

Auftragsbearbeitungsvereinbarung (AVV)

zwischen

dem Kunden der POOLARSERVER Schweiz GmbH

als datenschutzrechtlich Verantwortlichem

- nachstehend „**Auftraggeber**“ genannt –

und der

Poolarserver Schweiz GmbH
Platz 10
6039 Root D4
Schweiz

als Auftragsbearbeiter

- nachstehend „**Auftragnehmer**“ genannt.

1. Anwendungsbereich der AVV und Vertragsdauer

Diese Auftragsbearbeitungsvereinbarung („**Vereinbarung**“ oder „**AVV**“) findet Anwendung auf die Bearbeitung von Personendaten durch den Auftragnehmer – im Auftrag des Auftraggebers (dem datenschutzrechtlich Verantwortlichen) – bei der Erbringung der vertraglichen Leistungen gemäss dem zwischen Auftraggeber und Auftragnehmer abgeschlossenen Beauftragung über Softwareleistungen; die Bearbeitung von Personendaten bei der Erbringung der vertraglichen Leistungen auch: „**AV-Leistungen**“).

Die Laufzeit der Vereinbarung entspricht der Laufzeit der Beauftragung. Sofern der Auftragsbearbeiter auch nach dem formalen Ende des Auftrags Personendaten bearbeitet (etwa beim Vorhalt von Daten zum Abruf oder bei sonstigen Tätigkeiten zum Dienstleister-Wechsel), endet die Laufzeit dieser Vereinbarung erst mit dem Abschluss der Erbringung dieser ergänzenden Leistungen/Tätigkeiten und der vollständigen Löschung oder Rückgabe der Personendaten an den Auftraggeber nach Abschluss der Erbringung der Bearbeitungsleistungen gemäss Abschnitt 6 dieser Vereinbarung.

2. Gegenstand der Bearbeitung

Der Gegenstand dieser Vereinbarung ergibt sich aus der Beauftragung eines oder mehrerer Projekträume und gilt auch für Folgeaufträge sowie für Tochterunternehmen / Tochtergesellschaften des Auftraggebers.

3. Dauer der Bearbeitung

Die Dauer der Bearbeitung ist durch die Dauer der Erbringung der AV-Leistungen bestimmt.

4. Zweck der vorgesehenen Bearbeitung von Daten

4.1 Die Bearbeitung dient dem Zweck der Erbringung der AV-Leistungen, namentlich:

- der Bereitstellung von Software im Wege des Software-as-a-Service;
- der Bereitstellung von Support- und Wartungsleistungen hinsichtlich der SaaS-Leistungen;
- der Einrichtung und Anpassung der SaaS-Leistungen an die Anforderungen und Bedürfnisse des Auftraggebers;
- der Schulung und Fortbildung von Nutzern der SaaS-Leistungen („Schulungsleistungen“).

4.2 Soweit der Auftragnehmer Personendaten bearbeitet, um den Auftraggeber dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person nachzukommen (Abschnitt 3.4 dieser Vereinbarung) bzw. die Verpflichtungen im Zusammenhang mit der Datensicherheit sowie Datenschutz-Folgeabschätzungen einzuhalten, dient die Bearbeitung ausserdem dem Zweck der Unterstützung des Auftraggebers bei der Erfüllung seiner rechtlichen Verpflichtungen.

5. Art der Bearbeitung

Die Art der Bearbeitung sind alle für die Erbringung der AV-Leistungen und/oder der Pflichten (insbesondere zur Unterstützung nach Abschnitten 3.4 und 4.5 dieser Vereinbarung sowie zur Löschung nach Abschnitt 6 dieser Vereinbarung) unter dieser Vereinbarung erforderlichen Arten der Bearbeitung, wie etwa die Erhebung, Speicherung, Anpassung, Verwendung, Verknüpfung und/oder Löschung.

6. Arten von Personendaten

Folgende Arten von Personendaten werden bearbeitet:

- Stammdaten, Kontaktdaten
- Benutzeraktivitäten (z. B. Up-/Downloads), Auswertungen
- Backups
- Angebote, Aufträge, Abrechnungen
- Bankverbindungsdaten, Finanzdaten

7. Kategorien betroffener Personen

Gegenstand der Bearbeitung von Personendaten sind Personen der folgenden Kategorien:

- Mitarbeiter des Auftraggebers und Mitarbeiter von Dienstleistern des Auftraggebers
- Vertragspartner des Auftraggebers und ihre Mitarbeiter
- weitere im Rahmen der Projektdurchführung betroffene/beteiligte Personen, denen der Auftraggeber Zugang zu den AV-Leistungen gewährt
- Bewerber des Auftraggebers und der mit ihm verbundenen Unternehmen (nur bei Nutzung des Bewerbungsmoduls)

8. Pflichten des Auftragnehmers

8.1 Bearbeitung auf dokumentierte Weisung des Auftraggebers

- 8.1.1 Der Auftragnehmer bearbeitet die Personendaten, die Gegenstand dieser Vereinbarung sind, nur auf dokumentierte Weisung des Auftraggebers auch in Bezug auf die Übermittlung von Personendaten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Schweiz oder (soweit anwendbar) der Europäischen Union, dem der Auftragnehmer unterliegt, zur Bearbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Bearbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- 8.1.2 Erteilte Weisungen des Auftraggebers sind durch den Auftragnehmer zu dokumentieren. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens Textform).
- 8.1.3 Der Auftragnehmer hat den Auftraggeber auch unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Datenschutzvorschriften der Schweiz oder (soweit anwendbar) der Europäischen Union. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.
- 8.1.4 Weisungen, die über die vertraglichen Vereinbarungen hinausgehen und nicht erforderlich sind, um Rechtsverstösse im Zuständigkeitsbereich des AN zu verhindern bzw. abzustellen, können vom Auftragnehmer mit angemessener Vergütung in Rechnung gestellt werden.
- 8.1.5 Die Parteien werden sich die jeweiligen Ansprechpartner und deren Kontaktdaten zur Erteilung und zum Empfang von Weisungen pro Projektvereinbarung textlich mitteilen. Die Parteien werden sich unverzüglich über Änderungen dieser Ansprechpartner informieren.

8.2 Vertraulichkeit der Personen, die zur Bearbeitung der Personendaten berechtigt sind

Der Auftragnehmer gewährleistet, dass sich die zur Bearbeitung der Personendaten, die Gegenstand dieser Vereinbarung sind, befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

8.3 Technische und organisatorische Massnahmen

- 8.3.1 Der Auftragnehmer ergreift angemessene technische und organisatorische Massnahmen zum Schutz der Personendaten. Dabei sind der Stand der Technik, die Art und der Umfang, die Umstände und die Zwecke der Datenbearbeitung, das Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, und (soweit zulässig) die Implementierungskosten zu berücksichtigen. Die konkreten vom Auftragnehmer zu ergreifenden Massnahmen sind in Anlage 1 dieser Vereinbarung festgelegt.

- 8.3.2 Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer informiert den Auftraggeber über etwaige Änderungen der technischen und organisatorischen Massnahmen.

8.4 **Unterstützung des Auftraggebers bei der Erfüllung der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte des Betroffenen**

- 8.4.1 Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Bearbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Massnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Rechten der betroffenen Personen nachzukommen.
- 8.4.2 Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und dessen Weisungen abwarten.

8.5 **Unterstützung des Auftraggebers bei der Einhaltung der Pflichten im Zusammenhang mit der Datensicherheit sowie Datenschutz-Folgeabschätzungen**

- 8.5.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Bearbeitung sowie der ihm zur Verfügung stehenden Informationen bei der Einhaltung Pflichten im Zusammenhang mit der Datensicherheit sowie Datenschutz-Folgeabschätzungen.
- 8.5.2 Für Unterstützungsleistungen, die über das gesetzlich geforderte Mass hinausgehen, nicht in der Leistungsbeschreibung enthalten sind und nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

9. **Unterauftragsverhältnisse**

- 9.1 Die vertraglich vereinbarten Leistungen bzw. Teilleistungen werden unter Einschaltung der in Anlage 2 genannten Unterauftragnehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Unterauftragnehmern befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Unterauftragnehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
- 9.2 Der Auftragnehmer wird Unterauftragnehmern im Wesentlichen gleichwertige vertragliche Pflichten gegenüber den Pflichten, die sich für den Auftragnehmer aus dieser Vereinbarung ergeben, auferlegen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Massnahmen so durchgeführt werden, dass die Bearbeitung datenschutzkon-

form erfolgt. Der Auftragnehmer stellt sicher, dass der Unterauftragnehmer alle Pflichten erfüllt, denen der Auftragnehmer aus dieser Vereinbarung und den anwendbaren Datenschutzbestimmungen unterliegt.

- 9.3 Kommt der weitere Auftragsbearbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragsbearbeiters.
- 9.4 Ein Einspruch des Auftraggebers gegen eine beabsichtigte Änderung hinsichtlich der Hinzuziehung oder der Ersetzung von Unterauftragsbearbeitern ist nur zulässig, wenn dem Auftragnehmer ein sachlicher Grund nachgewiesen wird.
- 9.5 Der Auftraggeber kann nur innerhalb einer angemessenen Frist (normalerweise zwei [2] Wochen), nachdem er vom Auftragnehmer über die Änderung informiert wurde, aus sachlichem Grund Einspruch einlegen.

Trifft der sachliche Grund zu, liegt es im Ermessen des Auftragnehmers, die Bearbeitung ohne die geplante Änderung selbst oder über einen vom Auftragnehmer mit der Genehmigung des Auftraggebers beauftragten anderen Unterauftragsbearbeiter weiterzuführen oder alle Massnahmen zu ergreifen, um den vom Auftraggeber geltend gemachten Einspruchsgrund zu beseitigen, den Auftraggeber darüber zu informieren und erneut ein entsprechendes Einspruchsrecht einzuräumen sowie die Bearbeitung mit der geplanten Änderung fortzusetzen, wenn entweder (i) die neue Einspruchsfrist ohne einen erneuten Einspruch des Auftraggebers abgelaufen ist oder (ii) der Auftragnehmer lediglich die vom Auftraggeber vorgeschlagenen Massnahmen umgesetzt hat.

10. Kontrollrechte des Auftraggebers

- 10.1 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der gemäss anwendbaren Datenschutzbestimmungen niedergelegten Pflichten zur Verfügung und ermöglicht und trägt zu Überprüfungen – einschliesslich Inspektionen – bei, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden. Zur Erfüllung dieser Informationspflicht kann der Auftragnehmer, ohne Einschränkung seiner Pflichten, auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen vorlegen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- 10.2 Der Auftraggeber informiert den Auftragnehmer rechtzeitig, im Regelfall mindestens zwei (2) Wochen im Voraus, über die Durchführung einer Überprüfung, einschliesslich einer Inspektion. In dringenden, vom Auftraggeber nachzuweisenden und zu begründenden Ausnahmefällen ist der Auftraggeber berechtigt, eine Überprüfung, einschliesslich einer Inspektion, ohne Vorankündigung durchzuführen, wenn anderenfalls der Kontrollzweck gefährdet wäre.
- 10.3 Der Auftraggeber führt Inspektionen während der normalen Geschäftszeiten des Auftragnehmers durch.
- 10.4 Die Überprüfungen dürfen nicht zu einer übermässigen Beeinträchtigung des Geschehensablaufs führen.
- 10.5 Der Auftraggeber darf bei der Auswahl des Prüfers, der die Überprüfung durchführt, keine natürliche oder juristische Person auswählen, die in unmittelbarem Wettbewerbsverhältnis mit dem Auftragnehmer steht.

- 10.6 Der Auftraggeber hat die Betriebs- und Geschäftsgeheimnisse des Auftragnehmers, die dem Auftraggeber während einer Überprüfung – einschliesslich Inspektionen – bekannt werden, streng vertraulich zu behandeln. Der Auftraggeber erstellt keine Aufzeichnungen über diese Informationen, es sei denn, dies ist für die Ausübung seines Prüfungsrechts unbedingt erforderlich.

11. Löschung und Rückgabe von Personendaten

- 11.1 Nach Abschluss der Erbringung der Bearbeitungsleistungen wird der Auftragnehmer alle Personendaten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben und die vorhandenen Kopien löschen, sofern nicht nach dem Recht der Schweiz oder (soweit anwendbar) der Europäischen Union eine Verpflichtung zur Speicherung der Personendaten besteht.

11.1.1 Trifft der Auftraggeber gegenüber dem Auftragnehmer keine ausdrückliche Wahl, werden sämtliche Daten gelöscht.

11.1.2 Die Rückgabe erfolgt durch Zurverfügungstellung einer Archivkopie auf einem Datenträger oder durch Download der Daten durch den Auftraggeber.

12. Bearbeitung in Drittländern

Der Auftragnehmer und etwaige vom Auftragnehmer beauftragte Unterauftragsbearbeiter übermitteln und/oder bearbeiten grundsätzlich keine Personendaten, die Gegenstand dieses AVVs sind, an/in Drittländer(n) ausserhalb Schweiz und Deutschland, es sei denn, der Bundesrat bzw. die Europäische Kommission haben festgestellt, dass dieses Drittland einen angemessenen Schutz von Personendaten gewährleistet, oder es werden genügende Massnahmen getroffen, um einen angemessenen Datenschutz zu gewährleisten.

13. Schlussbestimmungen

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Soweit in dieser Vereinbarung keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrages. Im Fall von Widersprüchen zwischen dieser Vereinbarung und Regelungen aus sonstigen Vereinbarungen zwischen den Parteien, insbesondere aus den Projekträumen, gehen die Regelungen aus dieser Vereinbarung vor.

Schriftlich im Sinne dieser AVV meint mit Nachweis durch Text (d.h. auch in einem elektronischen Format).

Anlage 1: Technische und organisatorische Massnahmen (TOM)

Anlage 2: Unterauftragnehmer

Anlage 2: Technische und organisatorische Massnahmen (TOM)

der Poolarserver Schweiz GmbH

Stand: Oktober 2026

I. Vertraulichkeit

1. Zutrittskontrolle

a) Technische Massnahmen

- Betreffend unsere Büroräume
 - Chipkarten / Transpondersysteme
 - Manuelles Schliesssystem
 - Sicherheitsschlösser
 - Gesicherte Fenster und Zugangstüren, Räumlichkeiten ausschliesslich in oberen Etagen
 - Türen mit Knauf Aussenseite
- Betreffend unsere Produktionsserver bei Unterauftragsbearbeitern zusätzlich
 - elektronisches Zutrittskontrollsystem mit Protokollierung
 - Sicherung des Geländes durch Sicherheitszaun/ Mauer
 - Videoüberwachung an den Ein- und Ausgängen

b) Organisatorische Massnahmen

- Betreffend unsere Büroräume
 - Schlüsselmanagement, dokumentierte Schlüsselvergabe an Mitarbeiter und ggf. externe Arbeiter (z.B. Arbeitnehmerüberlassung)
 - Richtlinien zur Begleitung von Gästen im Gebäude/Besucher stets in Begleitung durch Mitarbeiter
 - Sorgfalt bei Auswahl Reinigungsdienste
 - Definierte Sicherheitszonen mit Berechtigungsregelung verknüpft mit Schlüsselmanagement
- Betreffend unsere Produktionsserver bei Unterauftragsbearbeitern zusätzlich
 - Registrierung, Begleitung durch Mitarbeiter und Kennzeichnung von Gästen

2. Zugangskontrolle

a) technische Massnahmen

- Login mit Benutzername + komplexe Passwörter (strenge Vorgaben zu Länge, Zeicheninhalt etc.)
- 2-Faktor-Authentifizierung
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Firewall
- Zentrale Erfassung von Schadcode-Alarmmeldungen

- Einsatz VPN bei Remote-Zugriffen
- Verschlüsselung von Datenträgern nach Stand der Technik
- Verschlüsselung mobiler Endgeräte nach Stand der Technik
- BitLocker (separates Passwort)
- Automatische Desktopsperre
- Konzept zum Patch-Management: regelmässige und gesteuerte Updates von eingesetzter Software
- Autostart von externen Medien deaktiviert

b) organisatorische Massnahmen

- Rechte- und Rollenkonzepte
- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Passwortrichtlinie
- Löschrichtlinie
- Vorgaben „Clean Desk“
- Allg. Richtlinie Datenschutz und Informationssicherheit
- Mobile Device Policy
- Verpflichtung zur „Manuelle Desktopsperre“, automatische Desktopsperre nach 5 min
- Regelmässige Auswertung von Informationen zu Sicherheitslücken eingesetzter Software
- Diverse Vorkehrungen bei falscher Passworteingabe

3. Zugriffskontrolle

a) technische Massnahmen

- Aktenshredder (mind. Stufe 3, cross cut)
- Physische Löschung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung mobiler Endgeräte nach Stand der Technik
- Verschlüsselung von Datenträgern nach Stand der Technik
- Löschung von Festplatten durch Überschreiben oder Verschlüsselung
- Zerstörung defekter Festplatten oder anderer Datenträger
- Löschung von Datenträgern vor Wiederverwendung
- Verschlüsselung von Messenger-Nachrichten und Dateien
- Transportverschlüsselung (TLS 1.2 oder höher) und Inhaltsverschlüsselung von Personendaten nach Stand der Technik bei hohem Risiko
- Sichere Aufbewahrung von Datenträgern

b) organisatorische Massnahmen

- Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Zentrale Verwaltung Benutzerrechte durch Administratoren
- Passwortrichtlinie
- Kryptographie-Vorgaben

4. Trennungskontrolle

a) technische Massnahmen

- Trennung von Produktiv- und Testumgebung
- physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Klientenfähigkeit relevanter Anwendungen

b) organisatorische Massnahmen

- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten
- Datensätze sind mit Zweckattributen versehen
- Datenträgerkontrolle
- physische und logische Trennung

5. Pseudonymisierung

a) technische Massnahmen

- Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)

b) organisatorische Massnahmen

- Interne Anweisung, Personendaten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

II. Integrität

1. Weitergabekontrolle

a) technische Massnahmen

- E-Mail-Verschlüsselung (und Inhaltsverschlüsselung von Personendaten nach Stand der Technik bei hohem Risiko)
- Einsatz von VPN
- Protokollierung der Zugriffe und Abrufe
- Verschlüsselte Datenübertragung (mind. TLS 1.2, Perfect Forward Secrecy) zwischen Client und Server

b) organisatorische Massnahmen

- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Übersicht regelmässiger Abruf- und Übermittlungsvorgängen
- Sorgfalt bei Auswahl von Dienstleistern (Lieferanten- und Dienstleister-Management)

- Schulung der Mitarbeitenden, Schulungsplan
- Datenschutzhandbuch
- Richtlinien für Mitarbeitende zu Themen E-Mail- und Internet-, Cloudnutzung, IT-Security, Schadsoftware-Erkennung, Verschlüsselung

2. Eingabekontrolle

a) technische Massnahmen

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle und automatisierte Kontrolle der Protokolle

b) organisatorische Massnahmen

- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können (Verfahrensverzeichnis)
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Aufbewahrung von Formularen, von denen Daten in automatisierte Bearbeitungen übernommen wurden
- Klare Zuständigkeiten für Löschungen
- Schulung der Mitarbeiter

III. Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

a) technische Massnahmen

- Betreffend unsere Büro-IT-Systeme
 - Feuer- und Rauchmeldeanlagen
 - Feuerlöscher Serverraum
 - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten
 - Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter)
 - Monitoring aller relevanten Server
 - Einsatz unterbrechungsfreier Stromversorgung
- Betreffend unsere Produktionsserver bei Unterauftragsbearbeitern zusätzlich
 - Dauerhaft aktiver DDoS-Schutz
 - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage

b) organisatorische Massnahmen

- Backup & Recovery-Konzept (ausformuliert) im Rahmen der Business Continuity Planung
- Kontrolle des Sicherungsvorgangs
- Regelmässige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

- Aufbewahrung der Sicherungsmedien an einem sicheren Ort ausserhalb des Serverraums
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums (soweit Server nicht extern)
- Existenz eines Notfallplans
- Getrennte Partitionen für Betriebssysteme und Daten
- Brandschutzkonzept

2. Belastbarkeitskontrolle

a) technische Massnahmen

- ausreichende Belastbarkeit eingerichtet

b) organisatorische Massnahmen

- kontinuierliches Monitoring

IV. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

1. Datenschutz-Management

a) technische Massnahmen

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter
- Sicherheitszertifizierung nach ISO 27001
- Eine Überprüfung der Wirksamkeit der technischen Schutzmassnahmen wird mind. jährlich durchgeführt (vgl. Auditplan)

b) organisatorische Massnahmen

- externer Datenschutzbeauftragter
- Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- Regelmässige Sensibilisierung der Mitarbeiter mindestens jährlich
- externer Informationssicherheits-Beauftragter
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- Die Organisation kommt den datenschutzrechtlichen Informationspflichten nach
- Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

2. Incident-Response-Management

a) technische Massnahmen

- Einsatz von Firewall und regelmässige Aktualisierung
- Einsatz von Spamfilter und regelmässige Aktualisierung
- Einsatz von Virens Scanner und regelmässige Aktualisierung
- Kontinuierliches Monitoring
- Redundante Mail-Dienste
- Geografische Redundanz

b) organisatorische Massnahmen

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
- Dokumentation von Sicherheitsvorfälle und Datenpannen
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

3. datenschutzfreundliche Voreinstellungen

a) technische Massnahmen

- Es werden nicht mehr Personendaten erhoben, als für den jeweiligen Zweck erforderlich sind

b) organisatorische Massnahmen

- Ausführliche Auftragsbearbeitung mit Kunden
- Datenschutzmanagement

4. Auftragskontrolle

a) technische Massnahmen

- Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen

b) organisatorische Massnahmen

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmassnahmen und deren Dokumentation (Risikobewertung)
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsbearbeitung bzw. EU Standard-Vertragsklauseln (mit allenfalls notwendigen Anpassungen und Ergänzungen für die Schweiz)
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis über Vereinbarung mit Auftragnehmer abgesichert
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

- Unsere Mitarbeiter werden in regelmässigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Richtlinien für die Datenbearbeitung

Anlage 2: Unterauftragsverarbeiter im Sinne des AVV

der POOLARSERVER Schweiz GmbH

Stand: Oktober 2026

Unterauftragsverarbeiter für das Hosting der Lösung:

Unterauftragsverarbeiter	Tätigkeiten
Poolarserver GmbH, Heilbronner Str. 74, 70191 Stuttgart, Deutschland	Entwicklung, Betrieb, Wartung und Support der Softwarelösung
Hetzner Online GmbH, Industriestr.25, 91710 Gunzenhausen	Hosting-Leistungen; Erstellung/Speicherung von Backups unserer Systeme
hosttech GmbH, Seestrasse 15a, 8805 Richterswil, Schweiz	Hosting-Leistungen; Erstellung/Speicherung von Backups unserer Systeme
OVH GmbH, Dudweiler Landstraße 5, 66123 Saarbrücken	Erstellung/Speicherung von Backups unserer Systeme
STACKIT GmbH & Co. KG, Stiftesbergstraße 1, 74172 Neckarsulm	Bereitstellung von Infrastrukturressourcen wie Rechenleistung, Speicherplatz, Netzwerkverbindungen und Datenbankdiensten.

Unterauftragsverarbeiter für Supportprozesse:

Unterauftragsverarbeiter	Tätigkeiten
Zendesk Inc., 181 Fremont St, San Francisco, CA 94105, USA.	Bereitstellung eines Ticketsystems zur Bearbeitung von Supportanfragen.

Unterauftragsverarbeiter für optional Funktionen:

Diese Unterauftragsverarbeiter ermöglichen einige unserer innovativen Funktionen, z.B: KI-Unterstützung. Auf Wunsch verzichten wir auf den Einsatz dieser Unterauftragsverarbeiter und deaktivieren diese Funktionen.

Unterauftragsverarbeiter	Tätigkeiten
Functional Software Inc. (Sentry) 45 Fremont Street, 8th Floor San Francisco, CA 94105, USA	Fehleranalyse, Fehlermonitoring und Stabilitätsverbesserung der mobilen App Poolar (Erstveröffentlichung 2026) (Crash-Reporting)

Microsoft Ireland Operations Ltd. One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Bereitstellung von KI-Diensten (Azure OpenAI Services – Verarbeitung in Rechenzentren innerhalb der Europäischen Union), insbesondere Audiotranskription sowie Bild- und Datenanalyse.
--	--