period of at least four months and no more than six months (calculated from the date of contract termination).

Logging

Fabasoft app.telemetry records every request (HTTPS requests) to the service package over time. This transaction information is collected in the user's web browser and in the cloud client or mobile apps, as well as in the services and system components of the Fabasoft Cloud. This transaction information is used exclusively for the continuous improvement of the services. The logging does not include any user data. The retention period for this transaction information is defined individually for each application and level and is a maximum of 13 months.

The information that the respective systems provide by default is logged as part of the logging of operating system and basic software events as well as application-specific events. Operating system, basic software events and application-specific events are stored for a maximum of 13 months.

Monitoring

Fabasoft app.telemetry is used to monitor the individual system components of the Fabasoft Cloud and to monitor performance and availability from the user's perspective.

Security-related user data is not logged. Access to auditing information is possible for appropriately authorized users of the customer in the web client, where exporting the auditing information is also possible. The retention periods for logs are 13 months (for audit logs) and 14 days for logging data from monitoring.

3.4 Governance

Scheduled maintenance work will be announced in the CSA Information Sheet under “Additional Helpful Links”, “Cloud Services/System Status” at least 14 days in advance. In urgent cases (e.g. risks associated with delay), maintenance work may be performed ad hoc.

The new features for each update will be documented in the “What’s New” document and made available in the CSA Information Sheet under the given website “Additional Helpful Links”, “What’s new”.

4 Data management

4.1 Data classification

User data

Data which the customer imports into the service package or creates in the service package is stored in Teamrooms which are assigned to a Fabasoft Cloud organization. The owner of the Fabasoft Cloud organization has all rights to the data which is stored in it. Through the access rights defined for the Teamroom, the owner or the organization member who creates the Teamroom can define who has access to this data and who is allowed to change or delete it.

User data is not synchronized between locations, but remains in the location of the Teamroom in which it was stored. To ensure availability, the contractor can set up the storage of a copy (backup) of the user data in a different location (see chapter 5.6).

The customer's user data remains exclusively in the customer's power of disposal and is neither known to the contractor nor is it subject to direct access by the contractor without the customer's express authorization.

Contact data

Required contact information:

email address (login), first name, last name, organizations, location, login information (time of login, time of logout, time of last access, authentication method and type, workplace, IP address), assigned solutions, assigned apps, membership status, last status change, last login (date and location)

Optional contact data for a contact:

photo, additional first names, title, additional title, gender, birth date, form of address, function in the organization, assignment to organizational units (organizational unit and role), assignment to teams, assignment to external organizations, language, registration status, addresses, phone numbers, e-mail addresses, website, standard method for two-factor authentication, cell phone number for mobile PIN, Email address for mobile PIN, User ID at RADIUS server, Primary organization for RADIUS server (DN), Device ID, E-mail address (E)/Common Name (CN) (certificate login), Primary organization for certificate authentication (DN), Primary organization (DN), Digital ID data (ID, first name , Last Name), Password, Active Directory Entity ID, SAML 2.0 Entity ID, OpenID Connect Primary Organization (DN), Authentication Alternative Email Address, External IDP ID, Authentication Methods Disabled, VCF File, Policies, Import Identifier, Delegate, Marketing Campaign Code, Notes, Subject

General contact data of a contact:

photo, first name, middle names, last name, title, additional title, gender, salutation, email domain, organization, function in organization, assignment to organizational units, assignment to teams, assignment to external organizations, language of communication, registration status

Working environment

Configuration settings for the contact (e.g. language, locale, default currency, settings for accessibility, etc.)

Contact data of a cloud organization:

name, billing address, VAT registration number, service packages, members, organizational units, teams, external members, external organizations, default Teamrooms, default data location, addresses, phone numbers, e-mail addresses, logos, owners, administrators, e-mail domains, support coordinator, compliance manager, support team, process administrators, persons to notify in the event of a personal data breach (first name, last name, postal address, email address, URL for data protection information), email communication in connection with organization administration, withdrawals, purchases, guidelines, encryption, authentication settings, security settings and other configuration settings

Contact data of organizational units:

name, members, administrators, addresses, phone numbers, e-mail addresses, standard Teamrooms, hierarchy level, departures, import ID, security settings and other configuration settings

Contact data of teams:

name, members, administrators, addresses, phone numbers, e-mail addresses, standard Teamrooms, departures, import ID, security settings and other configuration settings

Contact data of external organizations

Name, members, administrators, addresses, phone numbers, e-mail addresses, logos, standard Teamrooms, security settings and other configuration settings.

Contact data for collaboration in the service package are captured in the following situations:

- A future customer enters their contact data during the registration process.
- Contact data of internal and external organization members of a customer are captured by authorized users of the Fabasoft Cloud organization, as well as by organization members when defining access rights to a Teamroom.
- Authorized users for entering contact data are administrators, co-owners and owners of the cloud organization, as well as users who have been granted the authorization via policies in the cloud organization.

Contact data can be changed and corrected by authorized persons of the Fabasoft Cloud organization to which the contact belongs.

Contact data of contacts who have not yet registered in the Fabasoft Cloud can be changed, corrected and deleted by the person who entered the contact data.

The contact itself can also change and correct its contact data after registration in the Fabasoft Cloud, or it can be deleted via the support button in the Fabasoft Cloud. Contact data is not generally visible. Contact data is identified by the complete e-mail address. If, when a contact is entered, the Fabasoft Cloud detects that contact data has already been entered for the e-mail address entered, the user is given access to the general contact data.

The general contact data can also be viewed by other team members in the context of the Teamroom, unless the Teamroom has been configured differently.

When a Mobile PIN is sent, the phone number of a contact is transmitted to the SMS provider.

The contact data, with the exception of the login information, is synchronized across all Fabasoft Cloud locations.

Commercial data

Commercial data is information required for the processing of the business relationship with the customer (orders, invoices, utilization information of the licensed service packages per organization, etc.)

Derived data

Derived data is log and transaction information that does not include user data. This information is used solely for the purposes of maintaining operations, complying with service levels and continuously improving services.

4.2 Areas of responsibility

The Customer's user data shall remain solely within the Customer's control. The Customer itself is responsible for the lawfulness of processing this data, as well as the data protection obligations associated with data processing.

In cases in which the Contractor acts as processor for the Customer, processing of data that is passed from the Customer to the Contractor takes place exclusively on instruction by the Customer. The Contractor shall support the Customer in exercising their data protection obligations. The Customer's obligations as a data controller, and those of the Contractor as a processor, are defined in the document "Data Processing Agreement".

4.3 Data lifecycle

User data can be permanently deleted by the Customer (emptying the recycle bin, deleting a Teamroom). As of this point, it is no longer possible to access this data (metadata and documents). Metadata and references to documents are deleted immediately; the documents themselves are deleted after four months at the earliest and six months at the latest.

4.4 Data portability

Documents in a Teamroom can be exported by the customer as a structured ZIP archive (accessed via https) or via WebDAV. Metadata can be accessed via CMIS (Content Management Interoperability Services). It is not possible to export all historical versions of a document in their consolidated form.

5 Personal data protection

5.1 Codes of conduct, standards and certification mechanisms

Insofar as the data includes "personal data" as defined by the EU-General Data Protection Regulation or the respective national data protection laws, the Contractor shall adhere to data secrecy and all other statutory data protection regulations within the meaning of the applicable EU standards and the substantive data protection regulations of the respective countries.

Objectives	
Codes of conduct, standards and certification mechanisms	EU standards and the national data protection laws are observed

5.2 Specification of the intended use

The contractor processes personal data for no other purpose than requested by the customer and required to fulfill the contract.

Objectives	
Purpose	to fulfill the contractual obligations with the customer (Art. 6 (1) (b) GDPR); to take steps at the request of the data subject prior to entering into a contract (Article 6 (1) (b) GDPR); for the purpose of the legitimate interests of our company or legitimate interests of third parties (Art. 6 (1) (f) GDPR), namely • for the purpose of direct advertising with regard to Fabasoft products and services; • for the purpose of preventing cases of abuse; • for the purpose of internal administration; • for ensuring network and information security; • for archiving purposes.

Any contact data received by the Contractor in the course of their contractual relationship with the Customer will be processed by the Contractor in order to send emails, letters or advertising brochures to Customers for the purpose of depicting and presenting products of the Contractor (Art. 6 (1)(f) GDPR). The Customer has the right to object to this processing of the Customer's contact data for the purpose of direct advertising; this right can be exercised at any time without giving reasons by means of a letter to the Contractor or via email to the address given in the CSA Information Sheet under "Possible Contacts", "Data Privacy". The Contractor will process the Customer's contact data for this purpose for as long as the Customer lodges no objection, however, up to a maximum of three years after their last activity. Where other forms of direct advertising are concerned, the Contractor will only process the Customer's contact data if the Customer has given their express consent to the processing of their data (Art. 6 (1) (a) GDPR). If the Customer has given their consent to the data processing, they can revoke this consent without giving reasons by means of letter to the Contractor or via email to the address given in the CSA Information Sheet under "Possible Contacts", "Data Privacy". **The processing of the Customer's personal contact data for the purpose of direct advertising is not necessary for the execution of the contractual relationship.**

The Customer's contact data is not processed for any other purpose.
The following sections list the data that shall be stored and processed.

5.2.1 User data

The user data shall remain exclusively under the control of the customer and is neither known to the contractor in terms of content nor is it subject to direct access by the contractor without the express authorization of the customer.

The Contractor will only process user data in exceptional cases on the basis of an express written request and/or approval for the specific user data to be processed, given by the

Customer. Fabasoft Cloud shall process user data exclusively for the purposes requested by the Customer in compliance with the Cloud Service Agreement framework agreement and/or the Customer's instructions.

5.2.2 Collaboration

To support collaboration between users, a user's general contact information is visible to another user if the user knows the other user's email address.

5.2.3 Support

The Contractor provides 1st level support for their customers. Users can file a support request at any time using the Support button in the web interface, the Cloud Client or the mobile apps for iOS and Android. By using the Support button, the user's name, email address and problem description are submitted to the support of the Contractor. For better traceability of the problem, the user also has the option to send a screenshot. In the Cloud Client, system information about the workstation and log files can also be added. This data and the subsequent communication are collected in a support request. The user can access their support requests at any time via the menu item "My Support Requests" in the account menu.

Access to the support requests and the data transmitted during their processing is restricted to the support employees of the Contractor of other sub-processors concerned with support performance and the person submitting the support request.

5.2.4 Cookies

After you have logged in, Fabasoft Cloud Services use so-called "session cookies" to identify you during your visit. The session cookies contain parts of your registration data in encrypted form. After the end of the session, session cookies automatically expire.

The Contractor's Fabasoft Cloud Services use "permanent cookies" to store information about users who repeatedly access Fabasoft Cloud Services. The purpose of using these permanent cookies is to continuously improve our products and services for you and to make them easier to use. An individual profile of your usage behavior is not created.

5.3 Data minimization

The Contractor will store personal data only for as long as is necessary for the purpose for which the data was collected.

In the service package, temporary files and documents are generally deleted after use. For reasons of stability, no further garbage collection is implemented, especially since no personal data is affected.

5.4 Openness, traceability and announcement management

The Contractor shall not make your data available to a third party, except in the event of a statutory obligation or if you make such a request, i.e. with your consent. This will be the case, for example, when sending an invitation to a Teamroom or when purchasing a Cloud App from a third-party manufacturer.

The list of sub-processors to whom data is forwarded or transferred is available online at the website provided in the CSA Information Sheet under "Link to Basis of the Contract".

5.5 Accountability

If the Contractor observes unauthorized access to the user data of the Fabasoft Cloud organization or the contact data, or if there is sufficient justified suspicion, the person named in the data protection settings of the Fabasoft Cloud organization will be informed either by registered letter or by e-mail. In addition, the Contractor will attempt to contact this person as soon as possible by telephone or by e-mail.

5.6 Geographical location of data

The Customer can choose between different locations (contractual location) for storing user data (Teamrooms, folders, documents, etc.). It is only possible to choose a location other than the contractual location on the basis of a special, separate, written agreement.

The data regarding the user, the Fabasoft Cloud organization and the organizational unit (contact data) is replicated and synchronized across all locations (Germany, Austria, Switzerland). You can find a list of all relevant data in Section 5.2 “Specification of the intended use”. Settings in the user’s work environment are also synchronized if users have changed their location.

Data sent to sub-contractors is processed according to the conditions laid out by the sub-contractors (see Section 5.4 “Openness, traceability and announcement management”).

In artificial intelligence applications, parts of user data can be exchanged between locations for processing by large language models by the Contractor as part of “retrieval augmented generation” (RAG).

5.6.1 Data transfer/download in third countries

The Contractor processes data in Austria, Germany and Switzerland. As such, the Contractor will generally not transfer data to third countries.

The user data shall remain solely within the Customer’s control and the Contractor shall not know the content of this information, nor shall they have direct access to it.

If the Customer uses the Service Package on a terminal device in a third country, this may result in a data transfer to a third country by the Customer. In such a case, the Customer itself is responsible for adhering to the applicable data protection regulations.

5.7 Intervenability/statutory data protection rights

The applicable data protection law grants the customer various rights in connection with the processing of his personal data. In particular, the customer can request information about which data (= contact data) the contractor processes about him (see Art 15 GDPR for details). He can have his data (= contact data) stored in the Fabasoft Cloud restricted (blocked, see Art 18 GDPR), corrected or deleted by the contractor's support team (see Art 16 GDPR). The customer has the right to object to the data processing (see Art. 21 GDPR) and the right to data portability (Art. 20 GDPR).

User data can only be read, corrected or deleted by the customer himself or by users that the customer has authorized in the Teamrooms that contain the user data.

Should there be a violation of the customer's right to lawful processing of his data, despite the contractor's obligation to process the customer's data lawfully, the customer has the right to

file a complaint with the Austrian Data Protection Authority or with another data protection supervisory authority in your country, in particular at your place of residence or work.

Objectives	
Response time	Contact information for Support and support times are defined. (see Performance Characteristics Data Center Operation)

5.7.1 Customer self-service

The user data remains exclusively within the customer's power of disposition and is neither available to the contractor nor is it directly accessible to the contractor without the customer's express authorization. This user data can therefore only be managed (e.g. deleted, etc.) by the customer themselves.

The customer can access instructions via the settings in the service package, which, among other things, enables him to query his contact data and edit it directly himself. The customer can have his contact data deleted, corrected, anonymized or transferred via the support team, in accordance with data protection regulations.