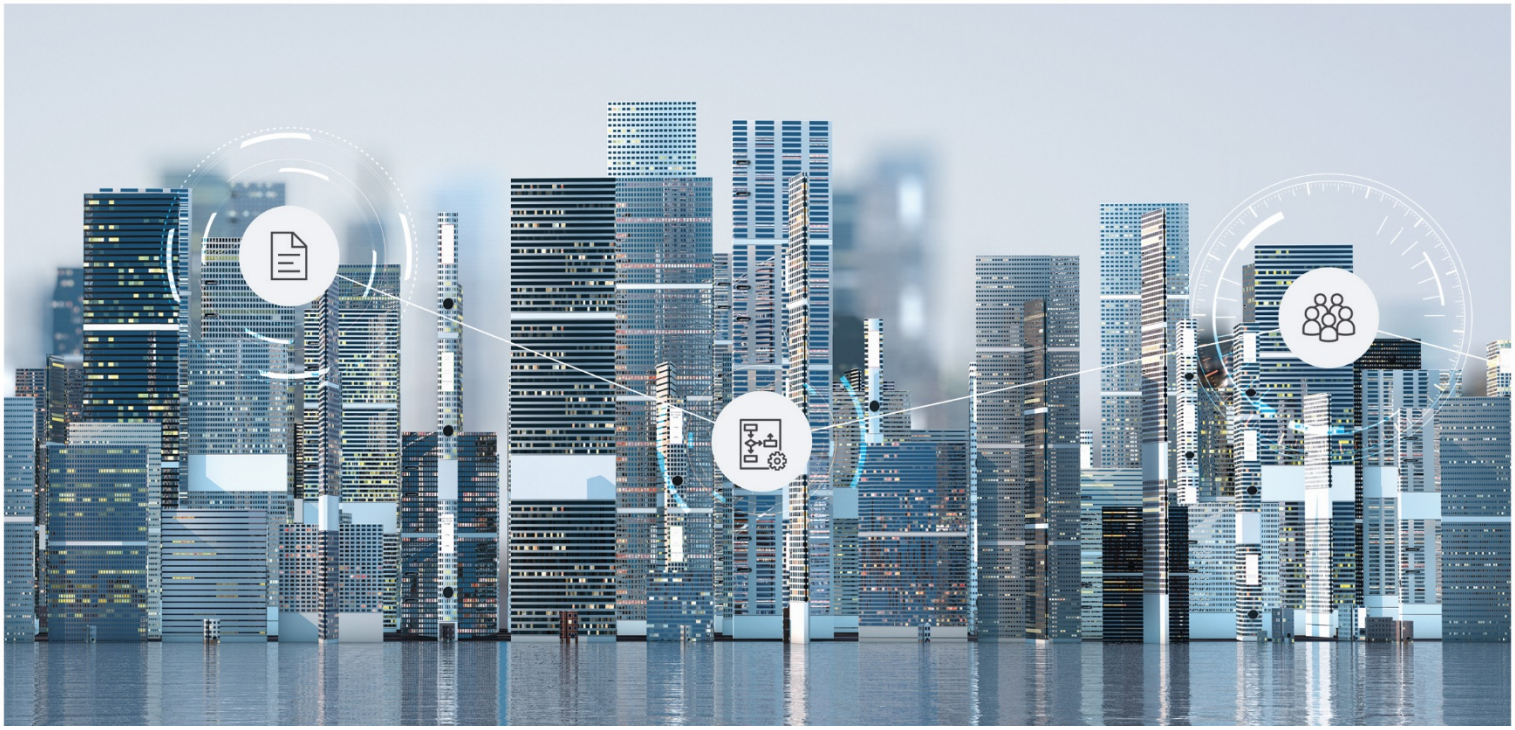
Fabasoft



Technical and Organizational Measures

Fabasoft Group

Valid from 2020-01-08

Public

1 Introduction

The following document outlines the primary technical and organisational measures for protecting personal data in the context of the Fabasoft Group's business activities (Fabasoft AG and its European affiliated companies; Mindbreeze GmbH is integrated as an affiliated company into the control system and thus into the technical and organizational measures of the Fabasoft Group).

Fabasoft processes personal data in such a way as to ensure that the following information security objectives are achieved in accordance with the Fabasoft Security Guideline:

Confidentiality. Customer data, business data and data from development areas are subject to the highest demands of confidentiality. No unauthorised persons may gain knowledge of them (restricted access authorisations, levels of confidentiality, encryption). All Fabasoft staff are obligated to maintain the applicable data confidentiality.

Integrity. Data and information must be correct and complete. IT systems must function end-to-end. Data and information must not be altered without approval.

Authenticity. Information may only be processed by authorised persons. It must be guaranteed that information is true and credible and that manipulation-free IT systems and IT applications are used.

Traceability. Alterations to information must be clearly identifiable and transparent (versioning).

Availability. Information must be available in compliance with the contractually assured service level. Downtimes must not have any significant impact on Fabasoft and its stakeholders. Damage with a high financial impact must be prevented.

Responsibility. All employees are aware of their responsibility with regard to the handling of data and IT systems. Compliance and awareness in respect of information security is embodied and promoted throughout the company.

Certifications. Certifications in accordance with internationally recognised regulations and standards are regularly renewed by means of independent, external audits and lend transparency to the Fabasoft level of security. Effective controls to assure compliance with the requirements are an integral part of Fabasoft processes.

Data protection and information security are of great importance to us. Amongst other things these validate our ISO certifications according to 9001 (quality management), 27001 and 27018 (information security and data protection), 20000-1 (IT service management) and our certification according to BSI C5 (Cloud Computing Compliance Controls Catalogue, issued by the German Federal Office for Information Security). An exhaustive list of certifications and audits is available on the Fabasoft website.

Fabasoft stores data on their own hardware in highly secure external data centres in Germany, or in the Fabasoft Cloud and Fabasoft Folio SaaS context in Austria, Germany or Switzerland. We ensure that operators of these centres must hold valid ISO 27001 certification. Fabasoft centres operate on premises using, space, power, air conditioning, Fabasoft obtains floor space, power supplies, air conditioning, connections between the data centres and Internet routing from the data centres in each case. The operators of these data centres have no access to the Fabasoft hardware and cannot access the data stored on them.

The technical and organisational measures outlined above are continuously monitored and altered accordingly, using state of the art technology in response to the current legal situation for data protection.

2 Technical and Organisational Measures

The following sections outline the current security measures taken by Fabasoft to achieve the security objectives we implemented. These security measures are regularly checked to ensure they are both effective and up-to-date and are subsequently changed wherever required.

2.1 Confidentiality (Art. 32 para. 1 lit. a DSGVO)

The storage and transmission of data within Fabasoft and on Fabasoft systems is always encrypted.

Access to Fabasoft systems is always via encrypted connections.

The transmission of personal data via the intranet and Internet to Fabasoft Services is also always encrypted.

When transferring data via e-mail, TLS encryption is offered.

Data transfer from the Fabasoft network to other external networks and storage on Fabasoft hardware is always encrypted.

Physical access / access to systems / access to data authorizations are assigned according to the principle of minimum rights. When hiring own personnel, they are obligated to comply with secrecy and data protection regulations and instructed by their superiors by means of a corresponding declaration.

The safe handling of end user devices and data carriers is enforced by organisational and technical measures.

Changes to the access and access arrows are made as part of a change management process (change management).

2.1.1 Monitoring Physical Access

Access to the Fabasoft premises is secured by an electronic access system. The Fabasoft premises are divided into different security levels. Access to the Fabasoft premises is only possible with an electronic access card or key. Failed access attempts are regularly evaluated and anomalies analysed.

Non-company persons are only allowed to move around the Fabasoft premises in certain areas and/or only when accompanied by Fabasoft personnel or with the appropriate permission.

For access to external data centres, there are access concepts of its own, which are checked regularly by Fabasoft when selecting the data centre and thereafter. Access to Fabasoft hardware in the external computer centres is only possible for authorized persons and is additionally monitored by Fabasoft.

2.1.2 Monitoring Access to Systems

Fabasoft employees only have access to the IT services they need to perform their tasks.

Internal and external access to the Fabasoft network is technically severely restricted. Access to Fabasoft IT services for users is based on Fabasoft guidelines.

The allocation, modification and withdrawal of access authorizations for users are carried out in accordance with Fabasoft processes and security guidelines that have been checked several times.

Programs for detecting viruses, malware and unauthorized access are used. The effectiveness and scope of these programs are regularly validated.

Unique user IDs are assigned in order to determine access to the systems individually or to uniquely identify each user of the Fabasoft systems. Several levels of authorization are implemented to ensure access to the systems.

Access to networks and computer systems is logged (e.g. logon/logoff events for users, creation of new users, password changes, etc.).

2.1.3 Monitoring Access to Data

Access to personal, confidential or other sensitive information is only granted to those persons who are authorized to access it through their service provision ("least privilege model"/"need-to-know principle"). The confidentiality levels defined in the internal classification guideline are also taken into account. The logging of accesses and the handling of these protocols are regulated in the Fabasoft guidelines.

Access is exclusively authenticated with personalized user accounts.

Access to data in Fabasoft IT Services is protected by the respective service-specific access control systems.

Access to data in the Fabasoft Cloud and Fabasoft Folio SaaS is logged in audit logs.

The use of screen locks is organizationally specified.

There are Clean Desk guidelines and Clear Screen instructions.

Guidelines for the return or loss of mobile end devices as well as for the handling of mobile data media (e. g. USB sticks) are established.

The dispatch or transport of data media is documented.

Data that is no longer needed is deleted in accordance with the defined retention periods.

Procedural instructions for classifying documents (data) are published and established internally.

2.1.4 Monitoring Segregation

Systems for software development, test and demonstration systems and production systems all operate separately from one another. Development, test and production environments are operated on separate hardware or virtual machines.

The separation of the data in the production systems is ensured by appropriate authorizations or client mechanisms.

Systems are separated into adequate subnets on the network side.

Firewall configurations ensure that communication is only possible between network segments for which communication must generally be possible.

2.2 Integrity

System components and programs are integrated into a patch management process.

A technical vulnerability management serves to detect newly occurring security gaps taking into account all relevant operating systems as well as relevant applications and system components in use.

Time synchronization is performed for all computer systems.

2.2.1 Monitoring Transfer

Data transfer from the Fabasoft networks to other, internal and external networks as well as storage on Fabasoft hardware is always encrypted. Management of the keys is carried out in accordance with internal Fabasoft guidelines.

All employees are bound by data confidentiality and receive regular training in handling confidential and personal data.

A policy for the secure dispatch of data carriers has been established.

2.2.2 Monitoring Input

Network communication across the boundaries of a virtual network (VTP domain) always takes place via a physical firewall.

The computer systems are protected against malware.

As part of the logging of user transactions in the Fabasoft IT services Fabasoft Cloud and Fabasoft Folio SaaS, it is possible to check and determine who entered or changed personal data.

2.3 Availability and Recoverability

Fabasoft possesses measures and processes that ensure the backup and recovery of Fabasoft IT systems.

Emergency drills are carried out on a regular basis. Emergency processes and manuals are regularly reviewed to check they are up-to-date and appropriate.

2.3.1 Monitoring Availability

Data centres are physically protected against fire, water, earthquakes, explosions, civil unrest and other forms of natural and man-made disasters.

Data centres shall have adequate air conditioning appropriate to the purpose of the business.

The data centres are equipped with sufficiently dimensioned UPS.

The data centres are equipped with emergency power systems.

The data centre and the computer systems are designed redundantly to meet high availability requirements.

The IT operating processes are documented and maintained.

Foresighted planning and preparation ensure that adequate capacities and resources remain available to provide the required system performance. To reduce the risk of system overloads, estimates are made for future capacity requirements. The operational requirements of new systems are identified, documented and tested before they are accepted and used.

Servers, applications and system software are managed within Asset Management.

Access to the IT infrastructure (server and network distribution rooms) is only permitted to authorized personnel.

All necessary security patches are installed regularly and the necessity of the installation is monitored regularly.

End devices, databases and applications are protected against malicious code.

2.3.2 Availability of the IT systems used

The development of the software is fault-tolerant and extensive load tests are carried out before commissioning.

For the Fabasoft Cloud and Mindbreeze InSpire SaaS, a PEN test is carried out regularly to check the system's resilience.

2.4 Measures to restore availability and access to personal data in the event of a technical incident

2.4.1 Recovery / backup systems

A data backup concept exists that is geared to compliance with the maximum tolerable loss of data.

The data backups are located at an alternative location or are generally persisted redundantly at two locations.

Emergency plans are in place for rapid restart and recovery of systems and data.

The emergency plans are tested before they are released for the first time.

The contingency plans are practiced at least once a year.

2.5 Purpose, review, rating and evaluation

2.5.1 Order control

Fabasoft only permits authorized persons to process personal data in the course of fulfilling their tasks. All employees are trained in the handling of personal data. The passing on of personal data for processing to external service providers is exclusively based on order data processing agreements.

Fabasoft has implemented controls and processes to ensure compliance with contract performance by Fabasoft and its service providers.

2.5.2 Data protection management

Every year, the IT controls are checked according to ISO 27001 in the form of a (monitoring) audit by the auditing body.

Processing activities are documented in accordance with legal requirements.

Valid risk analyses for the processing of personal data are available.

Fabasoft employees who process personal data regularly undergo data protection training.

The role of the information security officer is defined and assigned.

Data protection officers are appointed in accordance with the statutory requirements and can be accessed at www.fabasoft.com/privacy.

A procedure has been established for dealing with data protection violations.