



Leistungsmerkmale Datensicherheit

Fabasoft Cloud

Gültig ab 25.05.2018

Vertraulich

Copyright © Fabasoft R&D GmbH, AT-4020 Linz, 2018.

Alle Rechte vorbehalten. Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Marken der jeweiligen Hersteller.

Diese Unterlagen sind vertraulich.

Durch die Übermittlung und Präsentation dieser Unterlagen alleine werden keine Rechte an unserer Software, an unseren Dienstleistungen und Dienstleistungsergebnissen oder sonstigen geschützten Rechten begründet.

Die Weitergabe, Veröffentlichung oder Vervielfältigung ist nicht gestattet.

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

Der Schutz von personenbezogenen Daten und der Schutz der Informationen, die Kunden in der Fabasoft Cloud aufbewahren, ist für Fabasoft ein zentrales Anliegen. In diesem Dokument dokumentiert Fabasoft, wie die Fabasoft Cloud Daten schützt, verarbeitet und wie Daten mit anderen Nutzern ausgetauscht werden können.

Zudem hat sich Fabasoft als Gründungsmitglied zur Einhaltung des EU Cloud Code of Conduct verpflichtet.

Die Schlüsselinformationen zum Umfang des EU Cloud Code of Conduct können online unter <https://www.fabasoft.com/cloudservices/eucloudcoc> abgerufen werden.

Fabasoft Cloud Kunden können sich bei Fragen in Bezug auf die Verarbeitung von personenbezogenen Daten über die E-Mail-Adresse privacy@fabasoft.com an Fabasoft wenden. Diese Kontaktmöglichkeit steht auch für die Meldung und Kommunikation bei Sicherheits- und Datenschutzvorfällen zur Verfügung.

2 Performance

2.1 Umkehrbarkeit und Beendigungsprozess

Fabasoft ist ausdrücklich berechtigt, die in den Fabasoft Cloud Rechenzentren vom Kunden gespeicherten Daten nach Ablauf einer Frist von mindestens 4 Monaten und höchstens 6 Monaten, gerechnet ab Vertragsbeendigung, endgültig – das heißt nicht wiederherstellbar – zu löschen. Der Kunde wird bei Vertragsabschluss darauf hingewiesen und erhält vor Ablauf der Kündigungsfrist eine Erinnerungsinformation (siehe Fabasoft Cloud AGB, Punkt 4.6).

| Zielsetzung | |
|--|---|
| Zeitraum für Zugriffsmöglichkeit auf Benutzerdaten (Data retrieval period) | Bei einer Kündigung des Vertrags deaktiviert Fabasoft die Zugriffsmöglichkeiten auf die Fabasoft Cloud für den Kunden mit Beendigung des Vertrags. Siehe Fabasoft Cloud AGB, Punkt 4.6 |
| Zeitraum für die Aufbewahrung von Benutzerdaten (Data retention period) | Bei einer Kündigung des Vertrags ist Fabasoft berechtigt, die Benutzerdaten frühestens 4 Monate und spätestens 6 Monate nach Beendigung dieses Vertrags zu löschen. Siehe Fabasoft Cloud AGB, Punkt 4.6 |
| Zusätzliche Aufbewahrung von Benutzerdaten (Residual data retention) | Auf Wunsch des Kunden, der gegenüber Fabasoft vor Ablauf von 4 Monaten, gerechnet ab der Vertragsbeendigung, schriftlich per E-Mail zu erklären ist, ist Fabasoft innerhalb einer Zeitspanne von mindestens 4 Monaten und höchstens 6 Monaten nach Beendigung dieses Vertrags bereit, |

| | |
|--|--|
| | <p>vom Kunden konkret bezeichnete Daten, die der Kunde gemäß diesem Vertrag auf der von Fabasoft betriebenen Infrastruktur gespeichert hat, gegen im Einzelfall festzulegendes Entgelt dem Kunden auf maschinenlesbaren Aufzeichnungsträgern auszufolgen.</p> <p>Siehe Fabasoft Cloud AGB, Punkt 4.6</p> |
|--|--|

3 Sicherheit

3.1 Servicezuverlässigkeit

Die Verfügbarkeit der Fabasoft Cloud Services ist auf mindestens 99,9 % pro Beobachtungszeitraum (Quartal) ausgelegt. Die Rechenzentren orientieren sich an der Tier-III-Spezifikation des Uptime Institutes. Nähere Informationen finden Sie im Dokument „Leistungsmerkmale Rechenzentrumsbetrieb“.

| Zielsetzung | |
|------------------------|---|
| Redundanz | Siehe Leistungsmerkmale Rechenzentrumsbetrieb |
| Servicezuverlässigkeit | Siehe Leistungsmerkmale Rechenzentrumsbetrieb |

3.2 Authentifizierung und Autorisierung

Folgende Zwei-Faktor-Authentifizierungsmethoden stehen (abhängig von der Fabasoft Cloud Edition/dem gewählten Servicepaket) zur Verfügung.

Authentifizierung

- Benutzername und Passwort
 - Der Benutzername ist eine gültige E-Mail-Adresse des Benutzers.
 - Falls der Benutzer sein Passwort vergessen hat, kann ein neues Passwort über einen Link, der an die E-Mail-Adresse des Benutzers geschickt wird, vom Benutzer gesetzt werden. Die Möglichkeit des Zurücksetzens des Passworts wird beim Login angeboten.
 - Das Passwort wird von Fabasoft nicht im Klartext gespeichert und kann von Fabasoft nicht rekonstruiert werden.
- Client-Zertifikat
 - Das Wurzelzertifikat der CA und aller Zwischen-CAs müssen vom Administrator des Kunden in der Fabasoft Cloud Organisation konfiguriert werden, so dass eine Validierung des Client-Zertifikats bei der Authentisierung eines Benutzers erfolgen kann.
 - Der Kunde muss den Zugriff zu einer Sperrliste in der Fabasoft Cloud Organisation konfigurieren. Im Falle der Deaktivierung eines Client-Zertifikats durch den Kunden muss das zu deaktivierende Client-Zertifikat auf diese Sperrliste gesetzt werden.
- Single Sign-on (Active Directory)
 - Der Kunde muss ein von der Fabasoft Cloud über das Internet zugreifbares AD FS (Microsoft Active Directory Federation Services) betreiben. Das Authentisierungsservice

der Fabasoft Cloud ist als „Relying Party Trust“ im AD FS des Kunden zu konfigurieren. Für die Konfiguration in der Fabasoft Cloud müssen die erforderlichen Metadaten (FederationMetadata.xml) des AD FS vom Kunden bereitgestellt werden.

- Single Sign-on (SAML 2.0)
 - Der Kunde muss einen von der Fabasoft Cloud über das Internet zugreifbaren SAML 2.0 Identity Provider betreiben. Das Authentisierungsservice der Fabasoft Cloud ist als Service Provider im Identity Provider des Kunden zu konfigurieren. Für die Konfiguration in der Fabasoft Cloud müssen die erforderlichen Metadaten (metadata.xml) des Identity Providers vom Kunden bereitgestellt werden.
- Digital ID (deutscher Personalausweis, österreichische Bürgerkarte mit Handysignatur, SuisseID)
 - Falls die Anmeldung über eine Digital ID selbst auf mindestens zwei Faktoren beruht, entfällt die im nächsten Abschnitt beschriebene Validierung eines zweiten Faktors durch die Fabasoft Cloud.

Zweiter Faktor (sofern nicht die Authentisierung selbst auf zwei Faktoren beruht)

- Mobile PIN (SMS)
 - Eine fünfstellige Zahl (PIN) wird an eine Telefonnummer des Benutzers geschickt, welche dieser nach der Anmeldung mit dem ersten Faktor eingeben muss.
 - Diese PIN ist 5 Minuten lang gültig.
- E-Mail-PIN
 - Eine fünfstellige Zahl (PIN) wird an die E-Mail-Adresse des Benutzers geschickt, welche dieser nach der Anmeldung mit dem ersten Faktor eingeben muss.
 - Diese PIN ist 5 Minuten lang gültig.
- Einmalpasswort über RADIUS-Server
 - Der Kunde muss einen von der Fabasoft Cloud über das Internet zugreifbaren RADIUS-Server betreiben. Die Zugriffsdaten auf den RADIUS-Server müssen vom Administrator des Kunden in der Fabasoft Cloud Organisation konfiguriert werden.

Der Administrator des Kunden der Fabasoft Cloud Organisation kann für die Mitglieder seiner Organisation bzw. seiner externen Organisationen die Parameter für die Authentisierung konfigurieren, insbesondere die Telefonnummer bzw. E-Mail-Adresse für Mobile PIN und E-Mail-PIN, sowie eine Auswahl treffen, welche Methoden für den zweiten Faktor überhaupt und bevorzugt von den Mitgliedern verwendet werden müssen.

Autorisierung

Die Autorisierung des Zugriffs auf Benutzerdaten erfolgt über Teamrooms. Für jeden Teamroom können Teammitgliedern Zugriffsrechte (Leserechte, Änderungsrechte, alle Rechte) gewährt werden. Die Suche nach Benutzerdaten erfolgt unter Berücksichtigung der Zugriffsrechte. Es werden nur Treffer angezeigt, auf welche der jeweilige Benutzer auch zugreifen darf.

Ein Benutzer mit allen Rechten kann für einen Teamroom konfigurieren, dass so genannte „Öffentliche Links“ in diesem Teamroom erlaubt sind. Ein öffentlicher Link erlaubt den Zugriff auf den Teamroom, auf einen Ordner, auf ein Dokument oder auf sonst einen Inhalt im Teamroom, ohne vorherige Authentisierung, lediglich die Kenntnis des Links ist erforderlich. Darüber hinaus kann bei einem öffentlichen Link der Gültigkeitszeitraum des Links sowie ein Passwort hinterlegt werden. Diese Parameter werden beim Zugriff auf den Link geprüft, der

Zugriff wird – falls der Gültigkeitszeitraum abgelaufen ist und/oder das Passwort nicht korrekt angegeben wurde – vom System verweigert. Bei einem öffentlichen Link auf einen Teamroom oder Order ist der gesamte Inhalt des Teamrooms oder Ordners über diese öffentlichen Link zugänglich.

Der Zugriff auf die Fabasoft Cloud mit Drittanwendungen, die nur Benutzername und Passwort ohne zweiten Faktor unterstützen (z. B. Verbinden als Netzlaufwerk), muss über eigens dafür generierte Passwörter erfolgen. Für die Passwörter muss eine Gültigkeit festgelegt werden. Diese Passwörter für Anwendungen können während ihrer Gültigkeit und nach Ablauf der Gültigkeit vom Benutzer verlängert bzw. während ihrer Gültigkeit widerrufen werden.

| Zielsetzung | |
|---|---|
| Sicherheit der Authentifizierungsverfahren | aktueller Stand der Technik |
| Authentifizierungsverfahren | Benutzername und Passwort, Client-Zertifikat, Single Sign-on (Active Directory), Single Sign-on (SAML 2.0), Digital ID Grundsätzlich Zwei-Faktoren-Authentisierung |
| Entziehen der Rechte bei Organisationsausschluss | unmittelbar nach Deaktivierung eines Benutzer-Kontos durch den Administrator des Kunden |
| Schutz der Anmeldedaten | Passwörter für die Anmeldung werden in einem getrennten Service verschlüsselt und nicht rekonstruierbar gespeichert. |
| Unterstützung von Drittanbieter-Authentifizierungsverfahren | Digital ID, AD FS, SAML 2.0 RADIUS-Server für zweiten Faktor |

3.3 Verschlüsselung

Der Zugang zur Fabasoft Cloud ist nur über HTTPS mit TLS-Verschlüsselung möglich.

Die Benutzerdaten werden auf verschlüsselten Festplatten (SEDs), die mindestens dem Standard FIPS 140-2 Level 2 oder einem vergleichbaren Standard entsprechen, oder verschlüsselten Dateisystemen (EFS) abgelegt. Damit sind die Daten bei Verlust der Hardware geschützt.

Die gesondert zu erwerbende Appliance „Secomo“ (inkl. Hardwaresicherheitsmodul) erweitert die Fabasoft Cloud um eine Ende-zu-Ende-Verschlüsselung für hochsensible Dokumente. Die Entschlüsselung der Benutzerdaten erfolgt mit Secomo direkt und ausschließlich am Arbeitsplatz des Benutzers.

| Zielsetzung | |
|--|---|
| Absicherung gegen Brute-Force-Angriffe | Transport: HTTPS mit TLS-Verschlüsselung Storage: SEDs, EFSs |

| | |
|---------------------------------------|---|
| Absicherung der Schlüssel | Schlüssel werden am Zielsystem erstellt und verlassen die Zielsysteme nicht. Der Zugriff auf die Schlüssel wird über restriktive Zugriffsrechte (TLS) oder Kennwörter (beispielsweise SEDs oder EFS) gesichert. |
| Verwendung von Hochsicherheitsmodulen | Wird mit „Secomo“ als Zusatzprodukt von Fabasoft angeboten. |

3.4 Protokollierung und Überwachung

Auditing

Im Rahmen der Nachvollziehbarkeit werden die folgenden Auditing-Informationen gesammelt:

- Zugriffe auf Dokumente (lesend und bearbeitend)
- Änderungen von Metadaten
- Auflösen von Teamrooms und Löschen von Dokumenten
- Löschen der Historie von Teamrooms
- Zugriff auf öffentliche Links
- Export von Metadaten der Kontaktverwaltung

Abhängig von der Edition können Benutzer in Teamrooms mit allen Rechten auf die Auditlog-Auswertungen zugreifen. Auditlog-Einträge werden mindestens 12 Monate aufbewahrt. Der Kunde hat die Möglichkeit, die Auditlog-Einträge zu exportieren und gesondert aufzubewahren. Die Auditlog-Einträge werden spätestens nach Beendigung dieses Vertrags gemeinsam mit den Benutzerdaten nach Ablauf einer Frist von mindestens 4 Monaten und höchstens 6 Monaten (gerechnet ab Vertragsbeendigung) endgültig gelöscht.

Protokollierung

Fabasoft app.telemetry zeichnet jede Anfrage (HTTPS-Requests) an die Fabasoft Cloud im zeitlichen Verlauf auf. Die Erfassung dieser Transaktionsinformationen erfolgt am Arbeitsplatz des Benutzers im Web Browser und im Fabasoft Cloud Client, in den mobilen Apps der Fabasoft Cloud, sowie in den Services und Systemkomponenten der Fabasoft Cloud. Diese Transaktionsinformationen werden ausschließlich für die laufende Verbesserung der Dienste verwendet. Die Protokollierung umfasst keine Benutzerdaten. Die Aufbewahrungszeit für diese Transaktionsinformationen wird je Applikation und Ebene individuell festgelegt und beträgt höchstens 12 Monate.

Im Rahmen der Protokollierung von Betriebssystem und Basissoftware-Events sowie von applikationsspezifischen Events werden die Informationen protokolliert, die die jeweiligen Systeme standardmäßig zur Verfügung stellen. Betriebssystem, Basissoftware-Events sowie applikationsspezifischen Events werden maximal 6 Monate aufbewahrt.

Überwachung

Fabasoft app.telemetry wird zur Überwachung der einzelnen Systemkomponenten der Fabasoft Cloud und zur Überwachung von Performance und Verfügbarkeit aus Anwendersicht eingesetzt.

| Zielsetzung | |
|---|---|
| Auswahl der Daten im Log | Sicherheitsrelevante Benutzerdaten werden nicht protokolliert |
| Zugriffsmöglichkeiten des Kunden auf Logs | Der Zugriff auf Auditing-Information ist für entsprechend berechnigte Benutzer des Kunden im Web Client möglich, dort ist auch ein Export der Auditing-Information möglich. |

3.5 Audits und Sicherheitsverifizierungen

Externe und interne Sicherheitsanalysen sowie Audits der technischen, physikalischen und organisatorischen Sicherheitsmaßnahmen und Betriebsprozesse tragen maßgebend zur Sicherheit Ihrer Daten bei.

| Zielsetzung | |
|--|---|
| Externe Überprüfung der Sicherheit und des Datenschutzes durch Zertifizierungen und 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 Sterne) |

3.6 Governance

Geplante Wartungsarbeiten werden auf folgender Webseite mindestens 14 Tage vorher angekündigt: <https://www.fabasoft.com/cloudservices/system-status>. In dringenden Fällen (z.B. bei Gefahr in Verzug) können Wartungsarbeiten auch ad hoc durchgeführt werden.

Die Updates der Fabasoft Cloud werden im Allgemeinen als Zero-Downtime-Updates durchgeführt. Vorgesehen ist, dass Cloud Apps monatlich aktualisiert werden und die Fabasoft Cloud Basis alle zwei Monate. Die Neuigkeiten für jedes Update werden im „What’s New“-Dokument dokumentiert und auf <https://help.cloud.fabasoft.com> zur Verfügung gestellt.

Vertragliche Änderungen werden mindestens 14 Tage vor In-Kraft-Treten angekündigt.

| Zielsetzung | |
|-------------------------------|--|
| Bekanntmachung von Änderungen | „What’s-New“-Dokument auf https://help.cloud.fabasoft.com Vertragliche Änderungen auf https://www.fabasoft.com/cloudservices/gtc |

4 Datenmanagement

4.1 Datenklassifizierung

Benutzerdaten

Daten, die der Kunde in die Fabasoft Cloud einbringt oder in der Fabasoft Cloud erstellt, werden in Teamrooms gespeichert, die einer Organisation zugeordnet sind. Der Eigentümer der Organisation hat alle Rechte auf die darin gespeicherten Daten. Durch die beim Teamroom festgelegten Zugriffsrechte kann der Eigentümer bzw. jenes Organisationsmitglied, das den Teamroom erstellt, definieren, wer auf diese Daten Zugriff hat, bzw. wer diese Daten ändern oder löschen darf.

Benutzerdaten werden nicht zwischen Lokationen synchronisiert, sondern bleiben in der Lokation des Teamrooms, in dem sie gespeichert wurden.

Kontaktdaten

Kontaktdaten für die Zusammenarbeit in der Fabasoft Cloud werden in folgenden Situationen erfasst:

- ein zukünftiger Kunde gibt im Zuge des Registrierungsprozesses seine Kontaktdaten ein.
- Kontaktdaten von internen und externen Organisationsmitgliedern eines Kunden erfasst der Administrator der Organisation.
- Kontaktdaten von externen Organisationsmitgliedern können auch von Mitgliedern der Organisation beim Festlegen der Zugriffsrechte auf einen Teamroom erfasst werden.

Kontaktdaten können grundsätzlich vom Administrator der Organisation, der der Kontakt zugehört, geändert und korrigiert werden.

Kontaktdaten von Kontakten, die sich noch nicht in der Fabasoft Cloud registriert haben, können vom Ersteller der Kontaktdaten geändert, korrigiert und wieder gelöscht werden.

Der Kontakt selbst kann jedenfalls auch nach der Registrierung in der Fabasoft Cloud seine Kontaktdaten ändern und korrigieren, bzw. über den Fabasoft-Support-Button in der Fabasoft Cloud löschen lassen.

Kontaktdaten sind nicht allgemein einsehbar. Kontaktdaten werden über die vollständige E-Mail-Adresse identifiziert. Wenn im Zuge des Erfassens eines Kontakts vom System festgestellt wird, dass zur eingegebenen E-Mail-Adresse schon Kontaktdaten erfasst wurden, dann erhält der Benutzer Zugriff auf die allgemeinen Kontaktdaten (Foto, Vorname, weitere Vornamen, Nachname, Titel, nachgestellter Titel, Geschlecht, Geburtsdatum, Anrede, E-Mail-Domäne, Website, Organisation, Funktion in der Organisation, Zuordnung zu Organisationseinheiten, Zuordnung zu Teams, Zuordnung zu externen Organisationen, Sprache, Registrierungsstatus).

Diese allgemeinen Kontaktdaten sind auch im Kontext des Teamrooms für die anderen Teammitglieder einsehbar, falls dies nicht anders beim Teamroom konfiguriert wurde.

Im Rahmen des Versands einer Mobile PIN wird die Telefonnummer eines Kontakts an SMS-Provider übermittelt.

Die Kontaktdaten werden über alle Cloud-Lokationen synchronisiert.

Kaufmännische Daten

Kaufmännische Daten sind Informationen, die für die Abwicklung der Geschäftsbeziehung mit dem Kunden erforderlich sind (Bestellungen, Rechnungen, Auslastungsinformationen der lizenzierten Servicepakete je Organisation ...).

Abgeleitete Daten

Abgeleitete Daten sind Log- und Transaktionsinformationen, die keine Benutzerdaten umfassen. Diese Informationen werden ausschließlich für die Aufrechterhaltung des Betriebs, die Einhaltung der Service Levels und die laufende Verbesserung der Dienste verwendet.

| Zielsetzung | |
|-------------------------------------|--|
| Verarbeitung von Benutzerdaten | Keine andere Verarbeitung von Daten als vom Kunden angefordert |
| Verarbeitung von abgeleiteten Daten | Keine andere Verarbeitung von Daten als vom Kunden angefordert |

4.2 Datenlebenszyklus

| Zielsetzung | |
|------------------|--|
| Art der Löschung | Benutzerdaten können vom Kunden endgültig gelöscht werden (Ausleeren eines Papierkorbs, Auflösen eines Teamrooms). Ab diesem Zeitpunkt ist kein Zugriff mehr auf diese Daten (Metadaten und Dokumente) möglich. Metadaten und Referenzen auf Dokumente werden dabei unmittelbar, die Dokumente selbst frühestens nach vier und spätestens nach sechs Monaten gelöscht. |

4.3 Datenportabilität

Dokumente eines Teamrooms können vom Kunden als strukturiertes ZIP-Archiv oder über WebDAV exportiert werden. Auf Metadaten kann über CMIS (Content Management Interoperability Services) zugegriffen werden. Der konsolidierte Export aller historischen Versionen eines Dokuments ist nicht möglich.

| Zielsetzung | |
|--------------|---|
| Datenformate | Original-Dokumentformate XML für Metadaten über CMIS |
| Interfaces | HTTPS, WebDAV, CMIS |

5 Schutz personenbezogener Daten

5.1 Verhaltenskodizes, Standards und Zertifizierungsmechanismen

Insoweit Daten „personenbezogene Daten“ im Sinn der EU-Datenschutz-Grundverordnung oder des jeweilig national anzuwendenden Datenschutzgesetzes umfassen, beachtet Fabasoft entsprechend das Datengeheimnis sowie die sonstigen datenschutzrechtlichen Vorschriften im Sinne der anwendbaren EU-Normen und der nationalen materiellen datenschutzrechtlichen Vorschriften.

| Zielsetzung | |
|---|--|
| Verhaltenskodizes, Standards und Zertifizierungsmechanismen | Die EU-Normen und die national anzuwendenden Datenschutzgesetze werden eingehalten |

5.2 Spezifikation des Verwendungszwecks

Fabasoft verarbeitet personenbezogene Daten zu keinem anderen Zweck als vom Kunden angefordert und zur Vertragserfüllung erforderlich.

| Zielsetzung | |
|------------------|---|
| Verwendungszweck | <p>zur Erfüllung der vertraglichen Verpflichtungen mit dem Kunden (Art 6 Abs 1 lit b DSGVO);</p> <p>zur Durchführung vorvertraglicher Maßnahmen (Art 6 Abs 1 lit b DSGVO);</p> <p>zum Zwecke berechtigter Interessen unseres Unternehmens oder aufgrund von berechtigten Interessen Dritter (Art 6 Abs 1 lit f DSGVO), nämlich</p> <ul style="list-style-type: none">• zum Zwecke der Direktwerbung hinsichtlich von Fabasoft Produkten und Dienstleistungen;• zum Zwecke der Verhinderung von Missbrauchsfällen;• zum Zwecke interner Verwaltung;• zur Gewährleistung der Netz- und Informationssicherheit;• für Archivzwecke. |

Jene Daten, die Fabasoft im Zuge des Vertragsverhältnisses mit dem Kunden erlangt hat, wird Fabasoft verarbeiten, um dem Kunden zum Zwecke der Darstellung und Präsentation der Produkte von Fabasoft E-Mails, postalische Briefe oder Werbeprospekte zukommen zu lassen (Art 6 Abs 1 lit f DSGVO). Gegen diese Verarbeitung der Daten des Kunden zum Zwecke der Direktwerbung hat der Kunde ein jederzeitiges Widerspruchsrecht ohne Angabe von Gründen durch postalisches Schreiben an Fabasoft oder durch E-Mail an privacy@fabasoft.com. Fabasoft wird die Daten des Kunden für diesen Zweck solange verarbeiten, als der Kunde nicht widerspricht, jedoch nur bis 3 Jahre nach Vertragsbeendigung. Für andere Formen der Direktwerbung wird Fabasoft die Daten des Kunden nur dann verarbeiten, wenn der Kunde eine ausdrückliche Einwilligung in die Verarbeitung seiner Daten erteilt hat (Art 6 Abs 1 lit a DSGVO). Sollte

der Kunde in die Datenverarbeitung eingewilligt haben, kann er diese Einwilligung ohne Angabe von Gründen durch postalisches Schreiben an Fabasoft oder durch E-Mail an privacy@fabasoft.com widerrufen. Die Verarbeitung der personenbezogenen Daten des Kunden zum Zwecke der Direktwerbung ist für die Abwicklung des Vertragsverhältnisses nicht erforderlich.

Die Daten des Kunden werden für keinen anderen Zweck weiterverarbeitet.

In den folgenden Kapiteln sind die Daten aufgelistet, die erhoben und verarbeitet werden.

5.2.1 Benutzerdaten

Benutzerdaten werden von der Fabasoft Cloud ausschließlich für die vom Kunden angeforderten Zwecke gemäß des Hauptvertrags und den Weisungen des Kunden verarbeitet.

5.2.2 Kontaktdaten

Organisation:

Name, Rechnungsadresse, UID-NR, Servicepakete, Mitglieder, Organisationseinheiten, Teams, externe Mitglieder, externe Organisationseinheiten, Standard-Teamrooms, Adressen, Telefonnummern, E-Mail-Adressen, Logos, Eigentümer, Administratoren, Austritte, Einkäufe, Richtlinien, Verschlüsselung, Authentifizierungseinstellungen, Sicherheitseinstellungen und weitere Konfigurationseinstellungen

Organisationseinheiten:

Name, Mitglieder, Standard-Teamrooms, Hierarchieebene, Austritte, Importkennung, Sicherheitseinstellungen und weitere Konfigurationseinstellungen

Benutzer (erforderliche Daten):

E-Mail-Adresse (Log-in), Vorname, Nachname, Organisationen, Lokation, Anmeldeinformationen (Zeitpunkt des Logins, Zeitpunkt des Logouts, Zeitpunkt des letzten Zugriffs, Authentifizierungsmethode und -typ, Arbeitsplatz, IP-Adresse)

Benutzer (optionale Daten):

Foto, weitere Vornamen, Titel, nachgestellter Titel, Geschlecht, Geburtsdatum, Anrede, Funktion in der Organisation, Zuordnung zu Organisationseinheiten, Zuordnung zu Teams, Zuordnung zu externen Organisationen, Sprache, Registrierungsstatus, Adressen, Telefonnummern, E-Mail-Adressen, Website, zugeteilte Edition, zugeteilte Apps, Mitgliedschaftsstatus, letzte Statusänderung, letzter Log-in (Datum und Lokation), Versandart für Mobile PIN, Mobiltelefonnummer für Mobile PIN, E-Mail-Adresse für Mobile PIN, Benutzerkennung am RADIUS-Server, Common Name (Zertifikats-Log-in), Digital-ID-Daten (Kennung, Vorname, Nachname), Passwort, Deaktivierte Authentifizierungsmethoden, Richtlinien, Importkennung

Arbeitsumgebung

Konfigurationseinstellungen für den Benutzer (z. B. Sprache, Gebietsschema, Standardwährung, Einstellungen zu Bedienhilfen usw.)

5.2.3 Zusammenarbeit

Um die Zusammenarbeit von Benutzern zu ermöglichen, sind folgende Daten für einen Benutzer sichtbar, wenn ein Benutzer die E-Mail-Adresse eines anderen Benutzers kennt:

Foto, Vorname, weitere Vornamen, Nachname, Titel, nachgestellter Titel, Geschlecht, Geburtsdatum, Anrede, E-Mail-Domäne, Organisation, Funktion in der Organisation, Website, Zuordnung zu Organisationseinheiten, Zuordnung zu Teams, Zuordnung zu externen Organisationen, Sprache, Registrierungsstatus, Importkennung

5.2.4 Cookies

Die Fabasoft Cloud Services benutzen nach Ihrer Anmeldung sogenannte „Session-Cookies“, mit denen Sie während der Dauer Ihres Besuchs identifiziert werden können. Die Session-Cookies enthalten Teile Ihrer Anmeldedaten in verschlüsselter Form. Nach dem Ende der Sitzung verfallen Session-Cookies automatisch.

Die Fabasoft Cloud Services benutzen „permanente Cookies“, um Informationen über Nutzer festzuhalten, die wiederholt auf Fabasoft Cloud Services zugreifen. Der Zweck des Einsatzes dieser permanenten Cookies besteht darin, unsere Produkte und Dienstleistungen für Sie kontinuierlich zu verbessern und leichter bedienbar zu machen. Eine Einzelprofilbildung über Ihr Nutzungsverhalten findet nicht statt.

5.3 Datenminimierung

Fabasoft wird personenbezogene Daten nur solange speichern, wie es für jene Zwecke erforderlich ist, für die die Daten erhoben wurden.

| Zielsetzung | |
|---|--|
| Aufbewahrungszeit von temporären Daten | In der Fabasoft Cloud werden temporäre Dateien und Dokumente grundsätzlich nach deren Verwendung gelöscht. Aus Stabilitätsgründen ist darüber hinaus keine weitere Garbage-Collection implementiert, insbesondere auch, da davon keine personenbezogenen Daten betroffen sind. |
| Aufbewahrungszeit von personenbezogenen Daten | Vertragsende: siehe Fabasoft Cloud AGB Ansonsten: Wenn Daten vom Kunden gelöscht werden |

5.4 Benutzungs-, Aufbewahrungs- und Auskunftseinschränkung

Insoweit Fabasoft aufgrund einer gesetzlichen Verpflichtung oder im Zug eines rechtlichen Verfahrens vor Gericht oder einer sonstigen staatlichen Autorität verpflichtet wird, bei Fabasoft vom Kunden gespeicherte Daten dem Gericht oder der sonstigen staatlichen Autorität zugänglich zu machen, geht Fabasoft folgendermaßen vor:

- Sofern Fabasoft dadurch keine Gesetze verletzt, wird Fabasoft den Kunden hievon so rasch als möglich (elektronisch) verständigen, um dem Kunden dadurch die Möglichkeit zu verschaffen, gegen die Zugänglichmachung der Daten insbesondere rechtliche Schutzmaßnahmen auf eigene Kosten zu versuchen.
- Fabasoft wird – in vernünftiger Weise erwartbarem Umfang – mit dem Kunden kooperieren, um dessen Datenschutzinteresse zu unterstützen.

| Zielsetzung | |
|--|---------------------------|
| Anzahl von gesetzlichen Auskunftsanfragen | Wird nicht veröffentlicht |
| Anzahl von gesetzlichen Auskunftsanfragen mit Kundenmitteilung | Wird nicht veröffentlicht |

5.5 Offenheit, Nachvollziehbarkeit und Ankündigungsmanagement

Fabasoft stellt Ihre Daten Dritten grundsätzlich nicht zur Verfügung, außer aus einer gesetzlichen Verpflichtung heraus oder auf Ihren Wunsch, also mit Ihrer Einwilligung. Das ist z. B. bei einer Einladung zu einem Teamroom oder beim Kauf einer Cloud App eines Drittherstellers der Fall.

In den folgenden Kapiteln sind die Daten aufgelistet, die Dritten weitergeleitet/ an Dritte übermittelt werden. Alle unten aufgelisteten Dritten werden hinsichtlich Informationssicherheit sorgfältig ausgewählt und gegebenenfalls auch überprüft.

| Zielsetzung | |
|-----------------|-----------------------------------|
| Dritte | Siehe Aufstellung ab Punkt 5.5.1 |
| Datenkategorien | Kontaktdaten, keine Benutzerdaten |

5.5.1 Act-On

An Act-On Software, Inc., 8300 SW Creekside Place, Suite 250, Beaverton, Oregon 97008, USA werden folgende Daten zu Marketingzwecken übermittelt:

Objektadresse (interne ID), E-Mail-Adresse, Titel, Vorname, Nachname, Registrierungsdatum, Anrede, Geschlecht, Geburtsdatum, Firma, Organisation, Funktion in der Organisation, Land, Sprache, Einmal-Nutzer, Produkt-Edition, Produkt-Abo-Start, Produkt-Abo-Typ, Produkt-Abo-Ende, Maximaler Speicherverbrauch, Speicherverbrauch „Ist“, Maximale Anzahl der Objekte, Anzahl der Objekt „Ist“, Letzter Login, Anzahl der Apps, Kampagnen-Code, Aktiviert, Registrierungsadresse (z. B. <https://www.fabasoft.com>)

Act-On Software, Inc. ist nach dem REU-US Privacy-Shield zertifiziert. Nähere Informationen dazu sind unter <https://www.privacyshield.gov> abrufbar.

5.5.2 Microsoft Office Online

Office Online ist ein Service von Microsoft und die Verwendung unterliegt daher den Nutzungsbedingungen und der Privacy Policy von Microsoft. Um eine Datei anzeigen bzw. bearbeiten zu können, erstellt Office Online eine temporäre Kopie dieser Datei auf Office Online Servern. Zusätzlich wird der Name des Benutzers sowie interne IDs des Bearbeiters und des Eigentümers bereitgestellt.

Diese Funktionalität ist optional. Der Fabasoft Cloud Kunde kann in der Fabasoft Cloud Organisation festlegen, ob den Mitgliedern seiner Organisation diese Möglichkeit der Betrachtung und/oder Bearbeitung von Dokumenten zur Verfügung steht oder nicht.

5.5.3 A-Trust

An A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, Landstraßer Hauptstraße 5, 1030 Wien, Österreich werden folgende Daten für die Anmeldung mit der „Handysignatur“ übermittelt:

Mobiltelefonnummer und Signatur-Passwort (diese Daten werden über ein auf der Anmeldeseite der Fabasoft Cloud eingebettetes Formular von A-Trust vom Benutzer angefordert.)

5.5.4 Governikus GmbH & Co. KG

An Governikus GmbH & Co. KG, Am Fallturm 9, 28359 Bremen, Deutschland (vormals bremen online services GmbH & Co. KG) werden folgende Daten für die Anmeldung mit dem „Neuen Deutschen Personalausweis“ übermittelt:

Vorname, Nachname, PIN (diese Daten werden über ein eingebettetes Formular direkt an Governikus GmbH & Co. KG übergeben)

5.5.5 Dolphin Systems AG

An Dolphin Systems AG, Samstagernstraße 45, 8832 Wollerau, Schweiz, werden folgende Daten für die Zustellung der Mobile-PIN im Falle einer 2-Faktoren-Authentisierung über SMS übergeben:

Mobiltelefonnummer für Mobile-PIN, E-Mail-Adresse für die Anmeldung, Mobile-PIN

5.5.6 Simple SMS GmbH

An Simple SMS GmbH, Dr.-Schauer-Straße 26, 4600 Wels, Österreich, werden folgende Daten für die Zustellung der Mobile-PIN im Falle einer 2-Faktoren-Authentisierung über SMS übergeben:

Mobiltelefonnummer für Mobile-PIN, E-Mail-Adresse für die Anmeldung, Mobile-PIN

5.5.7 atms Telefon- und Marketing Services GmbH

An atms Telefon- und Marketing Services GmbH, Saturn Tower, Leonard-Bernstein-Straße 10, 1220 Wien, Österreich, werden folgende Daten für die Zustellung der Mobile-PIN im Falle einer 2-Faktoren-Authentisierung über SMS übergeben:

Mobiltelefonnummer für Mobile-PIN, E-Mail-Adresse für die Anmeldung, Mobile-PIN

5.6 Verantwortlichkeit

Der Eigentümer der Organisation wird per Einschreiben informiert, wenn Fabasoft einen unautorisierten Zugriff auf die Benutzerdaten der Organisation oder die Kontaktdaten beobachtet, ebenso, wenn es eine ausreichende begründete Verdachtslage gibt. Darüber

hinaus wird Fabasoft versuchen, mit dem Eigentümer der Organisation so rasch wie möglich telefonisch oder per E-Mail Kontakt aufzunehmen.

| Zielsetzung | |
|--------------------------------|---|
| Richtlinien bei Datendiebstahl | Siehe Text dieses Kapitels. |
| Dokumentation | https://www.fabasoft.com/trust Leistungsmerkmale Datensicherheit Leistungsmerkmale Rechenzentrumsbetrieb |

5.7 Geografische Lokation der Daten

Der Kunde kann für die Speicherung der Benutzerdaten (Teamrooms, Ordner, Dokumente usw.) zwischen verschiedenen Lokationen wählen (vertragsgegenständliche Lokation). Benutzerdaten werden außerhalb der vertragsgegenständlichen Lokation nur nach ausdrücklicher, schriftlicher Zustimmung des Kunden verarbeitet, gespeichert und gesichert.

Die Daten zum Benutzer, zur Organisation und zur Organisationseinheit (Kontaktdaten) werden über alle Lokationen (Deutschland, Österreich, Schweiz) hinweg repliziert und synchronisiert. Eine Auflistung der betroffenen Daten finden Sie im Kapitel 5.2 „Spezifikation des Verwendungszwecks“. Einstellungen in der Benutzer-Arbeitsumgebung werden ebenfalls synchronisiert, sofern der Benutzer einmal in die entsprechende Lokation gewechselt hat.

Daten, die an Subunternehmen übermittelt werden, werden entsprechend den Bedingungen der Subunternehmen verarbeitet (siehe Kapitel 5.5 „Offenheit, Nachvollziehbarkeit und Ankündigungsmanagement“).

| Zielsetzung | |
|-----------------------------------|---|
| Liste der verfügbaren Lokationen | Deutschland, Österreich, Schweiz |
| Auswahlmöglichkeit der Lokationen | Für Benutzerdaten vom Kunden wählbar Kontaktdaten werden zwischen allen Lokationen der Fabasoft Cloud synchronisiert |

5.8 Intervenierbarkeit / datenschutzrechtliche Rechte

Der Kunde kann Auskunft darüber verlangen, welche Daten Fabasoft über ihn verarbeitet (siehe im Detail Art 15 DSGVO). Er kann seine in der Fabasoft Cloud gespeicherten Daten vom Fabasoft Cloud Support einschränken (sperrern, siehe Art 18 DSGVO), berichtigen oder löschen lassen (siehe Art 16 DSGVO). Der Kunde hat das Recht, der Datenverarbeitung zu widersprechen (siehe Art 21 DSGVO) sowie das Recht auf Datenübertragbarkeit (Art 20 DSGVO).

Benutzerdaten können nur vom Kunden selbst bzw. von Benutzern, die der Kunde in den Teamrooms, die die Benutzerdaten beinhalten, berechtigt, gelesen, korrigiert und gelöscht werden.

Sollte es, trotz der Verpflichtung von Fabasoft, die Daten des Kunden rechtmäßig zu verarbeiten, wider Erwarten zu einer Verletzung des Rechtes des Kunden auf rechtmäßige

Verarbeitung seiner Daten kommen, hat der Kunde das Recht, eine Beschwerde bei der Österreichischen Datenschutzbehörde oder bei einer anderen Datenschutz-Aufsichtsbehörde in der EU, insbesondere an Ihrem Aufenthalts- oder Arbeitsort zu erheben.

| Zielsetzung | |
|---------------|---|
| Reaktionszeit | Kontaktinformation zum Fabasoft Support und Support-Zeiten sind definiert. (siehe Leistungsmerkmale Rechenzentrumsbetrieb) |