Anhang 4: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Alveon GmbH · Stand 19.11.2026

Stand 19.11.2026, Fassung 2. Ersetzt den Kurzüberblick in Ziffer 4 des Auftragsverarbeitungsvertrags nicht, sondern führt ihn aus.

Wie dieses Dokument zu lesen ist

Jede Maßnahme trägt einen Stand: **umgesetzt** heißt, sie ist in Betrieb und am angegebenen Ort nachprüfbar. **In Umsetzung** heißt, sie ist beschlossen und hat ein Zieldatum. Wir führen offene Punkte bewusst auf, statt sie wegzulassen: Eine Liste, die nur Erledigtes nennt, sagt einem Prüfer nichts darüber, wie ernst sie gemeint ist.

Schichtenmodell. Alveon betreibt die Anwendung (Cockpit, Worker, Sprachagent, Datenbank). Rechenzentrum, Strom, Zutritt und Hardware liegen bei der Hetzner Online GmbH (Rechenzentrum Falkenstein, Deutschland, ISO/IEC 27001 zertifiziert). Für diese Schicht verweisen wir auf die TOM von Hetzner (`nachweise/quellen/hetzner-tom.html`). Für die Dienste in Anhang 2 gelten deren eigene Maßnahmen, die wir bei Auswahl und jährlich prüfen.

1. Vertraulichkeit

1.1 Zutrittskontrolle

MASSNAHME	STAND
Rechenzentrum: Zutritt nur für berechtigtes Personal von Hetzner, elektronische Zutrittskontrolle, Videoüberwachung, 24/7-Sicherheitsdienst (Hetzner-TOM)	umgesetzt (Hetzner)
Alveon betreibt keine eigenen Server und hat keinen physischen Zugang zum Rechenzentrum	umgesetzt

Arbeitsplätze: Bildschirmsperre, verschlüsselte Datenträger der Arbeitsgeräte, keine Ausdrucke personenbezogener Daten (schriftliche Richtlinie)	in Umsetzung, bis 30.11.2026

1.2 Zugangskontrolle (Systeme)

MASSNAHME	STAND
Server-Zugang ausschließlich per SSH-Schlüssel für das Administratorkonto; Anmeldung als Administrator mit Passwort ist gesperrt	umgesetzt
Passwort-Anmeldung per SSH für alle Konten abschalten	mit dem Umzug auf die neue Infrastruktur, spätestens 31.03.2027
Host-Firewall mit Standard „verweigern“, nur Web (80/443) und SSH offen; Schutz gegen wiederholte Fehlanmeldung (fail2ban)	umgesetzt
Verwaltungsoberflächen (Proxy-Verwaltung, Container-Verwaltung) nur über das interne VPN erreichbar, nicht aus dem Internet	in Umsetzung, bis 24.11.2026
Interne Dienste ausschließlich über den TLS-Proxy erreichbar, keine direkt veröffentlichten Ports (die Dienste von alesio sind bereits nur über den Proxy erreichbar)	für alesio umgesetzt; übrige Dienste mit dem Umzug, spätestens 31.03.2027
Datenbank nur im internen Container-Netz und über VPN erreichbar, kein öffentlicher Port	umgesetzt
Automatische Sicherheitsupdates des Betriebssystems (unattended-upgrades)	umgesetzt

1.3 Zugangskontrolle (Anwendung, Cockpit)

MASSNAHME	STAND

Persönliche Konten je Person, keine geteilten Zugänge; Einladung per signiertem, zeitlich begrenztem Link (7 Tage), das Passwort setzt die Person selbst	umgesetzt
Passwörter nur als scrypt-Hash mit Salt gespeichert, Vergleich zeitkonstant, Mindestlänge 8 Zeichen	umgesetzt
Sitzungs-Cookie httpOnly, secure, SameSite; Sitzungen serverseitig widerrufbar (alle Anmeldungen vor einem Zeitpunkt werden ungültig)	umgesetzt
Erkennung von Auslese-Versuchen (Rate-Begrenzung je Sitzung, Alarm, Abmeldung)	umgesetzt
Zwei-Faktor-Anmeldung für alle Konten mit Zugriff auf Gesprächsdaten	in Umsetzung, bis 31.12.2026
Sitzungsdauer von 30 auf 12 Stunden verkürzen	in Umsetzung, bis 31.12.2026
Zwei-Faktor-Anmeldung für alle Verwaltungskonten bei Unterauftragsverarbeitern (LiveKit, AssemblyAI, Groq, ElevenLabs, Twilio, AWS, Hetzner)	in Umsetzung, bis 30.11.2026

1.4 Zugriffskontrolle

MASSNAHME	STAND
Rollen im Cockpit: Büroleitung (Verwaltung, Benutzer, Verträge) und Makler (Arbeit mit Interessenten)	umgesetzt
Zugriff auf Produktivsysteme nur durch die Geschäftsführer der Alveon GmbH, namentlich benannt auf Anfrage	umgesetzt

Supportzugriff von Alveon auf das Cockpit eines Kunden nur auf dessen Anfrage oder zur Störungsbehebung; jeder Zugriff wird protokolliert (wer, wann, welcher Mandant)	Protokoll in Umsetzung, bis 31.12.2026
Datenbankzugriff der Anwendung über eine eigene Rolle ohne Administratorrechte, damit die Mandantentrennung (1.6) auch bei einem Programmfehler greift	umgesetzt
Jeder Dienst erhält nur die Zugangsschlüssel, die er braucht (Trennung der Schlüssel je Container)	mit dem Umzug auf die neue Infrastruktur, spätestens 31.03.2027

1.5 Pseudonymisierung und Verschlüsselung

MASSNAHME	STAND
Transportverschlüsselung TLS 1.2 oder höher für alle Verbindungen zwischen Nutzer, Anwendung und Unterauftragsverarbeitern; Spracherkennung TLS 1.3	umgesetzt
Zugangsdaten zum CRM des Kunden mit AES-256-GCM verschlüsselt, Schlüssel getrennt vom Datenbestand	umgesetzt
Keine Tonaufnahme der Gespräche; die Stimme wird nur flüchtig in Text umgewandelt	umgesetzt
Aufzeichnung beim Medienvermittler (LiveKit) im Projekt abgeschaltet und zusätzlich im Programmcode ausgeschlossen	Projekt umgesetzt 19.11.2026, Code in Umsetzung bis 24.11.2026
Protokolle der Anwendung enthalten keine Gesprächsinhalte (nur Länge und Wortzahl), Rufnummern gekürzt	umgesetzt

Verschlüsselung aller Datensicherungen, bevor sie den Server verlassen (siehe 3.2)	teilweise umgesetzt, vollständig bis 24.11.2026
Verschlüsselung der Datenträger der Server	geprüft für die neue Infrastruktur

1.6 Trennungskontrolle (Mandantentrennung)

MASSNAHME	STAND
Jede fachliche Zeile trägt die Kennung des Kunden. Zugriff nur über eine Schicht, die den Kunden je Transaktion setzt, **und** Row-Level-Security der Datenbank (aktiviert und erzwungen). Ohne gesetzten Kunden liefert jede Abfrage null Zeilen	umgesetzt
Automatisierter Test, der die Trennung bei jeder Änderung prüft	umgesetzt
Zugang zum CRM des Kunden je Kunde getrennt (eigene Sitzung je Kunde, nie geteilt) und auf freigegebene Objekte beschränkt	umgesetzt
Getrennte Datenbanken für Produktion und Entwicklung; Testdaten sind erfunden	umgesetzt
Vorführumgebung (demo.app.alesio.at) als eigener Mandant mit erfundenen Daten; dort kann sich nur das Vorführkonto anmelden	umgesetzt

2. Integrität

2.1 Weitergabekontrolle

MASSNAHME	STAND

Weitergabe nur an die Unterauftragsverarbeiter in Anhang 2, verschlüsselt	umgesetzt
Kein Training mit Kundendaten, bei allen KI-Diensten vertraglich und in der Kontoeinstellung ausgeschlossen (Belege in Anhang 2)	umgesetzt
Keine Speicherung bei Sprachmodell und Spracherkennung (Zero Data Retention bei Groq und AssemblyAI)	umgesetzt 19.11.2026
Keine Datenträger, keine Exporte per E-Mail; Exporte nur durch den Kunden im Cockpit	umgesetzt
Interner Tagesbericht an Alveon enthält keine Gesprächsinhalte mehr	in Umsetzung, bis 24.11.2026

2.2 Eingabekontrolle

MASSNAHME	STAND
Jede Schreiboperation in das CRM des Kunden (Besichtigung angelegt oder abgesagt, Status gesetzt) wird mit Zeitpunkt, Objekt und Ergebnis protokolliert, ohne Geheimnisse	umgesetzt
Vertragsbestätigungen werden mit Fassung, Prüfsumme, Zeitpunkt und Person unveränderlich protokolliert	umgesetzt
Je Anruf werden Leitfaden-Fassung, Programmstand und eingesetzte Modelle gespeichert; damit ist nachvollziehbar, womit ein Gespräch geführt wurde	umgesetzt
Protokoll der Lesezugriffe auf Gesprächsinhalte	in Umsetzung, bis 31.12.2026

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

MASSNAHME	STAND
Rechenzentrum mit redundanter Strom- und Netzversorgung (Hetzner)	umgesetzt (Hetzner)
Container starten nach Ausfall automatisch neu; Aktualisierungen des Sprachagenten warten, bis kein Gespräch läuft	umgesetzt
Ersatzmodell und Ersatzstimme beim selben Anbieter, falls der Hauptdienst nicht antwortet	in Umsetzung, bis 24.11.2026
Begrenzung der Protokollgröße, damit kein Dienst durch volle Platten ausfällt	umgesetzt

3.2 Datensicherung und Wiederherstellung

MASSNAHME	STAND
Tägliche Sicherung aller Datenbanken und Datenvolumen (03:30 Uhr)	umgesetzt
Sicherungen an mehreren Orten außerhalb des Produktivservers: Hetzner Object Storage (Deutschland) und Amazon Web Services (Frankfurt, gegen Löschen gesperrt zum Schutz vor Manipulation und Erpressungssoftware)	umgesetzt
Jede ausgelagerte Sicherung wird vor dem Verlassen des Servers mit age verschlüsselt; der Schlüssel liegt nicht beim Speicheranbieter	teilweise umgesetzt, vollständig bis 24.11.2026
Datenbankspiegelung zum Bereitschaftsserver über einen verschlüsselten WireGuard-Tunnel	umgesetzt

Bereitschaftsserver (Standby) und getrennter Überwachungsserver	umgesetzt
Unverschlüsselte Zwischenkopien auf dem Produktivserver entfallen	mit dem Umzug auf die neue Infrastruktur, spätestens 31.03.2027
Wiederherstellungstest mindestens vierteljährlich, Ergebnis dokumentiert	in Umsetzung, erster dokumentierter Test bis 31.12.2026
Wiederanlaufziel (RTO) 8 Stunden, maximaler Datenverlust (RPO) 24 Stunden	Zielwerte, mit dem ersten Test bestätigt

4. Löschung und Datenminimierung

MASSNAHME	STAND
Transkript eines Gesprächs: automatisch nach 90 Tagen gelöscht (stündlicher Lauf, nicht abschaltbar)	umgesetzt
Gesprächszeile mit Zusammenfassung und Verbindungsdaten: automatisch nach 6 Monaten gelöscht	umgesetzt
SMS- und E-Mail-Verläufe: automatisch nach 6 Monaten gelöscht	umgesetzt
Interessenten-Stammdaten: automatisch 6 Monate nach dem letzten Kontakt gelöscht, sofern der Kunde nichts anderes festlegt	in Umsetzung, bis 31.12.2026
Löschen und Auskunft je Person im Cockpit (Art. 15, 17 DSGVO)	in Umsetzung, bis 31.12.2026
Besondere Kategorien (Art. 9): automatische Schwärzung im Transkript vor der Speicherung	in Umsetzung, bis 31.01.2027

Bei den Diensten: AssemblyAI und Groq speichern nichts, Speicherfrist bei AssemblyAI zusätzlich auf 1 Tag begrenzt	umgesetzt 19.11.2026
Sprachausgabe (ElevenLabs): Verlauf wird stündlich automatisch gelöscht, Antworttexte liegen dort höchstens rund 2 Stunden	umgesetzt 19.11.2026
Vertragsende: vollständige Löschung je Kunde, technisch geprüft (automatisierter Test: null Zeilen in jeder Tabelle), schriftliche Bestätigung binnen 14 Tagen	umgesetzt
Datensparsamkeit im Gespräch: der Leitfaden fragt keine besonderen Kategorien, keine Ausweis- oder Bankdaten ab	umgesetzt

5. Organisatorische Maßnahmen

5.1 Auftragskontrolle

MASSNAHME	STAND
Verarbeitung nur auf dokumentierte Weisung (AVV Ziffer 2)	umgesetzt
Auswahl der Unterauftragsverarbeiter nach Sitz, Übermittlungsgrundlage, Trainingsverbot und Speicherdauer; Originalbelege mit Abrufdatum und Prüfsumme	umgesetzt
Jährliche Prüfung der Anbieterzusagen und Zertifizierungen; sofort bei geänderter Rechtslage	umgesetzt

5.2 Personal

MASSNAHME	STAND

Schriftliche Verpflichtung auf Vertraulichkeit und Datengeheimnis (§ 6 DSG) für alle Personen mit Zugriff, auch freie Mitarbeiter	in Umsetzung, bis 30.11.2026
Schulung zu Datenschutz und KI-Kompetenz (Art. 4 KI-Verordnung) bei Eintritt und jährlich	in Umsetzung, Nachweis bis 31.12.2026

5.3 Umgang mit Sicherheitsvorfällen

MASSNAHME	STAND
Meldung an den Kunden binnen 24 Stunden nach Bekanntwerden, mit den Angaben nach Art. 33 Abs. 3 DSGVO	umgesetzt (vertraglich)
Schriftlicher Ablaufplan: erkennen, eindämmen, bewerten, melden, beheben, nachbereiten; jeder Vorfall wird dokumentiert	in Umsetzung, bis 30.11.2026
Sofortmaßnahmen ohne Deployment: Abschalten der Anrufe je Kunde (Kill-Switch), Widerruf aller Sitzungen, Sperre einzelner Konten	umgesetzt

5.4 KI-spezifische Maßnahmen

MASSNAHME	STAND
Offenlegung zu Gesprächsbeginn, dass eine digitale Assistenz anruft und für wen; auf Nachfrage Bestätigung als künstliche Intelligenz (Art. 50 KI-Verordnung); Wortlaut versioniert und je Anruf protokolliert	umgesetzt
Keine Entscheidung durch die KI über die Vergabe einer Wohnung; die Assistenz bereitet vor, der Kunde entscheidet	umgesetzt

Keine biometrische Verarbeitung, keine Emotionserkennung, keine Ableitung von Merkmalen aus der Stimme	umgesetzt
Antworten nur auf Basis der freigegebenen Objektdaten; bei unbekannten Angaben verweist die Assistenz an das Büro statt zu raten	umgesetzt
Wunsch nach einem Menschen wird erkannt und als Rückrufwunsch an das Büro übergeben; Widerspruch gegen weitere Anrufe wirkt sofort (Sperrliste)	umgesetzt
Jede Änderung am Leitfaden wird vor der Auslieferung gegen eine feste Sammlung von Gesprächssituationen geprüft	umgesetzt

6. Überprüfung und Weiterentwicklung

Neue Infrastruktur. Mit dem Start neuer Kundenprojekte zieht alesio auf eigene, dedizierte Server bei Hetzner in Deutschland um, getrennt von anderen Anwendungen. Die mit „mit dem Umzug“ bezeichneten Maßnahmen werden dort von Anfang an umgesetzt.

MASSNAHME	STAND
Überprüfung dieser Anlage mindestens jährlich und bei jeder wesentlichen Änderung; Änderungen teilt Alveon dem Kunden vorab mit	umgesetzt
Externer Penetrationstest der Anwendung	geplant, bis 31.03.2027
Ausrichtung an ISO/IEC 27001 Anhang A (Selbsteinschätzung mit Maßnahmenplan); eine Zertifizierung wird geprüft	in Umsetzung

Änderungshistorie

FASSUNG	DATUM	ÄNDERUNG
1	04.09.2026	Kurzüberblick im AVV Ziffer 4
2	19.11.2026	Vollständige Anlage; LiveKit EU (Frankfurt), Aufzeichnung abgeschaltet; AssemblyAI und Groq ohne Speicherung