Technische und organisatorische Maßnahmen

Fabasoft Gruppe

Gültig ab 08.06.2021

Öffentlich

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, z. B. Benutzer/-innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

1 Einleitung

Das vorliegende Dokument beschreibt die wesentlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten im Rahmen der Geschäftstätigkeit der Fabasoft (Fabasoft AG und ihre europäischen verbundenen Unternehmen; die Mindbreeze GmbH ist als verbundenes Unternehmen in das Kontrollsystem und damit in die technischen und organisatorischen Maßnahmen der Fabasoft Gruppe eingebunden).

Fabasoft verarbeitet personenbezogene Daten in einer Art und Weise, welche die Erreichung folgender Informationssicherheitsziele gemäß der Fabasoft Sicherheitsleitlinie sicherstellt:

Vertraulichkeit. Kundendaten, Geschäftsdaten und Daten der Entwicklungsbereiche unterliegen höchsten Vertraulichkeitsanforderungen. Sie dürfen nicht unrechtmäßig zur Kenntnis gelangen (limitierte Zugriffsberechtigungen, Vertraulichkeitsstufen, Verschlüsselung). Alle Fabasoft Mitarbeiterinnen und Mitarbeiter sind zur Wahrung des anwendbaren Datengeheimnisses verpflichtet.

Integrität. Daten und Informationen müssen richtig und vollständig sein. IT-Systeme müssen durchgängig funktionieren. Daten und Informationen dürfen ohne Genehmigung nicht verändert werden.

Authentizität. Informationen dürfen nur von autorisierten Personen bearbeitet werden. Es muss gewährleistest werden, dass Informationen echt und glaubwürdig sind und es sich um manipulationsfreie IT-Systeme und IT-Anwendungen handelt.

Nachvollziehbarkeit. Veränderungen von Informationen müssen eindeutig erkennbar und nachvollziehbar sein (Versionierung).

Verfügbarkeit. Informationen müssen entsprechend der vertraglich zugesicherten Service Levels verfügbar sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf Fabasoft und ihre Stakeholder haben. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

Verantwortung. Alle Mitarbeiterinnen und Mitarbeiter sind sich ihrer Verantwortung beim Umgang mit Daten und IT-Systemen bewusst. Compliance und Awareness für Informationssicherheit wird in allen Unternehmensbereichen gelebt und gefördert.

Zertifizierungen. Zertifizierungen nach international anerkannten Normen und Standards werden im Rahmen unabhängiger, externer Audits regelmäßig erneuert und verleihen dem Fabasoft Sicherheitsniveau Transparenz. Wirksame und effektive Kontrollen zur Erfüllung der Anforderungen sind fester Bestandteil des integrierten Managementsystems.

Datenschutz und Informationssicherheit sind für Fabasoft von zentraler Bedeutung. Dies bescheinigen unter anderem die folgenden aufrechten Unternehmens- bzw. Service-Zertifizierungen und Testate: ISO/IEC 9001, ISO/IEC 27001 inkl. ISO/IEC 27018, ISO/IEC 20000-1, ISAE 3402, BSI C5, SOC 2, TÜV Rheinland Certified Cloud Service, Cyber Risk Rating (Cyber Trust Austria), Ö-Cloud und EU Cloud Code of Conduct. Eine Übersicht der Zertifizierungen und Audits ist auch auf der Website der Fabasoft abrufbar.

Fabasoft speichert Daten auf eigener Hardware in hochsicheren externen Rechenzentren in Deutschland bzw. im Rahmen der Fabasoft Cloud und Fabasoft Folio SaaS in Österreich, Deutschland bzw. der Schweiz. Es wird sichergestellt, dass die Betreiber dieser Rechenzentren eine gültige Zertifizierung nach ISO 27001 haben. Fabasoft bezieht von den Rechenzentren jeweils Stellfläche, Strom, Klimatisierung, Internet-Routing und gegebenenfalls die Verbindung zwischen den Rechenzentren. Die Betreiber der Rechenzentren haben keinen Zugriff auf die Fabasoft Hardware bzw. auf die darauf gespeicherten Daten.

Die hier beschriebenen technischen und organisatorischen Maßnahmen werden laufend an die aktuell gültige Rechtslage des Datenschutzes und den aktuellen Stand der Technik angepasst.

Die gegenständlichen Sicherheitsmaßnahmen berücksichtigen insbesondere auch eine ortsunabhängige Tätigkeit wie etwa in Form von Telearbeit (z. B. Homeoffice). Die hier beschriebenen technischen und organisatorischen Maßnahmen finden gleichermaßen darauf Anwendung. Dadurch ist das Erreichen der Sicherheitsziele unabhängig vom Ort der Tätigkeit durch die hier beschriebenen technischen und organisatorischen Maßnahmen sichergestellt.

2 Technische und organisatorische Maßnahmen

In den folgenden Abschnitten werden die aktuellen Sicherheitsmaßnahmen von Fabasoft beschrieben, die zur Erreichung der Sicherheitsziele implementiert wurden. Diese Sicherheitsmaßnahmen werden regelmäßig auf ihre Aktualität und Wirksamkeit geprüft und gegebenenfalls präzisiert.

2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. a DSGVO)

Die Speicherung und die Übertragung der Daten innerhalb der Fabasoft und auf Fabasoft Systemen erfolgt grundsätzlich verschlüsselt.

Der Zugriff auf Fabasoft Systeme erfolgt grundsätzlich über verschlüsselte Verbindungen.

Die Übertragung personenbezogener Daten über das Intranet und Internet zu den Fabasoft Services erfolgt ebenfalls grundsätzlich verschlüsselt.

Bei der Übertragung von Daten via E-Mail wird eine TLS Verschlüsselung angeboten.

Die Datenübertragung aus dem Fabasoft Netzwerk in andere, externe Netzwerke sowie die Speicherung auf Fabasoft Hardware erfolgt grundsätzlich verschlüsselt.

Die Vergabe von Zutritts- /Zugangs- /Zugriffsberechtigungen erfolgt nach dem Prinzip der minimalen Rechte. Bei der Einstellung wird eigenes Personal durch entsprechende Erklärung auf die Einhaltung von Geheimhaltungs- und Datenschutzvorschriften hin verpflichtet und vom Vorgesetzten eingewiesen.

Der sichere Umgang mit Endbenutzergeräten und Datenträgern wird durch organisatorische und technische Maßnahmen erzwungen.

Änderungen bei den Zugangs-/Zutritts- und Zugriffsrechten erfolgen im Rahmen eines Change-Management-Prozesses (Änderungsverwaltung).

2.1.1 Zutrittskontrolle

Der Zutritt zu den Fabasoft Räumlichkeiten wird mit einem elektronischen Zutrittssystem gesichert. Die Fabasoft Räumlichkeiten sind dabei in unterschiedliche Sicherheitsstufen unterteilt. Der Zutritt zu den Fabasoft Räumlichkeiten ist nur mit elektronischer Zutrittskarte oder Schlüssel möglich. Fehlgeschlagene Zutrittsversuche werden regelmäßig ausgewertet und Auffälligkeiten analysiert.

Betriebsfremde Personen dürfen sich in den Fabasoft Räumlichkeiten nur in bestimmten Bereichen und/oder nur in Begleitung von Fabasoft Personal oder mit entsprechender Genehmigung bewegen.

Für den Zutritt zu externen Rechenzentren bestehen eigene Zutrittskonzepte, die bei der Auswahl des Rechenzentrums und danach regelmäßig von Fabasoft überprüft werden. Der Zutritt zur Fabasoft Hardware in den externen Rechenzentren ist nur autorisierten Personen möglich und wird zusätzlich von Fabasoft überwacht.

2.1.2 Zugangskontrolle

Die Fabasoft Mitarbeiterinnen und Mitarbeiter erhalten nur zu den IT-Services Zugang, die sie zur Erfüllung ihrer Aufgaben benötigen.

Der interne und externe Zugang auf das Fabasoft Netzwerk ist technisch stark eingeschränkt. Der Zugang zu den Fabasoft IT-Services für die Benutzerinnen und Benutzer erfolgt auf Basis der Fabasoft Richtlinien.

Die Vergabe, die Änderung und der Entzug von Zugangsberechtigungen für Benutzerinnen und Benutzer erfolgen gemäß mehrfach geprüfter Fabasoft Prozesse und Sicherheitsrichtlinien.

Programme zur Erkennung von Viren, Malware und unbefugtem Zugang werden eingesetzt. Die Wirksamkeit und der Umfang dieser Programme wird regelmäßig validiert.

Es werden eindeutige Benutzerkennungen vergeben um den Zugang zu den Systemen individuell festzulegen bzw. jeden Benutzer der Fabasoft Systeme eindeutig zu identifizieren. Es sind mehrere Ebenen der Autorisierung implementiert, um den Zugang zu Systemen sicherzustellen.

Der Zugang zu Netzen und zu Computersystemen wird protokolliert (z. B. Anmelde-/ Abmeldeereignisse für Benutzer, Anlegen neuer Benutzer, Kennwortänderungen etc.).

2.1.3 Zugriffskontrolle

Den Zugriff auf personenbezogene, vertrauliche oder sonstige sensible Informationen erhalten nur jene Personen, die zu diesem Zugriff durch ihre Leistungserbringung befugt werden („Least-Privileg-Model“/“Need-to-know-Prinzip“). Dabei werden auch die in der internen Klassifizierungs-Richtlinie definierten Vertraulichkeitsstufen berücksichtigt. Die Protokollierung der Zugriffe und die Handhabung dieser Protokolle sind in den Fabasoft Richtlinien geregelt.

Der Zugriff erfolgt ausschließlich authentisiert mit personalisierten Benutzerkonten.

Der Zugriff auf Daten in den Fabasoft IT-Services ist über die jeweiligen servicespezifischen Zugriffskontrollsysteme geschützt.

Der Zugriff auf Daten in der Fabasoft Cloud und in Fabasoft Folio SaaS wird in Auditlogs protokolliert.

Die Verwendung von Bildschirmsperren ist organisatorisch vorgegeben.

Es bestehen Clean Desk Richtlinien und Clear Screen Anweisungen.

Richtlinien zur Rückgabe oder bei Verlust von mobilen Endgeräten sowie zum Umgang mit mobilen Datenträgern (z. B. USB-Sticks) sind etabliert.

Der Versand bzw. Transport von Datenträgern wird dokumentiert.

Daten, die nicht mehr benötigt werden, werden unter Berücksichtigung der definierten Aufbewahrungsfristen gelöscht.

Verfahrensanweisungen zum Klassifizieren von Dokumenten (Daten) sind intern publiziert und etabliert.

2.1.4 Trennungskontrolle

Systeme für die Softwareentwicklung, Test- und Demosysteme sowie Produktionssysteme werden getrennt voneinander betrieben. Der Betrieb von Entwicklungs-, Test- und Produktionsumgebungen erfolgt auf getrennter Hardware bzw. virtuellen Maschinen.

Die Trennung der Daten in den Produktionssystemen wird durch entsprechende Berechtigungen bzw. Mandantenmechanismen sichergestellt.

Systeme sind netzwerkseitig in adäquate Subnetze separiert.

Über Firewall-Konfigurationen wird erreicht, dass die Kommunikation nur zwischen Netzsegmenten ermöglicht wird, für die die Kommunikation generell möglich sein muss.

2.2 Integrität

Systemkomponenten und Programme sind in einen Patch-Management-Prozess eingebunden.

Ein technisches Schwachstellen-Management dient dem Erkennen neu auftretender Sicherheitslücken unter Berücksichtigung aller relevanten Betriebssysteme sowie relevanter im Einsatz befindlicher Anwendungen und Systemkomponenten.

Für alle Computersysteme erfolgt eine Zeitsynchronisierung.

2.2.1 Weitergabekontrolle

Die Datenübertragung vom Fabasoft Netzwerk in andere, externe Netzwerke sowie die Speicherung auf Fabasoft Hardware erfolgt grundsätzlich verschlüsselt. Die Verwaltung der Schlüssel erfolgt nach Vorgabe in der internen Fabasoft Richtlinie.

Alle Mitarbeiterinnen und Mitarbeiter werden auf das Datengeheimnis verpflichtet und werden regelmäßig im Umgang mit vertraulichen und personenbezogenen Daten geschult.

Eine Policy zum gesicherten Versand von Datenträgern ist etabliert.

2.2.2 Eingabekontrolle

Die Netzkommunikation über die Grenzen eines virtuellen Netzes (VTP Domain) erfolgt immer über eine physische Firewall.

Die Computersysteme sind gegen Schadsoftware geschützt.

Im Rahmen des Loggings von Benutzertransaktionen in den Fabasoft IT-Services Fabasoft Cloud und Fabasoft Folio SaaS kann überprüft und festgestellt werden von wem personenbezogene Daten eingegeben oder verändert wurden.

2.3 Verfügbarkeit und Wiederherstellbarkeit

Fabasoft verfügt über Prozesse und Maßnahmen, die das Backup und die Wiederherstellung der Fabasoft IT-Systeme sicherstellen.

Notfälle werden regelmäßig geübt. Notfallprozesse und -handbücher werden regelmäßig auf Aktualität und Angemessenheit geprüft.

2.3.1 Verfügbarkeitskontrolle

Die Rechenzentren sind physisch geschützt gegen Feuer, Wasser, Erdbeben, Explosionen, zivile Unruhen und andere Formen natürlicher und von Menschen verursachter Katastrophen.

Die Rechenzentren verfügen über ausreichende, dem Betriebszweck angemessene Klimatisierung.

Die Rechenzentren verfügen über ausreichend dimensionierte USV.

Die Rechenzentren verfügen über Netzersatzanlagen.

Das Rechenzentrum und die Computersysteme sind bei hohen Verfügbarkeitsanforderungen redundant ausgelegt.

Die IT-Betriebsprozesse sind dokumentiert und gepflegt.

Vorausschauende Planung und Vorbereitung ermöglichen, dass angemessene Kapazitäten und Ressourcen verfügbar bleiben, um die geforderte Systemleistung zu erbringen. Um das Risiko von Systemüberlastungen zu reduzieren, werden Abschätzungen für zukünftige Kapazitätsanforderungen durchgeführt. Die Betriebsanforderungen von neuen Systemen werden ermittelt, dokumentiert und getestet, bevor diese abgenommen und benutzt werden.

Server, Applikationen und Systemsoftware werden innerhalb des Asset Management geführt.

Der Zutritt zur IT Infrastruktur (Server- und Netzwerkverteilerräumen) ist nur befugtem Personal erlaubt.

Es werden regelmäßig alle notwendigen Security Patches installiert und die Notwendigkeit der Installation wird regelmäßig überwacht.

Endgeräte, Datenbanken und Applikationen sind vor schädlichem Code geschützt.

2.3.2 Verfügbarkeit der eingesetzten IT-Systeme

Die Entwicklung der Software erfolgt fehlertolerant und vor der Inbetriebnahme werden umfangreiche Belastungstests durchgeführt.

Für die Fabasoft Cloud und Mindbreeze InSpire SaaS findet regelmäßig ein PEN-Test statt, um die Belastbarkeit des Systems zu überprüfen.

2.4 Maßnahmen zur Wiederherstellung der Verfügbarkeit und dem Zugang zu personenbezogenen Daten bei einem technischen Zwischenfall

2.4.1 Recovery / Backup-Systeme

Es existiert ein Datensicherungskonzept, das auf die Einhaltung des maximal tolerierbaren Datenverlusts ausgerichtet ist.

Die Datensicherungen befinden sich an einem Ausweichstandort bzw. werden generell redundant auf zwei Standorten persistiert.

Für Notfälle existieren Notfallpläne zum raschen Wiederanlauf und zur Wiederherstellung der Systeme und Daten.

Die Notfallpläne werden vor ihrer erstmaligen Freigabe getestet.

Die Notfallpläne werden mindestens jährlich geübt.

2.5 Zweckgebundenheit, Überprüfung, Bewertung und Evaluierung

2.5.1 Auftragskontrolle

Fabasoft gestattet es nur autorisierten Personen im Rahmen ihrer Aufgabenerfüllung personenbezogene Daten zu verarbeiten. Alle Mitarbeiterinnen und Mitarbeiter sind im Umgang mit personenbezogenen Daten geschult. Die Weitergabe von personenbezogenen Daten zur Verarbeitung an externe Dienstleister erfolgt ausschließlich basierend auf Auftragsdatenverarbeitungsvereinbarungen.

Fabasoft hat Kontrollen und Prozesse implementiert, um die Einhaltung der Vertragserfüllung durch Fabasoft und ihre Dienstleister sicherzustellen.

2.5.2 Datenschutzmanagement

Jährlich erfolgt eine Überprüfung der IT Kontrollen nach ISO 27001 in Form eines (Überwachungs-)Audits durch die Prüfstelle.

Verarbeitungstätigkeiten sind gemäß gesetzlicher Vorgaben dokumentiert.

Es liegen gültige Risikoanalysen zu den Verarbeitungen personenbezogener Daten vor.

Fabasoft Mitarbeiterinnen und Mitarbeiter, die personenbezogene Daten verarbeiten, absolvieren regelmäßig eine Datenschutzschulung.

Die Rolle des Informationssicherheitsbeauftragten ist definiert und zugewiesen.

Datenschutzbeauftragte sind gemäß den gesetzlichen Vorgaben bestellt und auf www.fabasoft.com/privacy abrufbar.

Ein Verfahren zum Vorgehen im Falle einer Datenschutzverletzung ist etabliert.