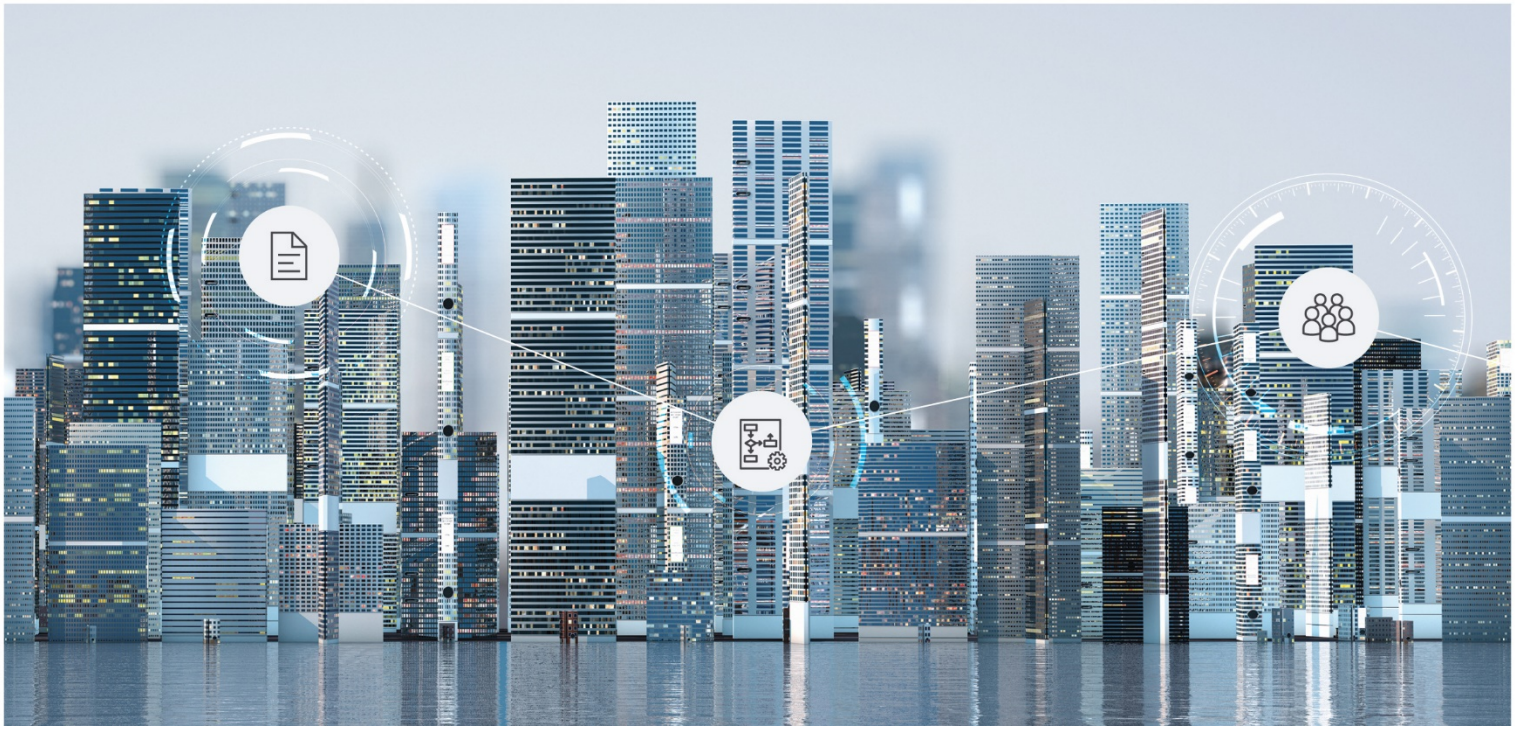
Fabasoft



Performance Characteristics Data Security

Fabasoft Cloud

Valid from January 1st, 2021

Confidential

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 protection of personal data and the protection of information customers store in Fabasoft Cloud is of paramount importance to Fabasoft. In this document, Fabasoft records the ways in which the Fabasoft Cloud protects and processes data and how this data can be exchanged with other users.

Fabasoft Cloud customers can contact Fabasoft using the following e-mail address privacy@fabasoft.com 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, Fabasoft shall be explicitly authorized to permanently delete data saved by the customer in the Fabasoft Cloud Data Centers – 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, Section 4.6).

Objectives	
Period of access to user data (data retrieval period)	Should the contract be terminated, Fabasoft shall deactivate customer access to the Fabasoft Cloud at the end of the contract period. See Cloud Service Agreement, Section 4.6
Period of retention of user data (data retention period)	Should the contract be terminated, Fabasoft is authorised to delete the user data within a period of four to six months after the contract has ended. See Cloud Service Agreement, Section 4.6
Continued retention of user data (residual data retention)	If requested by the customer in a written declaration to Fabasoft by e-mail within four months after contract termination, Fabasoft is prepared to transfer data specifically designated by the customer, that the customer had stored on the infrastructure operated by Fabasoft 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, Section 4.6

3 Security

3.1 Service reliability

Fabasoft Cloud Services are designed to offer 99.9% availability for each observation period (quarter). The Data Centers are designed based on the Tier III specifications of the Uptime Institute. 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 Fabasoft Cloud Edition or the service package selected).

Authentication

- Username and password
  - The username is the user’s valid e-mail address.
  - If a user has forgotten their password, they can set a new password via a link sent to their e-mail address. The option to set a new password is offered during the login process.
  - Fabasoft does not save the password in plain text and cannot reproduce it.
- Client certificate
  - The root certificate of the CA 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 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.

- Digital ID (German identification card, Austrian citizen card with mobile phone signature, SuisseID)
  - If digital ID login is based on at least two factors, the next section describing two-factor validation via the Fabasoft Cloud is not applicable.

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.
- E-mail PIN
  - A five-digit number (PIN) is sent to the user's e-mail 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 e-mail addresses for mobile PIN and e-mail 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 Fabasoft Cloud 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), Digital ID 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	Digital ID, AD FS, SAML 2.0 RADIUS server for second factor

3.3 Encryption

Users must access the Fabasoft Cloud 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 "Secomo" appliance (incl. hardware security module), which is available separately, expands the Fabasoft Cloud to include end-to-end encryption for highly sensitive documents. 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.

3.5 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 edition, users in Teamrooms with all rights can access the audit log evaluations. Audit log entries are stored for a minimum of 12 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 Fabasoft Cloud in chronological order. This transaction information is collected at the user's workstation, both in the web browser and in the Fabasoft Cloud Client, in the Fabasoft Cloud mobile apps as well as in the Fabasoft Cloud services and system components. This transaction information is used exclusively for the continuous improvement of Fabasoft 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 12 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 authorisation can access auditing information in the Web Client. Users can also export this auditing information.

3.6 Auditing and security verifications

External and internal security analyses and audits of technical, physical and organizational security measures and operating processes play a crucial role in ensuring the security of your data.

Objectives	
External assessment of security and data protection through certifications and audits	ISO 9001:2015 ISO/IEC 20000-1:2011 ISO/IEC 27001:2013 ISO/IEC 27018:2014 ISAE 3402 Type 2 BSI C5 (Cloud Computing Compliance Controls Catalogue) SOC 2 Type 2 Certified Cloud Service (TÜV Rheinland) EuroCloud Star Audit (5 Sterne)

To verify the data security measures and/or compliance with data security measures, the customer can request, in writing, an audit by an independent authority or carry out such an audit itself, provided the customer can prove that it has the required expertise to carry out this audit.

The customer will present and justify the need for this audit to Fabasoft in writing, within a period of at most 14 days from the request being made. The audit should be carried out without causing disruption to Fabasoft's operation, insofar as is possible. The customer and Fabasoft should then come to a mutual agreement on the process, choice of testing authority, date of audit and assignment.

The customer who requests the audit must bear the costs itself (i.e. costs of the audit and Fabasoft's expenses). If Fabasoft also incurs additional staffing costs beyond this, the customer must settle these additional costs in accordance with (Fabasoft's) standard hourly rates.

Fabasoft can also present the customer who requests the audit with the internal provisions on conducting an audit. The customer must adhere to these provisions.

The customer will present Fabasoft with the audit documentation in the form of the entire audit report.

Fabasoft can also comply with the customer's request as a matter of priority by providing the customer with a summary of the current audit reports of audits previously carried out.

In any case, a corresponding non-disclosure agreement (NDA) must be signed by the customer, Fabasoft and the independent auditing authority before starting.

The summary of an audit report and the audit reports themselves should be treated as strictly confidential documents. In general, all forms of transferring, disseminating or publishing the reports and summaries is prohibited unless explicitly authorized in writing by Fabasoft.

If the customer requires copies of the audit report from audits previously carried out on Fabasoft for the purposes of assessment procedures, investigations or measures taken by the data protection supervisory authorities, then Fabasoft will support the customer – at its request – to fulfil its obligations to the supervisory authorities and transfer the required audit reports directly to the supervisory authorities.

3.8 Governance

Scheduled maintenance work will be announced on the following website at least 14 days in advance: https://www.fabasoft.com/cloudservices/system-status. In urgent cases (e.g. risks associated with delay), maintenance work may be performed ad hoc.

The updates to the Fabasoft Cloud are generally carried out as zero downtime updates. Cloud Apps are scheduled to be updated on a monthly basis and the Fabasoft Cloud Basis will be updated every two months. The new features for each update will be documented in the "What's New" document and made available on https://help.cloud.fabasoft.com.

Contractual changes shall be announced at least 14 days before coming into effect.

Objectives	
Announcing changes	'What's New' document on https://help.cloud.fabasoft.com Contractual changes on https://www.fabasoft.com/contract

4 Data management

4.1 Data classification

User data

Data placed in the Fabasoft Cloud by the customer or data created in the Fabasoft Cloud is saved in Teamrooms assigned to an organization. The owner of the 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 synchronized between locations. It remains in the location of the Teamroom in which it was saved.

The customer's user data shall remain solely within the customer's control. Fabasoft shall not know the content of this information, nor shall it have direct access to it, without the express authorization of the customer.

Contact data

Contact data for collaboration in the Fabasoft Cloud is collected in the following circumstances:

- A future customer provides their contact data as part of the registration process.
- The administrator of the 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 organization when defining access rights for a Teamroom.

Administrators of the 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 Fabasoft Support button in the Fabasoft Cloud.

Contact data is not generally available to be viewed. Contact data is identified using the contact's full e-mail address. If, when setting up a contact, the system detects that contact data already exists for the e-mail 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, e-mail 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 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

4.3 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 Fabasoft acts as processor for the customer, processing of data that is passed from the customer to Fabasoft takes place exclusively on instruction by the customer. Fabasoft shall support the customer in exercising its data protection obligations. The customer's obligations as a data controller, and those of Fabasoft as a processor, are defined in the document "Data processing agreement".

4.4 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.

4.5 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, Fabasoft 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 fulfil 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 Fabasoft in the course of its contractual relationship with the customer will be processed by Fabasoft in order to send e-mails, letters or advertising brochures to customers for the purpose of depicting and presenting Fabasoft products (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 Fabasoft or e-mail to privacy@fabasoft.com. Fabasoft 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, Fabasoft 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 Fabasoft or e-mail to privacy@fabasoft.com. 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. Fabasoft shall not know the content of this information, nor shall it have direct access to it, without the express authorization of the customer.

Fabasoft 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, e-mail addresses, logos, owners, administrators, departures, 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):

E-mail 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)

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, e-mail addresses, website, assigned edition, assigned apps, membership status, last status change, last login (date and location), mode of dispatch for mobile PIN, mobile phone number for mobile PIN, e-mail 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

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 e-mail address of another user:

Photo, first name, middle names, surname, title, post-nominal title, gender, date of birth, salutation, e-mail 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

Fabasoft offers 1st Level Support for Fabasoft Cloud users. Users can file a support request at any time using the Support button in the Fabasoft Cloud web interface, the Fabasoft Cloud Client or the Fabasoft Cloud mobile apps for iOS and Android. By using the Support button, the user's name, e-mail address and problem description are submitted to Fabasoft Support. For better traceability of the problem, the user also has the option to send a screenshot. In the Fabasoft 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 Fabasoft Support employees, XPRON Systems GmbH, 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 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 behaviour.

5.3 Data minimisation

Fabasoft 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 Fabasoft Cloud, 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 Restrictions on use, retention and disclosure

Should Fabasoft be required to appear before a court or another government authority within the framework of a legal obligation or legal process and Fabasoft is obligated to make user data stored by the customer available for the court or the government authority, Fabasoft shall proceed as follows:

i. Governmental requests for information are thoroughly checked for their legality by qualified persons before they are complied with.

- As long as Fabasoft is not in violation of any laws, Fabasoft shall contact the customer as quickly as possible (electronically) in order to give the customer the opportunity to take legal action to prevent disclosure of the data at the customer’s own expense.
- Fabasoft will only permit access after a positively completed check (cf. item i.) and will cooperate with the Customer to the extent legally possible in order to protect the customer’s data protection rights.

ii. Fabasoft will only allow access to data covered by the request for information, insofar as this is possible using proportionate means. Fabasoft must rely on the support of the customer in

order to determine which data is covered by the request for information and which is not, as Fabasoft is not aware of the data stored in the Fabasoft Cloud.

Objectives	
Number of legal requests for information	Not published
Number of legal requests for information with customer notification	Not published

5.5 Openness, transparency and notice

Fabasoft 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 following sections list the data that is forwarded/transmitted to third parties and sub-processors. All third parties and sub-processors listed below are carefully selected and audited if necessary to ensure that they comply with all information security standards.

Objectives	
Third parties	See list starting at Section 5.5.1
Sub-processors	See list starting at Section 5.5.5
Data categories	Contact data, no user data

5.5.1 Microsoft

5.5.1.1 Microsoft Office Online

Office Online is a Microsoft service and its use is therefore subject to Microsoft's Terms of Use and Privacy Policy. To enable the display and processing of a file, Office Online creates a temporary copy of this file in Office Online servers. In addition, the name of the user and the internal IDs of the processors and owners are made available.

This function is optional. The Fabasoft Cloud customer can specify in the Fabasoft Cloud Organization whether this option for viewing and/or processing documents is available to the members of their organization or not.

5.5.1.2 Microsoft Teams

Microsoft Teams is a Microsoft service and its use is therefore subject to Microsoft's Terms of Use and Privacy Policy. If a Teams card is created using search or copy & paste, the information entered and displayed is transmitted to Microsoft servers. The inserted information (name, preview picture, information about the change and the link) is stored on Microsoft servers. When a custom tab is inserted, the link and its name is stored on Microsoft servers.

5.5.2 A-Trust

The following data is forwarded to A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, Landstrasser Hauptstrasse 5, 1030 Vienna, Austria for the purpose of logging in using the “Handy-Signatur” mobile phone signature:

Mobile number and signature password (this data is requested from A-Trust by the user via a form embedded in the login page of the Fabasoft Cloud).

5.5.3 Governikus GmbH & Co. KG

The following data is forwarded to Governikus GmbH & Co. KG, Am Fallturm 9, 28359 Bremen, Germany (formerly bremen online services GmbH & Co. KG) for the purpose of logging in using the “New German Identification Card”:

First name, last name, PIN (this data is transferred directly to Governikus GmbH & Co. KG using an embedded form)

5.5.4 Data Center operator

In the document “Performance Characteristics Data Center Operation”, Fabasoft states which Data Center operator is contracted for each Fabasoft Cloud location.

5.5.5 Sub-processors

In this section, Fabasoft discloses a current list of sub-processors. The most recent version of “Performance Characteristics of Data Security” can be viewed online at https://www.fabasoft.com/cloudservices/data-security.

5.5.5.1 EVALANCHE

The following data is forwarded to SC-Networks GmbH, Enzianstrasse 2, 82319 Starnberg, Germany for marketing purposes and information about updates of Fabasoft products and solutions:

E-mail address, title, first name, last name, salutation, gender, company or organization, role in the organization, country, language, contact category, list of purposes for processing personal data.

5.5.5.2 F24 Schweiz AG

The following data is forwarded by text to F24 Schweiz AG, Samstagernstrasse 45, 8832 Wollerau, Switzerland for delivery of the mobile PIN in the case of a two-factor authentication:

Mobile phone number for mobile PIN, e-mail address for login, mobile PIN

5.5.5.3 Simple SMS GmbH

The following data is forwarded by text to Simple SMS GmbH, Dr.-Schauer-Strasse 26, 4600 Wels, Austria for delivery of the mobile PIN in the case of a two-factor authentication:

Mobile phone number for mobile PIN, e-mail address for login, mobile PIN

5.5.5.4 atms Telefon- und Marketing Services GmbH

The following data is forwarded by text to atms Telefon- und Marketing Services GmbH, Saturn Tower, Leonard-Bernstein-Strasse 10, 1220 Vienna, Austria for delivery of the mobile PIN in the case of a two-factor authentication:

Mobile phone number for mobile PIN, e-mail address for login, mobile PIN

5.5.5.5 XPRON Systems GmbH

To process Fabasoft Cloud support requests XPRON Systems GmbH, Carl-Schurz-Strasse 2, 41460 Neuss, Germany, has access to the following data (in context of a support ticket):

Contact Data (see chapter 5.2.2)

5.5.6 Commissioning/conditions

Fabasoft commissions sub-processors exclusively under the provisions of Art. 28 GDPR and the conditions pursuant to the “Data processing agreement”.

Fabasoft commissions only sub-processors who provide sufficient guarantees that suitable technical and organizational measures are carried out in such a way that processing is conducted in compliance with the applicable data protection provisions and that the rights of the data subject are protected.

Customers be shall informed immediately of any sub-contracting or any change in the sub-processor. The customer shall then be granted a 14-day period to raise an objection for objectively justifiable reasons. If no objection to the sub-contracting or the change in sub-processor is raised for objectively justifiable reasons within the 14 days, then the new sub-processor shall be considered approved.

The conditions for an objectively justifiable objection and the extraordinary right to termination are defined in the “General terms and conditions” and the “Data processing agreement”.

With regard to the requirements on confidentiality, data protection and data security, Fabasoft and the contracted sub-processors have concluded a written agreement as defined in Art. 28 (4) GDPR. Fabasoft has contractually imposed on the commissioned sub-processor the same general obligations that are imposed on Fabasoft in the “Data processing agreement”.

Fabasoft has ensured that all sub-processors commit, in writing, to comply with the required data protection and confidentiality regulations. Fabasoft can, at any time, request from the sub-processor all information that Fabasoft considers to be necessary for exercising its comprehensive supervision of the task in compliance with the data protection provisions. With due notice, Fabasoft can make sure that data protection provisions are adhered to on site.

5.6 Accountability

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

Objectives

Guidelines for data theft	See text of this section.
Documentation	https://www.fabasoft.com/trust Performance Characteristics Data Security Performance Characteristics Data Center Operation

5.7 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 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 the sub-contractor is processed according to the conditions laid out by the sub-contractor (see Section 5.5 “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 Contact data is synchronized between all Fabasoft Cloud locations

5.7.1 Data transfer/download in third countries

Fabasoft processes data in Austria, Germany or Switzerland. As such, Fabasoft will generally not transfer data to third countries.

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

If the customer uses the Fabasoft Cloud 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.

5.8 Intervenability/statutory data protection rights

Customers can demand information about which data (= contact data) concerning them is processed by Fabasoft (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 Fabasoft Cloud 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 Fabasoft'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 Fabasoft Support and support times are defined. (see Performance Characteristics Data Center Operation)

5.8.1 Queries and points of contact

For notifications and communications regarding security and data protection incidents and when requesting support with regard to the customer's data protection obligations (as a controller), the customer can reach Fabasoft through the following channels:

- By e-mail: privacy@fabasoft.com
- By post: Fabasoft AG, c/o Datenschutz, Honauerstrasse 4, 4020 Linz, Austria

All requests and enquiries are to be made in writing and sent to Fabasoft.

In order to prevent misuse of the relevant rights by unauthorized persons, evidence of the identity of the enquiring party or the data subject must be provided to Fabasoft in a suitable form.

Fabasoft has a data security team at its disposal that is dedicated to data protection issues ("Privacy Team"), which can be reached through the aforementioned channels.

If the GDPR and/or national regulations require, Fabasoft will appoint a data protection officer. The contact details of this data protection officer are available at: https://www.fabasoft.com/privacy.

5.8.2 Customer self-service

The user data shall remain solely within the customer's control. Fabasoft shall not know the content of this information, nor shall it 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 Fabasoft Cloud settings, the customer can access instructions on how, for example, to autonomously request its contact data and to edit this data itself. Taking into account the data privacy regulations, the customer can use Fabasoft Support to erase, rectify or anonymize its contact data, or to have it transferred.

5.8.3 Complaint options

All complaints or uncertainties relating to the Fabasoft Cloud can be made to all Fabasoft companies through the following channels:

- By e-mail: privacy@fabasoft.com
- By post: Fabasoft AG, c/o Datenschutz, Honauerstrasse 4, 4020 Linz, Austria

All complaints should be addressed to Fabasoft in writing. In order to prevent misuse by unauthorized persons, evidence of the identity of the complainant must be provided to Fabasoft in a suitable form.