Anlage 1 zum AVV

Technische und organisatorische Maßnahmen (TOM)

AuraServe GmbH | Stand: Oktober 2026 | Rechtsgrundlage: Art. 32 DSGVO

1. Zutrittskontrolle

Wir betreiben keine eigenen physischen Server. Anwendung, Datenbank und Datensicherungen laufen in Rechenzentren der Hetzner Online GmbH in Deutschland (zertifiziert nach ISO/IEC 27001). Lokale Arbeitsgeräte sind durch Zugangssperren und Festplattenverschlüsselung gesichert.

2. Zugangskontrolle

- Passwörter werden ausschließlich als Hash (bcrypt bzw. scrypt) gespeichert, Klartext-Passwörter werden nie gespeichert.
- Für das Mandanten-Portal gilt eine Mindestpasswortlänge von 10 Zeichen.
- Für Verwaltungszugänge steht ein zweiter Anmeldefaktor (Einmalcode per E-Mail) zur Verfügung.
- Sitzungen sind zeitlich begrenzt; Sitzungs-Cookies sind für Skripte nicht lesbar und werden nur verschlüsselt übertragen.
- Anmelde- und ausgewählte Schnittstellen-Endpunkte sind gegen automatisierte Anmeldeversuche durch Ratenbegrenzung geschützt.
- Die gesamte Kommunikation erfolgt ausschließlich über verschlüsselte Verbindungen (HTTPS/TLS).
- Portal und Verwaltung nutzen getrennte Zugangsdaten, Sitzungen und Schnittstellen.
- Administrativer Zugang zu den Servern erfolgt nur schlüsselbasiert über SSH; Passwort-Anmeldungen sind deaktiviert, Anmeldungen werden protokolliert.

3. Zugriffskontrolle

- Nutzer haben ausschließlich Zugriff auf die Daten, die ihrer Rolle und ihrem gebuchten Leistungsumfang entsprechen.
- Zugriffe auf Mandantendaten werden serverseitig auf den jeweiligen Mandanten beschränkt. Mandantenübergreifenden Zugriff haben nur berechtigte Plattform-Administratoren.
- Zentral verwaltete API-Schlüssel der Plattform, OAuth-Zugangstokens für Kalender und Zugangsdaten der API-Bridge-Anbindungen werden verschlüsselt gespeichert (AES-256-GCM).
- Die Datenbank ist nicht öffentlich erreichbar; der Zugriff erfolgt über die Anwendung oder über den verschlüsselten Administrationszugang.
- Im Mandanten-Portal ist die Anzahl der Nutzer begrenzt; neue Nutzer werden nur von berechtigten Personen angelegt.

4. Weitergabekontrolle

- Alle Datenübertragungen erfolgen ausschließlich über verschlüsselte Verbindungen (TLS 1.2 oder höher).
- Ausgehende Webhooks werden mit einer HMAC-Signatur versehen, sofern für das Ziel ein Signaturschlüssel hinterlegt ist; so lassen sich Herkunft und Integrität prüfen.
- Personenbezogene Daten gehen nur an die im AVV (§ 6) genannten Unterauftragsverarbeiter und an vom Verantwortlichen selbst verbundene Dienste.

- Gesprächsaudio wird nicht dauerhaft aufgezeichnet; es wird nur während des Telefonats an die Voice-Anbieter übertragen.
- Daten werden nicht zum Training von KI-Modellen verwendet.

5. Eingabekontrolle

- Anmeldungen an der Verwaltung sowie Änderungen an Unternehmen, Assistenten, Benutzern, Wissensbasis und Systemeinstellungen werden mit Benutzer, Zeitpunkt und IP-Adresse protokolliert und 365 Tage aufbewahrt.
- Alle Eingaben werden serverseitig auf Zulässigkeit geprüft.
- Gespeicherte Gesprächs-, Anruf- und Nachrichtendaten werden nach den in § 10 AVV festgelegten Fristen automatisch gelöscht.

6. Auftragskontrolle

- Unterauftragsverarbeiter werden vertraglich nach Art. 28 Abs. 4 DSGVO auf dieselben Datenschutzpflichten verpflichtet (§ 6 AVV).
- Bei KI-Anbietern wird, soweit verfügbar, die kürzeste angebotene Aufbewahrung und keine Nutzung zu Trainingszwecken konfiguriert.
- Mandanten können ausschließlich Daten ihres eigenen Kontos einsehen und verwalten.

7. Verfügbarkeitskontrolle

- Die Produktivdatenbank wird alle sechs Stunden verschlüsselt (AES-256) in einen separaten Objektspeicher in Deutschland gesichert. Die Sicherungen sind gegen Löschen und Überschreiben gesperrt und werden spätestens nach 90 Tagen entfernt.
- Fehlgeschlagene Datensicherungen lösen eine E-Mail-Benachrichtigung aus.
- Gesprächs-, Anruf- und Kontaktdaten werden dauerhaft ausschließlich in der Datenbank gespeichert; auf dem Anwendungsserver liegen nur Logos und Screenshots aus Fehlerberichten, die mitgesichert werden.

8. Trennungsgebot

- Die Daten unterschiedlicher Mandanten werden logisch getrennt verarbeitet und serverseitig dem jeweiligen Mandanten zugeordnet.
- Portal und Verwaltung nutzen getrennte Zugangsdaten, Sitzungen und Schnittstellen.
- Produktions-, Staging- und Entwicklungsumgebungen sind getrennt. Personenbezogene Gesprächs-, Anruf- und Kontaktdaten werden nicht in Entwicklungsumgebungen kopiert. Die Staging-Umgebung läuft beim selben Hoster in Deutschland ohne öffentlichen Datenbankzugang.
- Ein lesender Zugriff auf Produktionsdaten erfolgt nur zur Fehleranalyse und im erforderlichen Umfang.

9. Pseudonymisierung

- Chat-Sitzungen erhalten zufällig generierte Kennungen ohne Personenbezug.
- Endnutzer des Chat-Widgets können anonym kommunizieren, eine Registrierung ist nicht erforderlich.
- Langfristige Nutzungsstatistiken enthalten nur Zahlen und Themen, keine Gesprächsinhalte.

10. Weitere Maßnahmen

- Einsatz typsicherer Programmiersprachen; Änderungen werden vor der Auslieferung automatisiert geprüft.

- Sicherheitsrelevante Konfigurationen werden nie im Quellcode hinterlegt.
- Nach Vertragsende werden alle Daten des Verantwortlichen vollständig gelöscht; die Löschung wird schriftlich bestätigt (§ 10 AVV).
- Alle eingesetzten Drittanbieter werden vor dem Einsatz auf DSGVO-Konformität geprüft.

11. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Die Geschäftsführung überprüft die Wirksamkeit dieser Maßnahmen mindestens einmal jährlich sowie bei wesentlichen Änderungen an Infrastruktur, Hosting, Unterauftragsverarbeitern oder Funktionen.
- Das Ergebnis der Überprüfung wird dokumentiert; dieses Dokument wird bei Bedarf aktualisiert. Der aktuelle Stand ist in der Kopfzeile angegeben.