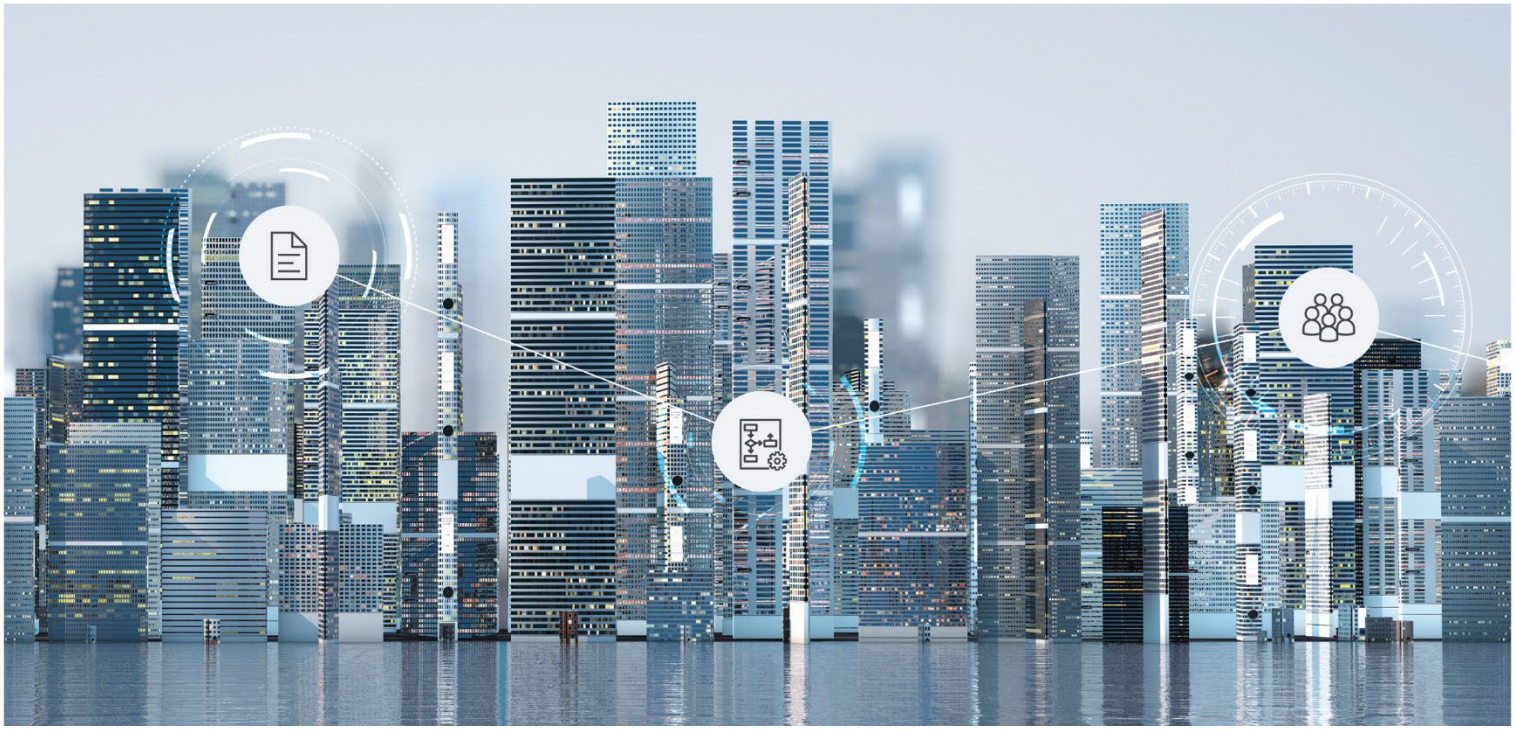

Technical and organisational measures

Fabasoft Group

Valid from 01/01/2025

Public

To aid readability, references to persons are not gender-specific.
Corresponding terms are used for the purpose of equal treatment of both genders.

1 Introduction

This document describes the essential technical and organisational measures for the protection of personal data within the framework of the business activities of the Fabasoft Group (specifically, the Fabasoft company with which the customer has the contractual relationship or the Fabasoft companies named in the appendix "Sub-processors", hereinafter referred to as "Fabasoft").

Fabasoft processes personal data in a manner that ensures the achievement of the following information security objectives in accordance with the Fabasoft Guideline on Information Security:

Confidentiality

Customer data, business data and data from the development divisions are subject to the highest confidentiality requirements. No unauthorised persons may gain knowledge of them (limited access authorisations, confidentiality levels, encryption, ...). Information may only be viewed by authorised persons. All Fabasoft employees are obliged to observe the applicable data secrecy and to maintain confidentiality.

Integrity

Data and information must be correct and complete. IT systems must function consistently. Data and information must not be altered without authorisation. Changes to information must be clearly recognisable and traceable (versioning).

Availability

Information must be available in accordance with the contractually guaranteed service levels. Downtimes must not have any significant impact on Fabasoft and its stakeholders. Information must be processed on systems and services that guarantee the necessary availability. In the event of a fault, it must be possible to restore systems and services within the agreed time.

Authenticity

It must be ensured that information is authentic, verifiable and credible and that IT systems and IT applications are free of manipulation.

2 Technical and organisational measures

The following sections describe the current technical and organisational measures implemented by Fabasoft to achieve the security objectives. These technical and organisational measures are regularly checked to ensure that they are up to date, effective and state-of-the-art, and are defined more precisely if necessary.

2.1 Confidentiality

2.1.1 Physical access control

The following measures are taken to prevent unauthorised persons gaining access to the data processing systems with which the personal data are processed:

- The regulations for securing physical access are documented in the Access Control Policy. This contains regulations regarding physical security in connection with the building and the office premises as well as the associated monitoring measures.
- Fabasoft premises are divided into security levels. Employees are granted access rights according to the criteria of the Access Control Policy.
- Fabasoft has implemented procedures so that changes to authorisations are only carried out with approval and in accordance with the specifications and guidelines (change management).
- Fabasoft employees are issued with an employee ID card which must be worn visibly at all Fabasoft locations.
- Visitors are supervised and accompanied by employees. External parties, who are permitted to move around in defined premises on the basis of an authorisation, are obliged to maintain confidentiality and must announce their arrival and departure in the Fabasoft office.

The following additional measures are taken for data centres:

- The regulations for securing physical access to Fabasoft data centres are set out in the document "Performance Characteristics Data Centre Operation", available at https://www.fabasoft.com/en/contracts-and-information.
- Strict security measures apply to all data centres. The external data centres must meet the requirements defined in the site audit checklist (e.g. physical security, power connection, cooling, fire protection, network connection, security, environmental hazard, maintenance of utilities, operational redundancy, protection of power supply and telecommunication lines) and organisational measures (e.g. audits, certifications).
- A technical system continuously monitors the status of the rack doors, temperature and power supply and escalates to Incident Management if the permissible control range is exceeded.

2.2 System access control

The following measures are taken to prevent the use of data processing systems by unauthorised persons:

- Internal and external access to the Fabasoft network is technically highly restricted. External access to the Fabasoft network and logging on to Fabasoft workstations is implemented with multi-factor authentication.

- The regulations for securing access to Fabasoft systems and services are documented in the Access Control Policy. This contains regulations regarding the allocation, modification and revocation of authorisations on Fabasoft systems and services.
- Fabasoft has implemented procedures so that changes to authorisations are only carried out with approval and in accordance with the specifications and guidelines (change management).
- The Fabasoft password guideline defines the requirement for generating, changing and using passwords.
- System access control is supported by the protection of the systems concerned by the following measures: Firewalls, malware detection programmes, use of SIEM, ongoing patch management and vulnerability management.
- Confidential documents and printouts that are no longer needed are disposed of in the closed containers provided for this purpose (closed containers with a deposit opening). The containers are regularly collected by an external service provider and the container contents are destroyed in accordance with ÖNORM S 2109-1 Destruction Level 3.

2.2.1 Data access control

The following measures are taken to ensure that persons authorised to use data processing systems only have access to personal data for which they have access rights. This ensures that personal data is not read, copied, modified or deleted during processing without authorisation.

- Access to personal, confidential or other sensitive information is only granted to those persons who are authorised to have such access through the provision of their services ("least privilege model"/"need-to-know principle"). The confidentiality levels defined in the internal classification guideline are also taken into account.
- Fabasoft defines procedures and requirements for logging in applications and services, the protection of logs, the storage of logs and the use of log data.
- Fabasoft defines procedures and requirements for encryption of data in transit (e.g. logs, ciphers) and at rest (including removable media, backup data) as well as for key management (key generation, issuing and obtaining certificates for public keys, key protection, key exchange, handling compromised keys and taking them back).

2.2.2 Separation control

The following measures are taken to ensure that personal data collected for different purposes can be processed separately:

- The separation of data in production systems is ensured by appropriate authorisations or client mechanisms.
- Systems for software development, test and demo systems as well as production systems are operated separately. Development, test and production environments are operated on separate hardware or virtual machines.
- Systems are separated into adequate subnets on the network side.
- Firewall configurations are used to ensure that communication is only possible between network segments for which communication must generally be possible.
- Requirements are defined for physical and virtual network design, segmentation and isolation (e.g., dedicated networks for infrastructure management), and network perimeter protection.

2.3 Integrity

2.3.1 Transmission control

The following measures are taken to prevent unauthorized reading, alteration or deletion of personal data during electronic transmission or while in transit:

- The employment contract regulates the consequences of violations of the secrecy and confidentiality obligations. The continuation of the secrecy obligation after termination of the employment relationship is expressly pointed out. Each employee recognises this regulation as binding with their signature.
- The information security agreement contains information for all Fabasoft employees regarding the secure handling of data and the systems to be used when transmitting data.
- Procedures and requirements for encryption of data in transit (e.g. logs, ciphers) and at rest (including removable media, backup data) as well as for key management (key generation, issuing and obtaining certificates for public keys, key protection, key exchange, handling compromised keys, revocation) are defined.

2.3.2 Input control

The following measures are taken to enable subsequent verification and determination of whether and by whom personal data have been entered into, modified or removed from data processing systems:

-The logging and monitoring guideline defines procedures and requirements for logging in applications and services, protection of logs, retention of logs, and use of log data. Individual products (for example, Fabasoft Cloud) offer "audit logging" functionality and have implemented it accordingly. This makes it possible to check and determine by whom personal data has been entered or modified.

2.3.3 Data integrity control

The following measures are taken to ensure that unauthorised or accidental changes to personal data are prevented:

- Fabasoft has documented protection requirements for malware and virus protection configuration in the System Security Policy and has implemented these.
- Vulnerabilities relevant to Fabasoft must be fully addressed and the vulnerability management process must be appropriate, adequate and effective.
- The Time Synchronisation Policy is a requirement for time synchronisation.
- Internal and external access to the Fabasoft network is technically highly restricted. External access to the Fabasoft network and logging on to Fabasoft workstations is implemented with multi-factor authentication.

2.4 Availability

2.4.1 Availability control

The following measures are taken to protect personal data from accidental or unauthorized destruction or loss:

- Procedures are documented to back up and restore systems.
- Systems availability is continuously monitored by systems and escalated to Incident Management when deviations occur.
- A possible emergency scenario is drafted annually and procedures for dealing with that scenario are tested in the context of an emergency exercise.
- The Business Continuity Management process is designed to respond to, mitigate, and recover from security events that disrupt business operations. The emergency response must regulate all emergency management processes aimed at minimising the impact and consequences of damage.
- Emergencies are tested on a regular basis. The test must take into account availability management requirements and the availability of key personnel. Fabasoft regularly tests and exercises emergencies based on a risk assessment.

2.4.2 Resilience and recoverability of the IT systems used

The following measures are taken to ensure that deployed systems and services can be restored in the necessary time in the event of a malfunction.

- Fabasoft SaaS/Cloud Services are regularly subjected to security audits or penetration tests that identify vulnerabilities, security deficiencies or team room isolation/segregation issues.
- Vulnerabilities, security deficiencies, or team room isolation/segregation issues identified during security audits or penetration tests are rectified.
- Fabasoft has documented procedures for backing up and recovering systems in the Fabasoft SaaS/Cloud environment in the Backup and Recovery Operations guideline.

The following additional measures are taken for data centres:

- Fabasoft operates components for Fabasoft SaaS/Cloud Services, Mindbreeze InSpire SaaS and Fabasoft internal services in external data centres. The external data centres must meet defined requirements (e.g. physical security, power connection, cooling, fire protection, network connection, security, environmental hazard, maintenance of utilities, operational redundancy, protection of power supply and telecommunication lines) and organisational measures (e.g. audits, certifications).
- Fabasoft SaaS/Cloud data (metadata and documents) are stored in geographically distributed data centres.

2.5 Authenticity

The following measures are taken to identify and authenticate users accessing personal data:

- Fabasoft has defined specifications in guidelines that specify password and confidentiality requirements for identification and authentication when accessing Fabasoft-internal information assets.
- Authentication in der Fabasoft Cloud is based on a multi-factor authentication.

2.6 Review, assessment and evaluation of the effectiveness of the technical and organisational measures

2.6.1 Control of processing on behalf of a controller

The following measures are taken to ensure that personal data processed on behalf of a controller are only processed in accordance with the controller's instructions:

- With regard to the commissioning of security-relevant suppliers and service providers, the Purchasing Policy must define specifications (e.g. communication of vulnerabilities, security incidents or faults) for all orders placed with Fabasoft suppliers and service providers who contribute significant parts to the development or operation of Fabasoft services and who, within the scope of their business relationship, are characterised by certain features defined in the policy.
- Suppliers or service providers are obliged to comply with the terms and conditions of purchase (including confidentiality obligations, contracts for processing personal data on behalf of a controller and associated provisions).
- The “Data Processing Agreement” as well as the "Performance Characteristics Data Security Fabasoft Cloud" as part of the "Cloud Service Agreement Fabasoft Cloud" are reviewed for compliance with the EU Cloud CoC criteria.
- All processing activities are recorded in a processing directory. The procedures include the type of personal data as well as the associated processes, systems and third parties involved in the processing of this data.

2.6.2 Data protection management

The following measures are taken to plan, implement, manage and control data protection requirements:

- The Fabasoft Group has a data protection team ("Privacy Team") that is entrusted with data protection issues and compliance with the requirements of the GDPR. Fabasoft has appointed external data protection officers.
- The Fabasoft Privacy Policy defines and communicates principles that are to be understood as data protection imperatives to be observed in all areas of Fabasoft's business activities, e.g. compliance with Privacy by Design and Privacy by Default principles pursuant to Art 25 of the GDPR.
- Fabasoft has documented the process "Processing of enquiries by the Privacy Team" in a process description. In addition to the relevant legal requirements, the process description takes particular account of compliance with the EU Cloud Code of Conduct.
- The information security agreement contains information for all Fabasoft employees on the communication channels to be used for enquiries and reports regarding security, data protection and compliance.
- All processing activities are recorded in a processing directory and updated regularly. The processing directory also contains the defined deletion periods to fulfil the principle of storage limitation.
- A platform has been implemented throughout the Group in which regular courses on information security and data protection are completed by all employees in order to improve security knowledge and awareness and to set an example of appropriate security behaviour to employees.

2.6.3 Security incident management

The following measures are taken to identify, manage, monitor and control security incidents:

- Security-relevant incidents are assessed within the framework of security incident management.
- The effects of security incidents are analysed, categorised/classified, prioritised according to the Security Incident Management Process and, if necessary, processed as a security incident.
- The Security Incident Management process includes concrete specifications for response (CSIRT and communication structure, analysis of the security incident including affected systems and data, preservation of evidence, risk assessment, information obligations, mitigation, damage limitation, termination of the threat and restoration of operations).