Performance Characteristics Data Security

for a Service Package on Fabasoft PROCECO

Valid from January 1st, 2024

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 email 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)	Should the contract be terminated, the Contractor shall deactivate Customer access to the Service Package at the end of the contract period. See Cloud Service Agreement, Clause 4.6
Period of retention of user data (data retention period)	Should the contract be terminated, the Contractor is authorized to delete the user data within a period of four to six months after the contract has ended. See Cloud Service Agreement, Clause 4.6
Continued 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 Service reliability

The Service Package of the Contractor is designed to offer 99.9% availability for each observation period (quarter). For more information on this topic, see the document “Performance Characteristics Data Center Operation”.

Objectives	
Redundancy	See Performance Characteristics Data Center Operation
Service reliability	See Performance Characteristics Data Center Operation

3.2 Authentication and authorization

The following two-factor authentication methods are available (depending on the service package selected).

Authentication

- Username and password
  - The username is the user’s valid email address.
  - If a user has forgotten their password, they can set a new password via a link sent to their email address. The option to set a new password is offered during the login process.
  - The Contractor does not save the password in plain text and cannot reproduce it.
- Client certificate
  - The root certificate of the CA (Certificate Authority) and all intermediate CAs must be configured by the Customer’s administrator in the Fabasoft Cloud Organization to ensure that the client certificate can be validated during user authentication.
  - The Customer must configure access to a block list in the Fabasoft Cloud Organization. Should the Customer choose to deactivate the client certificate, the client certificate to be deactivated must be placed on this block list.
- Single sign-on (active directory)
  - The Customer must operate an AD FS (Microsoft Active Directory Federation Services), which is made available over the internet by Fabasoft Cloud. The authentication service for the Fabasoft Cloud must be configured as a “Relying Party Trust” in the Customer’s AD FS in the Fabasoft Cloud. The metadata (FederationMetadata.xml) of the AD FS necessary for the configuration in the Fabasoft Cloud Organisation must be provided by the Customer.
- Single sign-on (SAML 2.0)
  - The Customer must operate an SAML 2.0 Identity Provider, which is made available online by Fabasoft. The Fabasoft Cloud authentication service must be configured as the Service Provider in the Customer’s Identity Provider. The Identity Provider metadata

(metadata.xml) necessary for the configuration in the Fabasoft Cloud must be provided by the Customer.

Second factor (if the authentication process is not based on two factors)

- Mobile PIN (text message)
  - A five-digit number (PIN) is sent to the user’s telephone number. The user must enter this number after logging in using the first factor.
  - This PIN is valid for five minutes.
  - The text message for the two-factor authentication is sent via external processors, for which the message is delivered via the Customer’s mobile phone operator or via a roaming partner of the mobile phone operator. Therefore, personal data required for the delivery is transferred to the aforementioned external processor. For Customers with a mobile phone number from third countries or if the Customer is in a third country, the personal data required to deliver the message will be transferred to a mobile operator or roaming partner established in that third country.
- Email PIN
  - A five-digit number (PIN) is sent to the user’s email address. The user must enter this number after logging in using the first factor.
  - This PIN is valid for five minutes.
- Single-use password via the RADIUS server
  - The Customer must operate a RADIUS server, which is made available online by Fabasoft Cloud. The access data to the RADIUS server must be configured by the Customer’s administrator in the Fabasoft Cloud Organization.

The Customer’s administrator in the Fabasoft Cloud Organization can configure the authentication parameters for the members of the Customer’s organization or external organizations. In particular, these parameters include the phone numbers or email addresses for mobile PIN and email PIN access. The administrator can also decide which methods the members can choose from and which they should priorities for the second factor.

Authorization

Access to user data shall be authorized via Teamrooms. Team members can be granted specific access rights (reading rights, editing rights, all rights) for each Teamroom. Searches for user data take these access rights into account. The search will only produce hits for which the user has access rights.

A user with all rights can configure a Teamroom in such a way that “public links” are allowed in this Teamroom. A public link allows access to the Teamroom, a folder, a document or any other content in the team room without prior authorization to all those with the exact link. A validity period and a password can also be specified for the public link. When a user attempts to access the link, the system checks these parameters. If the validity period has expired or if the password is incorrect, the system blocks access to the link. A public link to a Teamroom or a folder provides access to the entire contents of the Teamroom or folder via the link.

When accessing the Service Package using third-party applications that only require a username and password without a second factor (e.g. connecting as a network drive), specifically generated passwords must be used. The passwords must be assigned a validity period. Users can extend the validity period of the password either before or after it expires or cancel the password before it expires.

Objectives	
Security of the authentication processes	State-of-the-art technology
Authentication process	Username and password, client certificate, Single sign-on (Active Directory), Single sign-on (SAML 2.0) Generally, two-factor authentication
Rights revoked if the organization is excluded	Immediately upon deactivation of the user account by the Customer's administrator
Protection of login data	Passwords for login are encrypted using a separate service and are not saved in a way that allows them to be reproduced.
Support for third-party authentication processes	AD FS, SAML 2.0 RADIUS server for second factor

3.3 Encryption

Users must access the Service Package via HTTPS with TLS encryption.

User data is stored on encrypted hard drives (SEDs) with a minimum standard of FIPS 140-2 Level 2 or a comparable standard, or on encrypted file systems (EFS). This protects the data in case the hardware is lost.

The "Fabasoft Secomo" appliance (incl. hardware security module), which is available separately, expands the Service Package to include end-to-end encryption for highly sensitive documents. Fabasoft Secomo directly and exclusively decrypts the user data at the user's workstation.

Objectives	
Protection against brute force attacks	Transport: HTTPS with TLS encryption Storage: SEDs, EFSs
Key security	Keys are generated on the target system and do not leave the target systems. Access to keys is restricted using restrictive access rights (TLS) or passwords (for example, SEDs or EFS).
Use of high-security modules	Available in connection with "Secomo" as a separate Fabasoft product.

3.4 Logging and monitoring

Auditing

The following auditing information is collected for the purpose of traceability:

- Access to documents (read and edit authorizations)
- Changes to metadata
- Dissolution of Teamrooms and deletion of documents
- Deletion of a Teamroom’s history
- Access to public links
- Export of contact management metadata

Depending on the Service Package, users in Teamrooms with all rights can access the audit log evaluations. Audit log entries are stored for a minimum of 13 months. The Customer has the option of exporting the audit log entries and storing them separately. The audit log entries shall be permanently deleted on termination of this contract together with the user data after a period of at least four months and no more than six months (calculated from termination of the contract).

Logging

Fabasoft app.telemetry records every request (HTTPS requests) sent to the Service Package in chronological order. This transaction information is collected at the user’s workstation, both in the web browser and in the Cloud Client or in the mobile apps as well as in the Fabasoft cloud services and system components. This transaction information is used exclusively for the continuous improvement of the services. User data is not logged. The retention period for this transaction information is defined individually depending on the application and level and shall not exceed 13 months.

The information that is available to the respective systems by default is logged within the framework of the logging of the operating system, the basic software events and application-specific events. The operating system, basic software events and application-specific events are stored for a maximum of six months

Monitoring

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

Objectives	
Selection of data in the log	Security-related user data is not logged
Customer access to logs	Users with the proper authorization can access auditing information in the Web Client. Users can also export this auditing information.

3.5 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”.

Objectives	
Announcing changes	Link to the “What’s new” document pursuant to the CSA Information Sheet Link to the “Basis of the Contract” pursuant to the CSA Information Sheet in the latest valid version

4 Data management

4.1 Data classification

User data

Data placed in the Service Package by the Customer or data created in the Service Package is saved in Teamrooms assigned to a Fabasoft Cloud organization. The owner of the Fabasoft Cloud organization holds all rights to the data stored there. The owner or the member of the organization who created the Teamroom can define who has access to this data and who can change or delete this data by defining the access rights for the Teamroom.

User data is not synchronised between locations, but remains in the location of the Teamroom in which it was saved. To ensure availability, a copy (backup) of the user data can be saved in another location (see Chapter 5.6).

The Customer’s user data shall remain solely within the Customer’s control. The Contractor shall not know the content of this information, nor shall they have direct access to it, without the express authorization of the Customer.

Contact data

Contact data for collaboration in the Service Package is collected in the following circumstances:

- A future Customer provides their contact data as part of the registration process.
- The administrator of the Fabasoft Cloud organization collects the contact data of internal and external members of the organization.
- Contact data from external members of an organization can also be collected by members of the Fabasoft Cloud organization when defining access rights for a Teamroom.

Administrators of the Fabasoft Cloud organization to which the contact belongs are generally authorized to change and correct contact data.

Creators of the contact data can change, correct and delete the contact data of contacts that are not yet registered in the Fabasoft Cloud.

Once registered in the Fabasoft Cloud, contacts can change and correct their own contact data or request that their data be deleted using the Support button in the Fabasoft Cloud.

Contact data is not generally available to be viewed. Contact data is identified using the contact's full email address. If, when setting up a contact, the system detects that contact data already exists for the email address that has been entered, the user will be provided with access to the general contact data (photo, first name, middle names, surname, title, post-nominal title, gender, date of birth, salutation, email domain, website, organization, role in the organization, assignment to organizational units, assignment to teams, assignment to external organizations, language, registration status).

This general contact data is also visible to the other team members in the Teamroom unless the settings for the Teamroom have been configured not to allow this.

When a mobile PIN is sent to the user, the phone number of a contact is sent to the SMS provider.

The contact data is synchronized across all Fabasoft Cloud locations.

Commercial data

Commercial data is information required to establish a business relationship with the Customer (orders, invoices, capacity information for the licensed service packages for the organization, etc.).

Derived data

Derived data refers to log and transaction information that does not include user data. This information is used exclusively to maintain operation and service levels and to promote continuous improvement of services.

Objectives	
Processing of user data	Data is processed only as requested by the Customer
Processing derived data	Data is processed only as requested by the Customer

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

Objectives	
Type of deletion	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 or via WebDAV. The user can access metadata via CMIS (Content Management Interoperability Services). It is not possible to create a consolidated export of all past versions of a document.

Objectives	
Document formats	Original document formats XML for metadata via CMIS
Interfaces	HTTPS, WebDAV, CMIS

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 Purpose specification

Fabasoft processes personal data for no other purpose than that necessary to meet the requests of the Customer and to fulfill the contract.

Objectives	
Purpose	for the performance of the contract to which the Customer is party (Art. 6 (1)(b) GDPR); in order to take steps prior to entering into the contract (Art. 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 solely within the Customer's control. The Contractor shall not know the content of this information, nor shall they have direct access to it, 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 Contact data

Organization:

Name, billing address, VAT ID No., service packages, members, organizational units, teams, external members, external organizational units, standard Teamrooms, addresses, phone numbers, email addresses, logos, owners, administrators, email domains, support coordinator, compliance manager, support team, email communication in connection with organisation management, resignations,purchases, policies, encryption settings, authentication settings, security settings and additional configuration settings

Organizational units:

Name, members, standard Teamrooms, hierarchy level, departures, import ID, security settings and additional configuration settings

User (mandatory data):

Email address (login), first name, surname, organizations, location, login information (time of login, time of logout, time of last access, authentication method and type, workstation, IP address), assigned edition, assigned apps, membership status, last status change, last login (date and location)

User (optional data):

Photo, middle names, title, post-nominal title, gender, birth date, salutation, role in the organization, assignment to organizational units, assignment to teams, assignment to external organizations, language, registration status, addresses, phone numbers, email addresses, website, mode of dispatch for mobile PIN, mobile phone number for mobile PIN, email address for mobile PIN, user ID for RADIUS server, common name (certificate login), digital ID data (ID, first name, surname), password, deactivated authentication methods, policies, import ID, deputy, subject

Work environment

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

5.2.3 Collaboration

To enable users to collaborate, the following data is visible for a user if the user knows the email address of another user:

Photo, first name, middle names, surname, title, post-nominal title, gender, date of birth, salutation, email domain, organization, role in the organization, website, assignment to organizational units, assignment to teams, assignment to external organizations, language, registration status, import ID

5.2.4 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.

5.2.5 Cookies

After you have logged in, Fabasoft Cloud Services use “session cookies” which can identify you during your visit. These session cookies contain elements of your login data in encrypted format. Session cookies expire automatically at the end of the respective session.

Fabasoft Cloud services of the Contractor use “permanent cookies” to obtain information about users who repeatedly access Fabasoft Cloud services. The reason for using these permanent cookies is so that we can constantly improve our products and services and make them easier for you to use. We do not create individual profiles of your usage behavior.

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.

Objectives	
Retention period for temporary data	In the Service Package, temporary files and documents are generally deleted after they have been used. For reasons of stability, no additional garbage collection system is implemented, particularly because no personal data is involved.
Retention period for personal data	End of contract: see Cloud Service Agreement Otherwise: When data is deleted by Customers

5.4 Openness, transparency and notice

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 has detected unauthorized access to the Fabasoft Cloud organization’s user data or contact data or if there is reasonable suspicion of this, the person named in the Fabasoft Cloud organization’s data protection settings shall be informed via registered mail or by email. In addition, the Contractor shall attempt to contact this person as quickly as possible by phone or email.

Objectives	
Guidelines for data theft	See text of this section.
Documentation	Summary of Certifications and Audits Performance Characteristics Data Security Performance Characteristics Data Center Operation

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 "Purpose specification". 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, transparency and notice".

Objectives	
List of available locations	Germany, Austria, Switzerland
Possible options for locations	Can be selected for the Customer's user data To ensure availability, a copy (backup) of the user data can be saved in another location. Contact data is synchronized between all Fabasoft Cloud locations

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

Customers can demand information about which data (= contact data) concerning them is processed by the Contractor (see Art. 15 GDPR for more details). The Customer can have the data saved in the Fabasoft Cloud (= contact data) restricted (blocked see Art. 18 GDPR), rectified or erased (see Art. 16 GDPR) by the Contractor's Support. The Customer has the right to object to the data processing (see Art. 21 GDPR) and the right to data portability (see Art. 20 GDPR).

User data can only be read, rectified and erased by the Customer or by users authorized by the Customer to access the Teamroom containing the user data.

In the event of an unexpected breach of the Customer's right to lawful processing of their data, despite the Contractor's obligation to process the Customer's data in a lawful manner, the Customer has the right to lodge a complaint with the Austrian Data Protection Authority or with another data protection supervisory authority in the EU, in particular at their usual place of residence or place of 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 shall remain solely within the Customer's control. The Contractor shall not know the content of this information, nor shall they have direct access to it, without the express authorization of the Customer. It is therefore only possible for the Customer itself to manage this user data (e.g. delete it, etc.).

Using the settings in the Service Package, the Customer can access instructions on how, for example, to autonomously request their contact data and to edit this data itself. Taking into account the data privacy regulations, the Customer can use Support to erase, rectify or anonymize their contact data, or to have it transferred.