Leistungsmerkmale Datensicherheit

für ein Servicepaket on Fabasoft PROCECO

Gültig ab 1. Januar 2024
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

Die Leistungsmerkmale Datensicherheit des Servicepakets werden im Nachfolgenden beschrieben.

Kunden können sich bei Fragen in Bezug auf die Verarbeitung von personenbezogenen Daten über die im Informationsblatt CSA unter „Kontaktmöglichkeiten“, „Datenschutz“ angegebene E-Mail-Adresse an den Auftragnehmer wenden. Diese Kontaktmöglichkeit steht auch für die Meldung und Kommunikation bei Sicherheits- und Datenschutzvorfällen zur Verfügung.

2 Performance

2.1 Umkehrbarkeit und Beendigungsprozess

Der Auftragnehmer ist ausdrücklich berechtigt, die in den Datenlokationen 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 Cloud Service Agreement, Punkt 4.6).

Zielsetzung	
Zeitraum für Zugriffsmöglichkeit auf Benutzerdaten (Data retrieval period)	Bei einer Kündigung des Vertrags deaktiviert der Auftragnehmer die Zugriffsmöglichkeiten auf das Servicepaket für den Kunden mit Beendigung des Vertrags. Siehe Cloud Service Agreement, Punkt 4.6
Zeitraum für die Aufbewahrung von Benutzerdaten (Data retention period)	Bei einer Kündigung des Vertrags ist der Auftragnehmer berechtigt, die Benutzerdaten frühestens 4 Monate und spätestens 6 Monate nach Beendigung dieses Vertrags zu löschen. Siehe Cloud Service Agreement, Punkt 4.6
Zusätzliche Aufbewahrung von Benutzerdaten (Residual data retention)	Auf Wunsch des Kunden, der gegenüber dem Auftragnehmer vor Ablauf von 4 Monaten, gerechnet ab der Vertragsbeendigung, schriftlich per E-Mail zu erklären ist, ist der Auftragnehmer innerhalb einer Zeitspanne von mindestens 4 Monaten und höchstens 6 Monaten nach Beendigung dieses Vertrags bereit, vom Kunden konkret bezeichnete Daten, die der Kunde gemäß diesem Vertrag gespeichert hat, gegen im Einzelfall festzulegendes Entgelt dem Kunden auf maschinenlesbaren Aufzeichnungsträgern auszufolgen. Siehe Cloud Service Agreement, Punkt 4.6

3 Sicherheit

3.1 Servicezuverlässigkeit

Die Verfügbarkeit des Servicepakets des Auftragnehmers ist auf mindestens 99,9 % pro Beobachtungszeitraum (Quartal) ausgelegt. 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 vom 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 vom Auftragnehmer nicht im Klartext gespeichert und kann vom Auftragnehmer nicht rekonstruiert werden.
- Client-Zertifikat
  - Das Wurzelzertifikat der (Certificate Authority) 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 Organisation 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.

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.
  - Die SMS für die 2-Faktoren-Authentifizierung wird über externe Dienstleister versendet, wobei die Zustellung der SMS über den Mobilfunkbetreiber des Kunden oder einen Roamingpartner dieses Mobilfunkbetreibers erfolgt und daher an diesen die für die Zustellung erforderlichen personenbezogene Daten übermittelt werden. Bei Kunden mit einer Mobiltelefonnummer aus Drittstaaten oder dann, wenn sich der Kunde in einem Drittstaat befindet, werden die für die Zustellung der Nachricht erforderlichen personenbezogenen Daten an einen Mobilfunkbetreiber oder Roamingpartner in diesem Drittland übermittelt.
- 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 Links zugänglich.

Der Zugriff auf das Servicepaket 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) 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	AD FS, SAML 2.0 RADIUS-Server für zweiten Faktor

3.3 Verschlüsselung

Der Zugang zum Servicepaket 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 „Fabasoft Secomo“ (inkl. Hardwaresicherheitsmodul) erweitert das Servicepaket um eine Ende-zu-Ende-Verschlüsselung für hochsensible Dokumente. Die Entschlüsselung der Benutzerdaten erfolgt mit Fabasoft 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 vom Servicepaket können Benutzer in Teamrooms mit allen Rechten auf die Auditlog-Auswertungen zugreifen. Auditlog-Einträge werden mindestens 13 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 das Servicepaket im zeitlichen Verlauf auf. Die Erfassung dieser Transaktionsinformationen erfolgt am Arbeitsplatz des Benutzers im Web Browser und im Cloud Client bzw. in den mobilen Apps, 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 13 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 13 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 berechtigte Benutzer des Kunden im Web Client möglich, dort ist auch ein Export der Auditing-Information möglich.

3.5 Governance

Geplante Wartungsarbeiten werden auf der im Informationsblatt CSA unter „Weitere hilfreiche Links“, „Cloud Services/System Status“ genannten Webseite mindestens 14 Tage vorher angekündigt. In dringenden Fällen (z.B. bei Gefahr in Verzug) können Wartungsarbeiten auch ad hoc durchgeführt werden.

Die Neuigkeiten für jedes Update werden im „What’s New“-Dokument dokumentiert und unter der im Informationsblatt CSA angegebenen Website „Weitere hilfreiche Links“, „What`s New“ zur Verfügung gestellt.

Zielsetzung	
Bekanntmachung von Änderungen	Link zu „What’s-New“-Dokument gemäß Informationsblatt CSA Link zu „Vertragsgrundlagen“ gemäß Informationsblatt CSA in der jeweils aktuellen Fassung

4 Datenmanagement

4.1 Datenklassifizierung

Benutzerdaten

Daten, die der Kunde in das Servicepaket einbringt oder in dem Servicepaket erstellt, werden in Teamrooms gespeichert, die einer Fabasoft Cloud Organisation zugeordnet sind. Der Eigentümer der Fabasoft Cloud 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. Zur Sicherstellung der Verfügbarkeit kann eine Kopie (Sicherung) der Benutzerdaten in einer anderen Lokation (siehe Kapitel 5.6) gespeichert werden.

Die Benutzerdaten des Kunden bleiben ausschließlich in der Verfügungsmacht des Kunden und sind dem Auftragnehmer inhaltlich weder bekannt, noch unterliegen sie – ohne ausdrückliche Berechtigung durch den Kunden – dem direkten Zugriff des Auftragnehmers.

Kontaktdaten

Kontaktdaten für die Zusammenarbeit im Servicepaket 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 Fabasoft Cloud Organisation.
- Kontaktdaten von externen Organisationsmitgliedern können auch von Mitgliedern der Fabasoft Cloud Organisation beim Festlegen der Zugriffsrechte auf einen Teamroom erfasst werden.

Kontaktdaten können grundsätzlich vom Administrator der Fabasoft Cloud 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 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 Fabasoft 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 Verantwortungsbereiche

Die Benutzerdaten des Kunden bleiben ausschließlich in der Verfügungsmacht des Kunden. Der Kunde ist für die Rechtmäßigkeit der Verarbeitung dieser Daten, sowie die datenschutzrechtlichen Verpflichtungen, die mit der Datenverarbeitung einhergehen, selbst verantwortlich.

In den Fällen, in denen der Auftragnehmer als Auftragsverarbeiter für den Kunden auftritt, erfolgt eine Verarbeitung der Daten, die vom Kunden an den Auftragnehmer weitergegeben werden, ausschließlich aufgrund einer Weisung durch den Kunden. Der Auftragnehmer wird

den Kunden bei der Wahrnehmung seiner datenschutzrechtlichen Verpflichtungen unterstützen. Im Dokument „Vereinbarung zur Auftragsdatenverarbeitung“ sind die Verpflichtungen des Kunden als Verantwortlicher, sowie jene des Auftragnehmers als Auftragsverarbeiter präzisiert.

4.3 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.

4.4 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 der Auftragnehmer 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

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

Zielsetzung	
Verwendungszweck	zur Erfüllung der vertraglichen Verpflichtungen mit dem Kunden (Art 6 Abs 1 lit b DSGVO); zur Durchführung vorvertraglicher Maßnahmen (Art 6 Abs 1 lit b DSGVO); zum Zwecke berechtigter Interessen unseres Unternehmens oder aufgrund von berechtigten Interessen Dritter (Art 6 Abs 1 lit f DSGVO), nämlich • 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 Kontaktdaten, die der Auftragnehmer im Zuge des Vertragsverhältnisses mit dem Kunden erlangt hat, wird der Auftragnehmer verarbeiten, um dem Kunden zum Zwecke der Darstellung und Präsentation der Produkte des Auftragnehmers E-Mails, postalische Briefe oder Werbeprospekte zukommen zu lassen (Art 6 Abs 1 lit f DSGVO). Gegen diese Verarbeitung der Kontaktdaten des Kunden zum Zwecke der Direktwerbung hat der Kunde ein jederzeitiges Widerspruchsrecht ohne Angabe von Gründen durch postalisches Schreiben an den Auftragnehmer oder durch E-Mail an die im Informationsblatt CSA unter „Kontaktmöglichkeiten“, „Datenschutz“ angegebenen E-Mail-Adresse. Der Auftragnehmer wird die Kontaktdaten des Kunden für diesen Zweck solange verarbeiten, als der Kunde nicht widerspricht, jedoch nur maximal drei Jahre ab der letzten Aktivität. Für andere Formen der Direktwerbung wird der Auftragnehmer die Kontaktdaten 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 den Auftragnehmer oder durch E-Mail an die im Informationsblatt CSA unter „Kontaktmöglichkeiten“, „Datenschutz“ angegebenen E-Mail-Adresse widerrufen. Die Verarbeitung der personenbezogenen Kontaktdaten des Kunden zum Zwecke der Direktwerbung ist für die Abwicklung des Vertragsverhältnisses nicht erforderlich.

Die Kontaktdaten 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

Die Benutzerdaten bleiben ausschließlich in der Verfügungsmacht des Kunden und sind dem Auftragnehmer weder inhaltlich bekannt, noch unterliegen sie – ohne ausdrückliche Berechtigung durch den Kunden – dem direkten Zugriff des Auftragnehmers.

Eine Verarbeitung von Benutzerdaten durch den Auftragnehmer erfolgt ausnahmsweise im Einzelfall, aufgrund ausdrücklichen schriftlichen Verlangens und/oder erteilter Freigabe der konkreten Benutzerdaten durch den Kunden. Diese Benutzerdaten werden von der Fabasoft Cloud ausschließlich für die vom Kunden angeforderten Zwecke gemäß der Rahmenvereinbarung Cloud Service Agreement und/oder 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, E-Mail-Domänen, Support-Koordinator, Compliance-Manager, Support-Team, E-Mail-Kommunikation in Zusammenhang mit der Organisationsverwaltung, 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), zugeteilte Lösungen, zugeteilte Apps, Mitgliedschaftsstatus, letzte Statusänderung, letzter Log-in (Datum und Lokation)

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, 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, Stellvertreter, Betreff

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 Support

Der Auftragnehmer bietet einen 1st Level Support für seinen Kunden. Das Erfassen einer Supportanfrage ist mit dem Support-Button direkt im Webinterface, im Cloud Client bzw. in den mobilen Apps für iOS und Android generell rund um die Uhr möglich. Durch die Verwendung des Support-Button werden Namen, E-Mail-Adresse und die Problembeschreibung an den Support des Auftragnehmers übermittelt. Zur besseren Nachvollziehbarkeit des Problems kann der Benutzer optional einen Screenshot sowie im Cloud Client auch Systeminformationen über den Arbeitsplatz und Protokoll-Dateien mitsenden. Diese Daten und die anschließende Kommunikation werden in einer Supportanfrage gesammelt. Auf die Supportanfragen kann der Benutzer jederzeit über den Menüpunkt „Meine Supportanfragen“ im Kontomenü zugreifen.

Der Zugriff auf die Supportanfragen und der im Zuge der Abarbeitung übermittelten Daten ist auf Support Mitarbeiter des Auftragnehmers und der sonstigen Sub-Auftragsverarbeiter betreffend Support-Leistungen sowie den Einbringer der Supportanfragen beschränkt.

5.2.5 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 des Auftragnehmers 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

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

Zielsetzung	
Aufbewahrungszeit von temporären Daten	Im Servicepaket 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 Cloud Service Agreement Ansonsten: Wenn Daten vom Kunden gelöscht werden

5.4 Offenheit, Nachvollziehbarkeit und Ankündigungsmanagement

Der Auftragnehmer 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.

Die Liste von Sub-Auftragsverarbeitern, an die Daten weitergeleitet bzw. übermittelt werden, ist online abrufbar unter der im Informationsblatt CSA unter „Link zu Vertragsgrundlagen“ angegebenen Website.

5.5 Verantwortlichkeit

Die in den Datenschutzeinstellungen der Fabasoft Cloud Organisation namhaft gemachte Person wird entweder per Einschreiben oder per E-Mail informiert, wenn der Auftragnehmer einen unautorisierten Zugriff auf die Benutzerdaten der Fabasoft Cloud Organisation oder die Kontaktdaten beobachtet, ebenso, wenn es eine ausreichende begründete Verdachtslage gibt. Darüber hinaus wird der Auftragnehmer versuchen, mit dieser Person so rasch wie möglich telefonisch oder per E-Mail Kontakt aufzunehmen.

Zielsetzung	
Richtlinien bei Datendiebstahl	Siehe Text dieses Kapitels.
Dokumentation	Übersicht der Zertifizierungen und Audits Leistungsmerkmale Datensicherheit Leistungsmerkmale Rechenzentrumsbetrieb

5.6 Geografische Lokation der Daten

Der Kunde kann für die Speicherung der Benutzerdaten (Teamrooms, Ordner, Dokumente usw.) zwischen verschiedenen Lokationen wählen (vertragsgegenständliche Lokation). Die Wahl einer anderen als der vertragsgegenständlichen Lokation ist nur aufgrund einer gesonderten, speziellen, schriftlichen Vereinbarung möglich.

Die Daten zum Benutzer, zur Fabasoft Cloud 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 5.4 „Offenheit, Nachvollziehbarkeit und Ankündigungsmanagement“.

Zielsetzung	
Liste der verfügbaren Lokationen	Deutschland, Österreich, Schweiz
Auswahlmöglichkeit der Lokationen	Für Benutzerdaten vom Kunden wählbar Zur Sicherstellung der Verfügbarkeit kann eine Kopie (Sicherung) der Benutzerdaten in einer anderen Lokation gespeichert werden Kontaktdaten werden zwischen allen Lokationen der Fabasoft Cloud synchronisiert

5.6.1 Datenübermittlung / Download Drittland

Eine Verarbeitung durch den Auftragnehmer erfolgt in Österreich, Deutschland und in der Schweiz. Es werden daher durch den Auftragnehmer grundsätzlich keine Daten in ein Drittland übermittelt.

Die Benutzerdaten bleiben ausschließlich in der Verfügungsmacht des Kunden und sind dem Auftragnehmer weder inhaltlich bekannt, noch unterliegen sie dem direkten Zugriff des Auftragnehmers.

Durch die Verwendung des Servicepakets auf Endgeräten des Kunden in einem Drittland, kann es zu einer Datenübertragung in ein Drittland durch den Kunden kommen. Der Kunde ist in diesem Fall für die Einhaltung der anwendbaren datenschutz-rechtlichen Bestimmungen selbst verantwortlich.

5.7 Intervenierbarkeit / Datenschutzrechtliche Rechte

Das anwendbare Datenschutzrecht gewährt dem Kunden verschiedene Rechte in Zusammenhang mit der Bearbeitung seiner personenbezogenen Daten. Insbesondere kann der Kunde Auskunft darüber verlangen, welche Daten (= Kontaktdaten) der Auftragnehmer über ihn verarbeitet (siehe im Detail Art 15 DSGVO). Er kann seine in der Fabasoft Cloud gespeicherten Daten (= Kontaktdaten) vom Support des Auftragnehmers einschränken (sperren, 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 des Auftragnehmers, 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 Ihres Landes, insbesondere an Ihrem Aufenthalts- oder Arbeitsort zu erheben.

Zielsetzung

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

5.7.1 Self-Service durch Customer

Die Benutzerdaten bleiben ausschließlich in der Verfügungsmacht des Kunden und sind dem Auftragnehmer weder inhaltlich bekannt, noch unterliegen sie – ohne ausdrückliche Berechtigung durch den Kunden – dem direkten Zugriff des Auftragnehmers. Eine Verwaltung dieser Benutzerdaten (z.B. Löschen, etc.) kann daher nur durch den Kunden selbst erfolgen.

Der Kunde kann über die Einstellungen im Servicepaket eine Anleitung abrufen, die es ihm unter anderem eigenverantwortlich ermöglicht seine Kontaktdaten abzufragen und direkt selbst zu bearbeiten. Über den Support kann der Kunde – unter Berücksichtigung der datenschutz-rechtlichen Vorgaben – seine Kontaktdaten löschen, berichtigen, anonymisieren oder übertragen lassen.