

# DOKUMENTATION DER DATENSCHUTZ- UND INFORMATIONSSICHERHEIT VON DOCPLUS PREMIUM

## ALLGEMEINE DOKUMENTENINFORMATIONEN

### Unternehmen

Haufe-Lexware GmbH & Co. KG, Munzinger Str. 9, D-79111 Freiburg

### Dokumenten Titel

Dokumentation der Datenschutz- und Sicherheitsmaßnahmen von DocPlus Premium

Dokumentenverantwortlicher	Seiten	Version	Nächste Aktualitätsprüfung
Michael Kienzler	1	1.0	31.12.2026

# INHALTSVERZEICHNIS

Allgemeine Dokumenteninformationen	1
<b>Allgemeine Informationen</b>	<b>3</b>
1.1 Applikationsbeschreibung	3
1.2 Netzwerk- /Architektur-diagramm	4
1.3 Weitere Angaben zur Organisation des Datenschutzes und der Datensicherheit	5
1.4 Hosting der Applikation	5
1.5 Hosting der Applikation für die Anbindung eines HRIS des Kunden	6
1.6 Hosting des Large Language Modell	6
1.7 Spezielle Sicherheitsmaßnahmen	6
<b>Technische und organisatorische Maßnahmen</b>	<b>7</b>

# ALLGEMEINE INFORMATIONEN

Dieses Dokument wurde auf Basis von vorgelegten Informationen von Amazon Webservices und Mitarbeitern der IT und Entwicklungsabteilungen der Haufe Group nach Durchführung von Interviews durch die Autoren nach bestem Wissen erarbeitet.

## 1.1 APPLIKATIONSBESCHREIBUNG

Die Software Haufe DocPlus ist ein Produkt, das eine vereinfachte Erstellung von HR-Dokumenten ermöglicht. DocPlus Premium optimiert hierzu zwei Bereiche – die Kernfunktion der Erstellung durch Vorlagen, Layout und Dokumentenmanagement, sowie Kollaborationsfunktionalitäten wie Freigabe- und Inputworkflows.

### Die wesentlichen Funktionen im Überblick:

Die Kernfunktion von DocPlus besteht aus drei Bereichen:

- Im Layoutbereich können unterschiedliche Layoutvorlagen angelegt werden. Hier werden entweder Kopf-, Fußzeile und Logo, Schriftarten, Zeilenabstände und Ränder in der Applikation angelegt oder aus einer Word-Vorlage übernommen.
- Der Zweite Bereich ist der Vorlagenbereich: hier stehen über 30 rechtssichere Haufe Vorlagen zur Verfügung, die Individualisiert werden können. Außerdem können eigene Vorlagen angelegt oder mit dem KI Upload hochgeladen werden. Im Vorlagenbereich werden Textblöcke, Eingabefelder und Logiken angelegt.
- Der dritte Bereich ist der Dokumentenbereich, in dem durch Auswahl von Textblöcken und das Ausfüllen der Eingabefeldern ein Dokument erstellt wird.

### Die Kollaboration

Neben den Kernfunktionen unterstützt DocPlus auch bei Prozessen, die rund um das HR-Dokument entstehen.

DocPlus bildet den Prozess der Informationssammlung, sowie der Freigabe ab.

DocPlus bietet durch die Änderungshistorie und den Status volle Transparenz

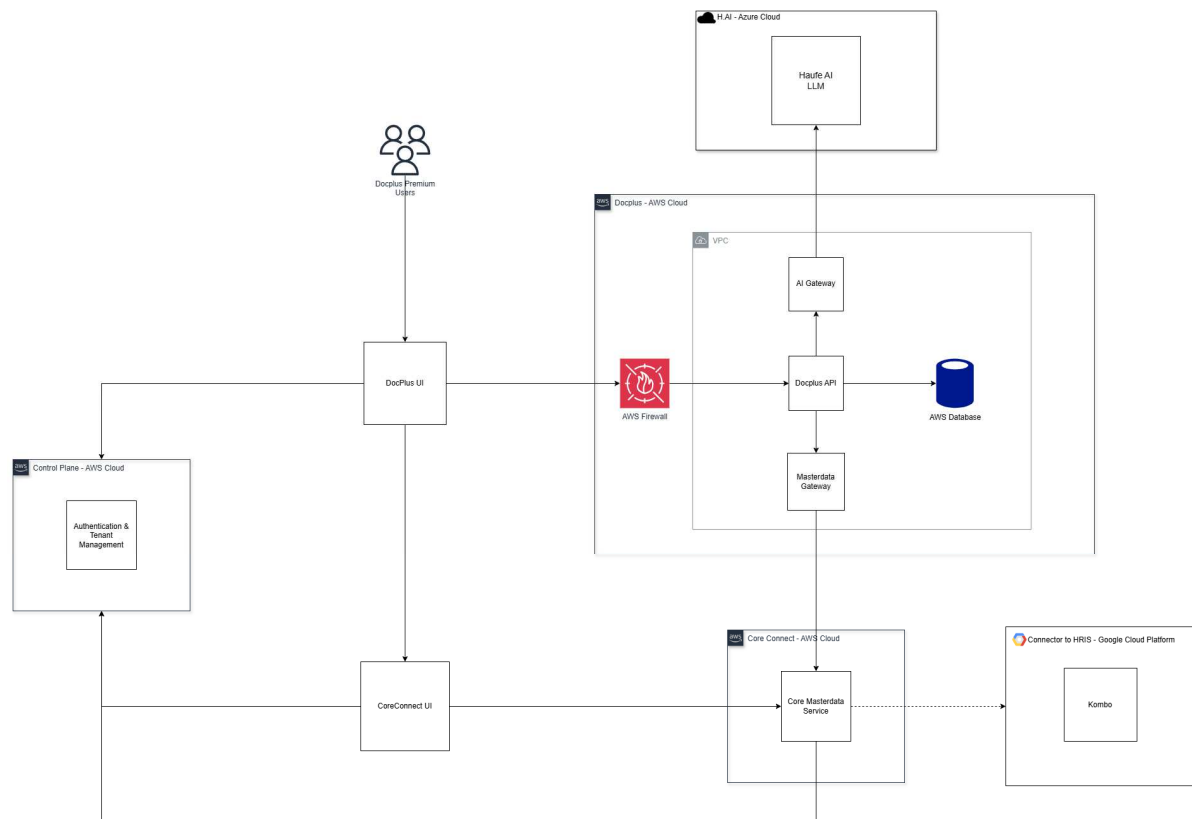
### Künstliche Intelligenz

Beim Hochladen von Dokumenten/Formularen durch die Nutzer verwenden wir eine KI-Komponente. Diese KI-Komponente identifiziert die entsprechenden Abschnitte und Eingabefelder und bereitet die Dokumente/Formulare für die weitere Verwendung entsprechend auf.

Die Basis hierfür bildet das Sprachmodell (Large Language Model, LLM) von OpenAI sowie spezialisierte Agenten für verschiedene Detailaufgaben.

Die hochgeladenen Dokumente/Formulare werden nicht zum Training des LLM verwendet, so dass hier eine datenschutzkonforme Verarbeitung der Daten gewährleistet ist.

## 1.2 NETZWERK- /ARCHITEKTUR-DIAGRAMM



## 1.3 WEITERE ANGABEN ZUR ORGANISATION DES DATENSCHUTZES UND DER DATENSICHERHEIT

Innerhalb der Haufe Group existieren diverse Richtlinien und Vorgaben hinsichtlich der Informationssicherheit beziehungsweise der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit. Zu unseren internen Richtlinien gehören unter anderem:

- Vertraulichkeitsvereinbarungen: Innerhalb der Haufe Group existieren diverse Vorlagen für ein- oder beidseitige Vertraulichkeitsvereinbarungen. Auch sind entsprechende Vereinbarungen Teil der Verträge, die durch den Stabsbereich Legal erstellt sowie betreut werden.
- Datenschutzrichtlinie der Haufe Group: Ziel und Zweck ist es, die Grundlagen für die Umsetzung der Datenschutzanforderungen aus der Datenschutz-Grundverordnung (DSGVO) und dem BDSG festzulegen. Festgelegt sind Grundprinzipien der Datenverarbeitung, der Aufbau der Datenschutzorganisation, Rollenverteilung der Organe innerhalb der Datenschutzorganisation, Datenschutzmanagement-Grundlagen, die Datenübertragung an Dritte, das Verhalten bei Datenschutzvorfällen sowie die Sanktionen bei Verstößen.
- Richtlinie Datenschutzvorfälle in der Haufe Group: Geregelt werden der Umgang mit Datenschutzvorfällen oder Datenpannen, angemessene und rechtskonforme Reaktion bei Datenschutzvorfällen und die rechtlichen Meldepflichten.
- Darüber hinaus existieren bei der Haufe Group Richtlinien zum Themengebiet der Datensicherheit, welche Handlungsanweisungen hinsichtlich sicherer Entwicklung, Authentifizierung und dem Umgang mit Passwörtern enthalten.

Für die Haufe-Lexware GmbH & Co. KG, Haufe-Lexware Services GmbH & Co. KG und Haufe Service Center GmbH ist:

Herr Raik Mickler, E-Mail: [dsb@haufe-lexware.com](mailto:dsb@haufe-lexware.com)

als Datenschutzbeauftragter bestellt.

Alle Mitarbeiter/-innen sind schriftlich auf die Vertraulichkeit verpflichtet. Die Dokumentation der Verpflichtung erfolgt in der Personalabteilung der Haufe-Lexware Services GmbH & Co. KG. Weiterhin erfolgen jährliche Datenschutzzschulungen der Datenschutzvorgaben in Form von Präsenzs Schulungen oder webbasierten Trainings.

Haufe-Lexware GmbH & Co. KG verarbeitet die Daten ausschließlich im Zusammenhang mit der Erfüllung von Vertrags-/Bestellverpflichtungen ihrer Kunden. Bei Firmenkunden werden Verträge gem. Art. 28 DSGVO über die Auftragsdatenverarbeitung abgeschlossen.

## 1.4 HOSTING DER APPLIKATION

Das Hosting von DocPlus Premium erfolgt in einem Rechenzentrum der Amazon Web Services in Frankfurt am Main (EU-central-1). Mit diesem Dienstleister besteht ein Vertrag nach Art. 28 DSGVO über Auftragsdatenverarbeitung.

AWS verfügt über die folgenden Zertifizierungen:

- ISO 27001: Informationssicherheit allgemein

- ISO 27017: Informationssicherheit beim Cloud Computing
- ISO 27018: Datenschutz-Standard für Cloud Dienste
- ISO 27701: Erweiterung der ISO 27001 hinsichtlich Datenschutz
- ISO 22301: Standard für Business Continuity Management
- BSI C5: Cloud Computing Compliance Criteria Catalogue des BSI

## 1.5 HOSTING DER APPLIKATION FÜR DIE ANBINDUNG EINES HRIS DES KUNDEN

Die Applikation der Kombo Technologies GmbH, Berlin, wird im Rechenzentrum der Google Cloud in den Niederlanden (Europe-west4) gehostet.

## 1.6 HOSTING DES LARGE LANGUAGE MODELL

Das LLM von OpenAI wird bei Azure Sweden Central gehostet.

## 1.7 SPEZIELLE SICHERHEITSMASSNAHMEN

Wegen des Schutzbedarfs der Daten werden:

- Die Server-Systeme in das kommerzielle Vulnerability Management System der Haufe Group aufgenommen. Dieses System führt in zyklischen Abständen authentifizierte Scans der Server-Systeme durch und überprüft diese auf das Fehlen von Sicherheitsupdates.
- Externe Penetrationstest der Applikation durch Dritte zyklisch durchgeführt (i.d.R. jährlich).
- Alle Daten sind at rest verschlüsselt.

# TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

## 1. Allgemeines

1.1 Existieren formale schriftlich dokumentierte Richtlinien hinsichtlich der Informationssicherheit?	<p>Ja, es existieren diverse Richtlinien und Vorgaben hinsichtlich der Informationssicherheit beziehungsweise der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit, wie z.B.:</p> <ul style="list-style-type: none"> <li>• Vertraulichkeitsvereinbarungen</li> <li>• Datenschutzrichtlinie</li> <li>• Richtlinie Datenschutzvorfälle</li> </ul>
1.2 Ist ein Datenschutzbeauftragter bestellt?	<p>Herr Raik Mickler E-Mail: <a href="mailto:dsb@haufe-lexware.com">dsb@haufe-lexware.com</a></p>
1.3 Ist ein IT-Sicherheitsbeauftragter / Chief Information Security Officer beschäftigt?	<p>Jochen Vogel ist der CISO der Haufe Group. E-Mail: <a href="mailto:security@haufe-lexware.com">security@haufe-lexware.com</a></p>
1.4 Werden die Mitarbeiter/-innen auf Vertraulichkeit verpflichtet? Wie werden diese Verpflichtungen dokumentiert?	<p>Sämtliche Mitarbeiter, die mit personenbezogenen Daten arbeiten, sind auf Vertraulichkeit verpflichtet. Die Dokumentation erfolgt in der Personalabteilung.</p>
1.5 Sind die Mitarbeiter/-innen hinsichtlich der datenschutzrechtlichen Vorgaben nachweislich geschult?	<p>Ja, es finden regelmäßige Trainings zur Sensibilisierung statt.</p>
1.6 Gibt es ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DSGVO?	<p>Ja</p>
1.7 Wer wird bei entdeckten Sicherheitsvorfällen unverzüglich informiert?	<p>Der CISO der Haufe Group, bei möglichen Verletzungen des Schutzes personenbezogener Daten der Datenschutzbeauftragte der Haufe Group.</p>
1.8 Sind die Ergebnisse von Penetration-Tests einsehbar?	<p>Eine Einsichtnahme ist möglich. Details zu möglichen Schwachstellen oder Informationen mit Personenbezug können aus Datenschutz- und Sicherheitsgründen nicht eingesehen werden.</p>
1.9 Wie ist das System vor Fremdangriffen geschützt?	<ul style="list-style-type: none"> <li>• Gemäß Best Practices</li> <li>• Secure Development Lifecycle</li> <li>• Secure Operations</li> <li>• Unabhängige Überprüfung</li> </ul>
1.10 Gibt es eine Passwortrichtlinie?	<p>Der Benutzer darf sein Passwort selbst vergeben und ändern</p> <p>Das Kennwort muss mindestens 8 Zeichen lang sein, Groß- und Kleinbuchstaben enthalten, mindestens eine Ziffer und ein Sonderzeichen enthalten. Das Passwort darf nicht mit Leerzeichen anfangen und enden.</p>

## 1. Allgemeines

1.11 Kann sichergestellt werden, dass Daten nicht außerhalb einer geographisch-definierten Region migrieren?	Ja. Alle personenbezogenen Daten verbleiben in Europa.
1.12 Haben Administratoren oder Supportmitarbeiter Einblick in personenbezogene Daten?	<ul style="list-style-type: none"> <li>Entwickler haben im Notfall (Lizenzprobleme, Login-Probleme) Zugang zu personenbezogenen Daten von Systembenutzern. Dies wird allerdings nur in Absprache mit dem Kunden durchgeführt.</li> <li>Auf Testsystemen werden keine Echtzeiten verwendet.</li> <li>Der Haufe-Support hat keinen Zugang</li> </ul>
1.13 Wann werden die personenbezogenen Daten gelöscht?	<ul style="list-style-type: none"> <li>Sie können jederzeit im Programm selbst die Daten löschen.</li> <li>Bei Kündigung haben wir die Daten noch 30 Tage für Sie gespeichert, danach werden sämtliche Daten unwiderruflich gelöscht.</li> <li>Datensicherungen werden täglich erstellt und 30 Tage aufbewahrt.</li> </ul>
1.14 Wie sind die Daten abgespeichert?	<ul style="list-style-type: none"> <li>Die Daten werden nach Mandanten getrennt abgespeichert. Durch die Steuerung des Zugriffs über Access Tokens wird sichergestellt, dass nur die eigenen Mandanten-Daten geladen werden können.</li> <li>Sämtliche Daten sind verschlüsselt</li> </ul>
1.15 Existiert ein Business Continuity Plan / Disaster Recovery Plan? Wie oft werden diese getestet?	Die Infrastruktur wurde als „Infrastruktur als Code“ definiert; die Produktionsumgebung wird regelmäßig komplett neu provisioniert.
1.16 Existiert ein Notfallkonzept / -Handbuch?	Ja
1.17 Wurde das Unternehmen anlassbezogen durch die zuständige Datenschutz-Aufsichtsbehörde geprüft?	Nein
1.18 Erfolgt die Vertragserfüllung ausschließlich in Liegenschaften und auf Systemen mit Standorten innerhalb der EU? Relevant sind hierbei die eingesetzten Sub-Dienstleister, die im Rahmen der Auftragserfüllung Zugriff auf personenbezogene Daten haben.	Ja
1.19 Erfolgt eine Information des Kunden bei Sicherheits- und Datenschutzvorfällen, welche die Daten des Mandanten betreffen könnten?	Ja, es existiert ein Prozess, welcher eine Information des Kunden bei Datenschutzverletzungen i.S.v. Art. 4 Nr. 12 DSGVO vorsieht.
1.20 Existiert ein Datenschutz- bzw. Sicherheitskonzept für die Anwendung?	Ja, die hier vorliegende Dokumentation zu den technischen und organisatorischen Maßnahmen enthält die Ausführungen zu Datenschutz und Datensicherheit.

## VERTRAULICHKEIT (Art. 32 Abs. 1 lit. b DS-GVO)

### 2. Zutrittskontrolle

Definition: Maßnahmen, die dazu geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

2.1 Existiert ein schriftlich dokumentiertes Zutrittsberechtigungssystem für Mitarbeiter des Unternehmens bzw. nicht zutrittberechtigte Personen (z.B. Geschäftskunden / Besucher, Reinigungsfirmen, Wartungsfirmen etc.)?

Nur autorisiertes AWS-Personal erhält Zugang zu den physischen Rechenzentren. Alle Mitarbeiter, die Zugang zu einem Rechenzentrum benötigen, müssen zunächst einen Antrag auf Zugang stellen und eine gültige geschäftliche Begründung vorlegen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Die Anfrage wird geprüft und von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt.

Der Zugang von Dritten muss von autorisierten AWS-Mitarbeitern beantragt werden, die auch eine gültige geschäftliche Begründung für diesen Zugang vorlegen müssen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Diese Anfragen werden von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt. Personen mit einem Besucherausweis müssen diesen bei Ankunft am Standort vorlegen und werden von autorisiertem Personal angemeldet und begleitet.

2.2 Gibt es einen Sicherheitsdienst? Welche Verantwortungsbereiche / Aufgaben übernimmt dieser?

Der physische Zugang wird durch professionelles Sicherheitspersonal an den Gebäudeeingängen kontrolliert. Dabei werden Überwachung, Meldeanlagen und andere elektronische Vorrichtungen eingesetzt. Autorisiertes Personal erlangt über Multi-Faktor-Authentifizierungsmechanismen Zugang zu den Rechenzentren. Die Eingänge zu den Serverräumen sind mit Geräten abgesichert, die Alarm auslösen, wenn die Tür aufgebrochen oder offengehalten wird.

2.3 Findet eine Videoüberwachung statt? Wie lange werden die Videos gespeichert?

Physische Zugangspunkte zu Serverräumen werden von CCTV-Kameras mit Aufzeichnungsfunktion überwacht. Die Aufnahmen werden gemäß behördlichen und Compliance-Anforderungen aufbewahrt.

## VERTRAULICHKEIT (Art. 32 Abs. 1 lit. b DS-GVO)

### 2. Zutrittskontrolle

Definition: Maßnahmen, die dazu geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

<p>2.4 Gibt es ein Alarmsystem? Wer wird über dieses alarmiert?</p>	<p>In der Datenebene sind elektronische Einbruchmeldesysteme installiert, die sicherheitsrelevante Ereignisse erkennen und automatisch die zuständigen Mitarbeiter alarmieren. Die Ein- und Ausgänge zu den Serverräumen sind mit Geräten gesichert, die von jeder Person eine Multi-Faktor-Authentifizierung verlangen, bevor sie Zutritt erhält, und einen Ausweis, bevor sie den Raum verlässt. Diese Geräte lösen einen Alarm aus, wenn die Tür ohne Authentifizierung gewaltsam geöffnet, offengehalten oder während eines Notfalls zum Verlassen der Wohnung geöffnet wird. Türalarmanlagen sind auch so konfiguriert, dass sie Situationen erkennen, in denen eine Person eine Datenebene ohne Multi-Faktor-Authentifizierung betritt oder ohne ordnungsgemäßes Badging verlässt. In diesem Fall wird umgehend ein Alarm ausgelöst und an die AWS Security Operations Center zur Protokollierung, Analyse und Reaktion gesendet.</p>
---	---

### 3. Zugangskontrolle

Definition: Maßnahmen, die dazu geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

<p>3.1 Gibt es Regelungen zu Vergabe, Entzug und zyklischen Reviews (auf die Notwendigkeit) von Zugangsberechtigungen?</p>	<p>Entsprechendes wird über den Starter-Changer-Leaver-Prozess realisiert. Weiterhin finden zyklische Reviews auf die Notwendigkeit der Berechtigungen statt. Diese finden mindestens einmal pro Jahr statt.</p>
<p>3.2 Werden sämtliche Berechtigungen lediglich auf Basis der minimalen Rechte (Need-to-Know) vergeben?</p>	<p>Es werden für die einzelnen Ebenen unterschiedliche Teams eingesetzt, die lediglich Zugriff auf die von diesen Mitarbeitern verantworteten Komponenten haben.</p>
<p>3.3 Existieren Maßnahmen zum Schutz von Passwortdateien und Passwörtern auf der Applikationsebene?</p>	<p>Die Passwörter werden mittels bcrypt gespeichert.</p>
<p>3.4 Gibt es eine Begrenzung der Anmeldeversuche bei wiederholten Fehlversuchen (Anzahl / Konfigurierbarkeit)?</p>	<p>Auf Applikationsebene können maximal 5 Anmeldeversuche pro Minute durchgeführt werden.</p>
<p>3.5 Wie erfolgt der Zugriff im Rahmen z.B. von Telearbeit / Homeoffice bzw. mobile Computing? Welche Vorgaben existieren?</p>	<p>Telearbeit ist lediglich unter Verwendung eines VPNs mit einer Zwei-Faktor-Authentifizierung (Zertifikat in Kombination von einem Benutzernamen und Passwort) möglich. Die Dateisysteme der Notebooks sind verschlüsselt.</p>
<p>3.6 Existieren Regelungen bei Verlassen des Arbeitsplatzes (z.B. Sperren des Rechners)?</p>	<p>Die Rechner werden automatisch nach 15 Minuten Inaktivität gesperrt.</p>
<p>3.7 Werden Intrusion Detection / Prevention Systeme eingesetzt?</p>	<p>Ja.</p>

### 3. Zugangskontrolle

Definition: Maßnahmen, die dazu geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

3.8 Wird ein Virens Scanner auf allen Server-Systemen eingesetzt? Wenn ja, in welchem Intervall werden die Signaturen geupdated?	Für Daten innerhalb der Anwendung wird ein Clam-AV eingesetzt. Dieser wird einmal täglich mit den neusten Anti-Viren-Signaturen versehen.
3.9 Existieren Regelungen zum Einsatz lokaler Administrationsrechte?	Es werden keine lokalen Admin-Rechte vergeben.

### 4. Zugriffskontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

4.1 Existiert ein Berechtigungskonzept für die Applikation zur bedarfsorientierten Ausgestaltung der Zugriffsrechte (differenzierte Berechtigungen für Profile, Rollen, Transaktionen und Objekte)?	Derzeit ist kein Rollen-/Rechte-System vorhanden.
4.2 Einsatz von Verschlüsselungstechnik bei Notebooks?	Ja, eine Festplattenverschlüsselung wird eingesetzt. Diesbezüglich kommen unterschiedliche Lösungen wie z.B. Truecrypt, Bitlocker oder die Festplattenverschlüsselung von Apple zum Einsatz.

### 5. Trennungskontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

5.1 Wie und wo erfolgt die Trennung der Daten von Daten anderer Kunden / Mandanten (z.B. physisch getrennte Server-Systeme je Kunden)?	Die Daten verschiedener Kunden liegen in einer zentralen Datenbank; getrennt / separiert über die Mandantennummer.
5.2 Erfolgt eine logische und physikalische Trennung der Produktions-, Integrations- und Entwicklungssysteme voneinander?	Neben der produktiven Umgebung existiert eine Staging-Umgebung für Tests sowie Entwicklungsumgebungen.
5.3 Werden produktive Daten des Mandanten auf anderen Systemen als dem Produktivsystem (z.B. Verwendung der Echt Daten auf den Testsystemen zu Testzwecken) gespeichert?	Auf den Testsystemen (Staging) werden nur anonymisierte Daten verwendet, bei denen sämtliche schützenswerten personenbezogene Daten anonymisiert sind.

### 6. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Definition: Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Wie werden sensible personenbezogene Daten in der Applikation pseudonymisiert?	<p>Eine Verschlüsselung personenbezogener Daten erfolgt</p> <ul style="list-style-type: none"> <li>sowohl bei der Übermittlung (https)</li> <li>als auch bei der Speicherung durch die Verschlüsselung der Datenbank</li> </ul>
--	---

## INTEGRITÄT (Art. 32 Abs. 1 lit. b DS-GVO)

### 7. Weitergabekontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

7.1 Ist der Zugriff auf die Applikation lediglich verschlüsselt möglich?

Ja, wir unterstützen TLS 1.2 und TLS 1.3 unter Verwendung von RSA 4096 bits.

7.2 Werden vertrauliche sowie personenbezogene Daten innerhalb gesicherter Netzwerke (Firmennetzwerk) verschlüsselt übertragen?

Ja, zur Datenbank mittels TLS.

7.3 Werden Datenträger (z.B. Backups) an eine zusätzliche Lokalität (z.B. Katastrophenarchiv, Tresor, Bankschließfach) transportiert?

Nein, es erfolgt keine Sicherung außerhalb der AWS Rechenzentren (EU-centraol-1).

### 8. Eingabekontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

8.1 Was wird auf Datenbankebene (Transaktionsprotokoll / Audit-Log der Datenbank) protokolliert? Bitte entsprechende Log-Kategorien inklusive Log-Inhalte je Kategorie nennen. Wie lange werden diese Log-Daten aufbewahrt?

Es werden Transaktionsprotokolle erstellt, welche auf Stundenbasis als Backup verwendet werden. Aus diesen können Veränderungen an Inhalten entsprechend rekonstruiert werden. Diese Daten werden für 90 Tage gespeichert.

8.2 Wird sichergestellt, dass die Protokolldaten nicht verändert werden können?

Ja, durch die Übertragung der Protokolldaten an einen zentralen Server.

## VERFÜGBARKEIT UND BELASTBARKEIT (Art. 32 Abs. 1 lit. b DS-GVO)

### 9. Verfügbarkeitskontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

9.1 Existiert ein Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung (Notfallplan)?

Ja; gem. ISO 22301.

9.2 Werden zwei unabhängige Rechenzentren mit ausreichend Geo-Redundanz verwendet (zwei unterschiedliche Risikoumgebungen)?

Die Infrastruktur wird redundant über Rechenzentren verteilt, dementsprechend ist der Service auch bei Komplettausfall eines Rechenzentrums weiterhin verfügbar.

9.3 Existieren Tests und Freigabeverfahren (z.B. nach Patches, neuen Releases etc.)? Wenn ja, wie sehen diese aus?

Die Prozesse orientieren sich diesbezüglich an der IT Infrastructure Library (ITIL).

## Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

### VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

#### 10. Auftragskontrolle

Definition: Maßnahmen, die dazu geeignet sind, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

10.1 Welche Subauftragnehmer / Dienstleister haben Zugriff auf Daten des Auftraggebers?

Aufgrund der Verschlüsselung der Daten hat nur Haufe Zugriff auf die Daten. Unterauftragsverarbeiter haben keinen Zugriff.

10.2 Welche Subauftragnehmer außerhalb der EU haben Zugriff auf personenbezogene Daten des Auftraggebers?

Keine.

10.3 Liegt mit Subunternehmern ein schriftlicher Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO, ein NDA, eine Verpflichtung zur Vertraulichkeit vor?

Mit dem oben genannten Dienstleister besteht ein Vertrag gem. Art. 28 DSGVO; die Mitarbeiter, die Zugriff auf Daten des Auftraggebers haben, sind auf das Datengeheimnis / Vertraulichkeit verpflichtet.

10.4 Ist eine Kontrolle der technischen und organisatorischen Maßnahmen bei vorheriger Anmeldung und Terminabstimmung vor Ort beim Subunternehmer möglich?

Nein.

10.5 Wie oft wird eine Kontrolle der technischen und organisatorischen Maßnahmen beim Subunternehmer durchgeführt?

Es erfolgen Kontrollen durch den Datenschutzbeauftragten bei den oben genannten Dienstleistern. Diese Prüfung erfolgt einmal jährlich.

10.6 Erfolgt bei Fehlern hinsichtlich der Datenverarbeitung oder Verstoß gegen den Datenschutz sowie IT-Sicherheitsvorfällen eine unverzügliche Information an den Auftraggeber? Wer erhält diese Information?

Ja, die Information erfolgt an die im Vertrag mit dem Auftraggeber benannte Stelle.

Freiburg, den 17.09.2025