VOXR

Technische und Organisatorische Maßnahmen nach Art. 32 DSGVO

Stand: 2026 · Abrufbar unter: voxr.com/tom

Auftragsverarbeitungsvertrag (AVV): voxr.com/avv

0. Nutzung eines externen Rechenzentrums

VOXR nutzt seit 2015 die langjährige Erfahrung und Reputation der Fa. Hetzner GmbH, Gunzenhausen, für den physischen Schutz der Daten- und Informationssicherheit. Es besteht hierzu ein AVV einschließlich TOM nach DSGVO.

Hetzner hat weder Zugriff auf die Event-Daten von VOXR, die Datenbank, die Server-Software noch die Admin-Oberfläche der bei Hetzner stationierten singulären (Dedicated) VOXR-Server.

1. Vertraulichkeit

1.1 Risikominimierung im operativen Betrieb

- Minimierung der erhobenen Datenmenge und Speicherdauer. Über das von der DSGVO geforderte Maß hinaus verpflichtet VOXR seine Nutzer vertraglich zur Löschung persönlicher Daten binnen 10 Tagen nach Event-Ende.
- Alle Daten werden ausschließlich verschlüsselt übertragen (TLS 1.2 / 1.3). Sensible Datenbankfelder werden zusätzlich at-rest verschlüsselt.
- VOXR verhindert die öffentliche Anzeige von persönlichen Daten dort, wo diese gezielt von Event-Teilnehmern eingegeben werden, insbesondere in der Funktion des E-Mail-Collectors.
- VOXR weist Auftraggeber bereits vor Vertragsabschluss auf die rechtlichen Notwendigkeiten bei der Erhebung von persönlichen Daten hin.

1.2 Zutrittskontrolle

Durch Rechenzentrum Hetzner GmbH (für physische Maßnahmen siehe die TOM des Rechenzentrums).

1.3 Zugangskontrolle

Durch Rechenzentrum Hetzner GmbH sowie durch VOXR-interne Maßnahmen: Zwei-Faktor-Authentifizierung für alle administrativen Zugänge; Passwörter nach aktuell empfohlenen Mindeststandards (Mindestlänge, Komplexität, regelmäßige Erneuerung).

1.4 Zugriffskontrolle

- Richtlinie für sichere Passwörter für Server, Datenbank und alle Software-Umgebungen.
- Regelmäßige Sicherheitsupdates des Betriebssystems und aller eingesetzten Softwarekomponenten.
- Verbindliches Berechtigungsvergabeverfahren nach Need-to-know-Prinzip.
- Datenspeicherung ausschließlich auf servereigenen Laufwerken; kein Einsatz externer Wechseldatenträger.

1.5 Trennungskontrolle

- VOXR Event-Daten werden physisch und logisch von VOXR-Kundendaten getrennt gespeichert.
- Daten verschiedener Kunden sind durch separate Datenbankstrukturen logisch voneinander getrennt (Mandantentrennung).
- Die Datensicherung erfolgt ebenfalls logisch getrennt.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

- Alle Mitarbeiter, die mit persönlichen Daten in Berührung kommen, sind i.S.d. Art. 32 Abs. 4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Die Weitergabe von Daten an externe Dienste (insbesondere KI-Dienste) erfolgt ausschließlich auf Basis geeigneter Rechtsgrundlagen (Standardvertragsklauseln gem. Art. 46 DSGVO) und nur mit expliziter Aktivierung durch den Verantwortlichen.

2.2 Eingabekontrolle

Die Kontrolle der Eingabe von Event-Daten, ggf. einschließlich persönlicher Daten, obliegt ausschließlich dem Verantwortlichen. VOXR übernimmt für die Rechtmäßigkeit der Erhebung und/oder Speicherung keine Verantwortung.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- VOXR verfügt über ein automatisches Monitoring des Servers, welcher bei Nicht-Verfügbarkeit sofort die notwendigen Stellen informiert.
- Alle relevanten Daten werden täglich logisch getrennt gesichert. Das Backup wird maximal 30 Tage aufbewahrt und danach vollständig und endgültig gelöscht.
- VOXR-Server werden regelmäßig auf die neusten Betriebs- und Schutzprogramme geprüft und ggf. aktualisiert.
- VOXR-Server laufen im Festplattenspiegelungsbetrieb (RAID).
- Über das Rechenzentrum besteht: unterbrechungsfreie Stromversorgung (USV), Netzersatzanlage, dauerhaft aktiver DDoS-Schutz.
- Es ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist.

4. KI-Dienste und Drittstaaten-Datenübermittlung

VOXR bietet optionale KI-gestützte Funktionen an (z.B. KI-Zusammenfassungen, Event-Chat, maschinelle Übersetzungen). Diese Funktionen nutzen externe Dienste, bei denen Daten außerhalb der EU verarbeitet werden können.

4.1 Eingesetzte KI-Dienste

- OpenAI, L.L.C. (USA): Für KI-Zusammenfassungen und Event-Chat-Funktionen. Rechtsgrundlage für Drittstaatentransfer: Standardvertragsklauseln gem. Art. 46 DSGVO auf Basis des OpenAI Data Processing Agreements (DPA).
- DeepL SE (Deutschland): Für maschinelle Übersetzungen. Verarbeitung innerhalb der EU/des EWR.

4.2 Datenschutzprinzipien für KI-Verarbeitung

- Privacy by Default: Alle KI-Funktionen sind standardmäßig deaktiviert. Eine Verarbeitung durch externe KI-Dienste erfolgt ausschließlich auf ausdrücklichen, freiwilligen Wunsch des Verantwortlichen.
- Datenminimierung: Anfragen an KI-Dienste werden auf das für die jeweilige Funktion notwendige Minimum beschränkt.
- Keine Speicherung zur Modellverbesserung: VOXR nutzt die API-Optionen der Dienste, die eine Speicherung zur Modellverbesserung ausschließen (Zero Data Retention wo verfügbar).
- Transparenz: Der Verantwortliche wird bei Aktivierung einer KI-Funktion über die damit verbundene Datenweitergabe und den Drittstaatentransfer informiert.

5. Verfahren zur regelmäßigen Überprüfung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

5.1 Datenschutz-Managementsystem

Vereintes Datenschutz- und Informationssicherheits-Managementsystem durch Rechenzentrum (für die dort angesiedelten Teile) sowie internes VOXR-Handbuch für Daten- und Informationssicherheitsschutz.

5.2 Incident-Response-Management

Durch Rechenzentrum sowie internes VOXR-Handbuch. Im Falle einer Datenpanne wird der Verantwortliche durch VOXR unverzüglich, spätestens innerhalb von 48 Stunden, benachrichtigt (vgl. AVV §7 Abs. 8).

5.3 Privacy by Design und Privacy by Default

Datenschutzfreundliche Voreinstellungen werden bei der Entwicklung von VOXR berücksichtigt (Art. 25 Abs. 2 DS-GVO). Neue Features werden regelmäßig einem Datenschutz-Folgenabschätzungs-Screening unterzogen.

5.4 Auftragskontrolle

- Mitarbeiter von VOXR werden regelmäßig im Datenschutzrecht unterwiesen.
- VOXR bestellt einen Datenschutzbeauftragten, soweit gesetzlich erforderlich.
- VOXR prüft die bestehenden Datenschutzverträge mit Unterverarbeitern alle zwei Jahre sowie bei Änderungen der gesetzlichen Lage.