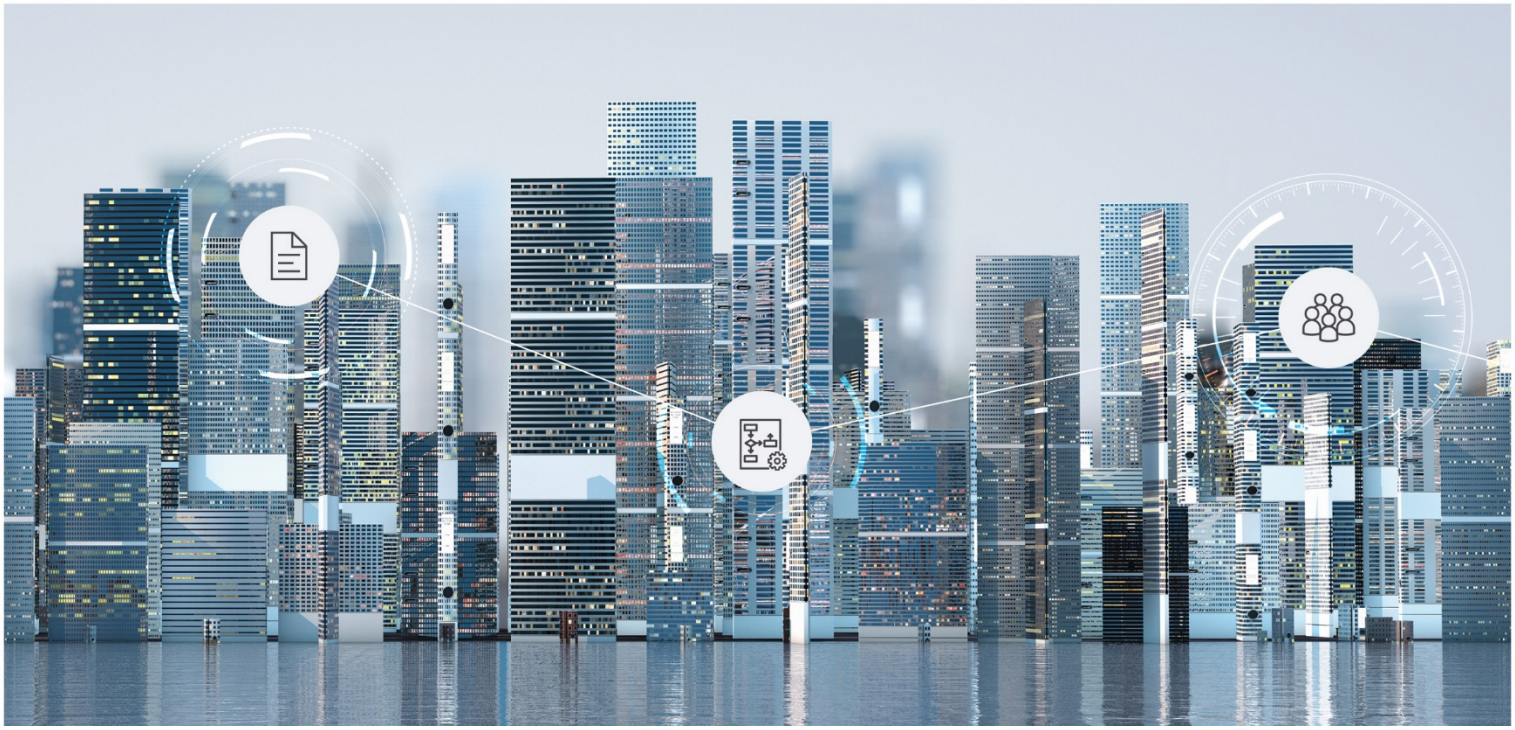
Fabasoft



Performance Characteristics Data Security

Fabasoft Cloud

Valid from 2018-05-25

Confidential

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 documents the ways in which the Fabasoft Cloud protects and handles data and how this data can be exchanged with other users.

In addition, Fabasoft as a founding member has undertaken to comply with the EU Cloud Code of Conduct.

Key information on the scope of the EU Cloud Code of Conduct is available online at https://www.fabasoft.com/cloudservices/eucloudcoc.

Fabasoft Cloud customers can contact Fabasoft using the following email address privacy@fabasoft.com in case of any questions regarding the handling 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. the data cannot be restored. The customer shall be informed upon signing the contract and shall receive a reminder before the termination date (see Fabasoft Cloud GTC, 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 Fabasoft Cloud GTC, Section 4.6.
Period of retention of user data (data retention period)	Should the contract be terminated, Fabasoft is authorized to delete the user data within a period of four to months after the contract period. See Fabasoft Cloud GTC, Section 4.6.
Residual retention of user data (residual data retention)	If requested by the Customer, who must declare to Fabasoft in writing by e-mail within a period of four month after contract termination, within a period of at least four months and no more than six months after the termination of this Contract, 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 See Fabasoft Cloud GTC, Section 4.6.

3 Security

3.1 Service Reliability

Fabasoft Cloud Services are designed to offer an availability of 99.9 percent for each observation period (quarter). The data centers are designed in line with 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

- User name and password
  - The user name is the valid e-mail address of the user.
  - If users have forgotten their password, they can select a new password using a link sent to their e-mail address. The option to set a new password is offered during the login process.
  - The password from Fabasoft is not saved in plain text and cannot be reproduced by Fabasoft.
- Client certificate
  - The root certificate of the CA and all intermediate CAs must be configured by the administrator of the customer 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 of the Fabasoft Cloud must be configured as "Relying Party Trust" in the AD FS of the

customer 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 by Fabasoft over the Internet. The authentication service of the Fabasoft Cloud must be configured as Service Provider in the Identity Provider of the customer. The metadata (metadata.xml) of the Identity Provider necessary for the configuration in the Fabasoft Cloud must be provided by the Customer.
- Digital ID (German identification card, Austrian citizen card with 'Handy-Signatur' mobile phone signature, SuisseID)
  - If the login using a digital ID is based on at least two factors, the next section describing two-factor validation via the Fabasoft Cloud is not required.

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

- Mobile PIN (SMS)
  - The 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.
- E-mail PIN
  - The 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-user password via the RADIUS server
  - The customer must operate a RADIUS server, which is made available over the Internet by Fabasoft Cloud. The access data to the RADIUS server must be configured by the administrator of the customer in the Fabasoft Cloud Organization.

The administrator of the customer in the Fabasoft Cloud Organization can configure the authentication parameters for the members of the customer's organization or external organizations. These parameters include the phone numbers or e-mail addresses for mobile PIN and e-mail PIN access. Administrators can also decide on which methods for two-factor authentication are necessary and preferred for the members.

Authorization

Authorization for access to user data is managed using Teamrooms. For each Teamroom, team members are granted specific access rights (read rights, change rights, all rights). Searches for user data take these access rights into account. The search only produces hits for which the user has access rights.

A user with all rights can configure a Teamroom to allow 'public links' in the Teamroom. A public link allows users to access the Teamroom, a folder, a document, or other content in the Teamroom without prior authentication. The user only needs to have the 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 the folder via the link.

When accessing the Fabasoft Cloud using third-party applications that only require a user name 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 process	State-of-the-art technology
Authentication process	User name and password, client certificate Single Sign-on (Active Directory), Single Sign-on (SAML 2.0), Digital ID Generally, two-factor authentication
Rights revoked with exclusion of organization	Immediately upon deactivation of the user account. Rights revoked by administrator of customer
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 Cryptography

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 product from Fabasoft

3.4 Logging and Monitoring

Auditing

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

- Access to documents (read and write authorizations)
- Changes to metadata
- Desolving Teamrooms and deletion of documents
- Deletion of the history of a Teamroom
- 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 opportunity to export the audit log entries and store them separately. The audit log entries are permanently deleted on termination of this Contract together with the user data after expiry of a period of at least 4 months and maximum 6 months (calculated as of 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 stored at the user's workstation, both in the web browser and in the Fabasoft Cloud Client, in the mobile apps of the Fabasoft Cloud as well as in the services and system components of the Fabasoft Cloud. 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 is maximum 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 maximum 6 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 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 security assessment 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) Certified Cloud Service (TÜV Rheinland) EuroCloud Star Audit (5 stars)

3.6 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 Fabasoft Cloud Basis will be updated bimonthly. 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 must be announced at least 14 days prior to going into effect.

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

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.

Contact data

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

- Future customers provide 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 in the context of 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 Fabasoft Support button in the Fabasoft Cloud.

Contact data is not generally available to be viewed. Contact data is identified using the contact's complete e-mail address. When creating contact data, should the system detect 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 initial, surname, title, post title, sex, date of birth, salutation, e-mail domain, website, organization, function in the organization, assignment to organizational units, assignment to teams, assignment to external organizations, language, registration state).

This general contact data is also visible to the other team members in the Teamroom unless the configuration for the Teamroom has been changed.

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	
Handling of user data	Data is handled only as requested by the customer
Handling of derived data	Data is handled only as requested by the customer

4.2 Data Lifecycle

Objectives	
Type of deletion	User data can be permanently deleted by the customer (emptying the trash, 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.

4.3 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	
Data 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 this data includes 'personal data' as defined by the EU General Data Protection Regulation or the respective national data protection laws, Fabasoft shall observe data secrecy and all other statutory data protection regulations within the meaning of the applicable EU standards and the substantive data protection laws of the respective countries.

Objectives	
Codes of conduct, standards, and certification mechanisms	The 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 request of the customer and the performance of 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.

Those data received by Fabasoft in the course of its contractual relationship with the customer, will be processed by Fabasoft in order to send emails, 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 data for the purpose of direct advertising, said right can be exercised at any time without giving reasons by means of letter to Fabasoft or email to privacy@fabasoft.com. Fabasoft will process the customer data for this purpose for as long as the customer lodges no objection, however, up to a maximum of 3 years after termination of the contract. Where other forms of direct advertising are concerned, Fabasoft will only process the customer data if the customer has expressly given its express consent to the processing of its data (Art. 6 (1)(a) GDPR). If the customer has given its consent to the data processing, it can revoke this consent without giving reasons by means of letter to Fabasoft or email to privacy@fabasoft.com. The processing of the personal data of the customer for the purpose of direct advertising is not necessary for the execution of the contractual relationship.

The data of the customer are not processed for any other purpose

The following sections list the data that shall be stored and handled.

5.2.1 User Data

Fabasoft Cloud shall handle user data exclusively for the purposes requested by the customer in compliance with the main contract and the instructions of the customer.

5.2.2 Contact Data

Organization:

Name, billing address, UID-No., service packages, members, organizational units, teams, external members, external organizational units, standard Teamrooms, addresses, phone numbers, e-mail addresses, logos, owners, administrators, exclusions, purchases, policies, encryption settings, authentication settings, security settings, and additional configuration settings

Organizational units:

Name, members, standard Teamrooms, security settings, hierarchy level, departures, import ID, 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 initial, title, post title, sex, birth date, salutation, function in the organization, assignment to organizational units, assignment to teams, assignment to external organizations, language, registration state, addresses, phone numbers, e-mail addresses, website, assigned edition, assigned apps, member state, last state 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 used 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, when a user knows the e-mail address of another user:

Photo, first name, middle initial, surname, title, post title, sex, date of birth, salutation, e-mail domain, organization, function in the organization, website, assignment to organizational units, assignment to teams, assignment to external organizations, language, registration state, import id

5.2.4 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 why we use 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

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

Objectives	
Retention period for temporary data	In the Fabasoft Cloud, temporary data 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 Fabasoft Cloud GTC Otherwise: When data is deleted by customers

5.4 Use, Retention, and Disclosure Limitation

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 available for the court or the government authority, Fabasoft shall proceed as follows:

- As long as Fabasoft is not in violation of any laws, Fabasoft shall contact the customer immediately (electronically) to give the customer the opportunity to take legal action to prevent disclosure of the data at the customer's own expense.
- Fabasoft shall cooperate with the customer to the extent possible to protect the customer's data protection rights.

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 are forwarded to / transmitted to third parties. All third parties 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
Data categories	Contact data, no user data

5.5.1 Act-On

The following data is forwarded to Act-On Software, Inc., 8300 SW Creekside Place, Suite 250, Beaverton, Oregon 97008, USA for marketing purposes:

Object address (internal ID), e-mail address, title, first name, last name, registration date, salutation, gender, birth date, company, organization, function in the organization, country, language, one-off user, product edition, product subscription start, product subscription type, product subscription end, maximum storage requirements, 'current' storage requirements,

maximum number of objects, number of ‘current’ objects, last login, number of apps, campaign code, activated, registration address (e.g., https://www.fabasoft.com)

Act-On Software, Inc. is certified in compliance with REU-US Privacy-Shield. More detailed information can be found under https://www.privacyshield.gov.

5.5.2 Microsoft Office Online

Office Online is a service from Microsoft and its use is therefore subject to the Terms of Use and the Privacy Policy of Microsoft. 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 functionality is optional. The Fabasoft Cloud customer can determine in the Fabasoft Cloud Organization whether this option for the viewing and/or processing of documents is available to the members of its organization or not.

5.5.3 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).

5.5.4 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)

5.5.5 Dolphin Systems AG

The following data is forwarded per text message to Dolphin Systems AG, Samstagernstrasse 45, 8832 Wollerau, Switzerland for delivery of the mobile PIN in the case of a 2-factor authentication:

Mobile Phone Number for Mobile PIN, E-Mail Address for Login, Mobile PIN

5.5.6 Simple SMS GmbH

The following data is forwarded per text message to Simple SMS GmbH, Dr.-Schauer-Strasse 26, 4600 Wels, Austria for delivery of the mobile PIN in the case of a 2-factor authentication:

Mobile Phone Number for Mobile PIN, E-Mail Address for Login, Mobile PIN

5.5.7 atms Telefon- und Marketing Services GmbH

The following data is forwarded per text message 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 2-factor authentication:

Mobile Phone Number for Mobile PIN, E-Mail Address for Login, Mobile PIN

5.6 Accountability

If Fabasoft has detected unauthorized access to the user data of the organization or the contact data or if there is reasonable suspicion, the owner of the organization shall be informed via registered mail. In addition, Fabasoft shall attempt to contact the owner of the organization as quickly as possible via 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 select between different locations (contractual location) for storing user data (Teamrooms, folders, documents, etc.). User data are only ever processed, stored and backed-up outside of the contractual location with the express, written consent of the customer.

The data regarding the user, the organization and the organizational unit (contact data) is replicated and synchronized over all locations (Germany, Austria, Switzerland). You can find a list of all relevant data in Section5.2 'Purpose Specification'. Settings in the user's work environment are also synchronized if users have changed their location.

Data sent to the subcontractor is handled according to the conditions laid out by the subcontractor (see Section 5.5 'Openness, Transparency, and Notice.

Objectives	
List of available locations	Germany, Austria, Switzerland
Selection options for locations	Can be selected for user data by customers Contact data is synchronized between all Fabasoft Cloud locations

5.8 Intervenability / Statutory Data Protection Rights

The customer can demand information about which data concerning it is processed by Fabasoft (see Art. 15 GDPR for more details). The customer can have its data saved in the Fabasoft Cloud restricted (blocked see Art. 18 GDPR), rectified or deleted (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 deleted by the customer or by users authorized by the customer to access the Teamroom containing the user data.

In the event an unexpected breach of the right of the customer to lawful processing of its data occurs despite the obligation of Fabasoft to process the data of the customer 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 its 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)