VOXR- Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

0. Nutzung eines externen Rechenzentrums

VoxR nutzt seit 2015 die langjährige Erfahrung und Reputation der Fa. Hetzner für den physischen Schutz der Daten- und Informationssicherheit. Es besteht hierzu ein AVV einschl. TOM nach DSGVO.

Hetzner hat weder Zugriff auf die Event-Daten von VOXR, die Datenbank, die Server Software, oder auch nur 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 vereinbart VOXR mit VOXR-Nutzer stets extrem kurze Speicherdauern für persönliche Daten, nämlich maximal 10 Tage.
- VOXR verhindert die öffentliche Anzeige von persönlichen Daten dort, wo diese gezielt von Event-Teilnehmern eingegeben und somit erhoben und gespeichert werden, insbesondere in der Funktion des Email-Collectors (auch Lead-Generator genannt).
- VOXR weist Auftraggeber bereits vor Abschluss des Nutzungsvertrages auf die rechtlichen Notwendigkeiten bei der Absicht der Erhebung von persönlichen Daten, aber auch für den Fall von unabsichtlicher Erhebung und / oder Speicherung hin und regelt die Verantwortlichkeiten im Nutzungsvertrag.

1.2. Zutrittskontrolle wird gewährt durch Rechenzentrum (für diese und weitere TOM siehe die entsprechenden TOM des Rechenzentrums)

1.3. Zugangskontrolle durch Rechenzentrum

1.4. Zugriffskontrolle

- Richtlinie für sichere Passwörter für Server, Datenbank und alle Software-Umgebungen (Mindestlänge, Komplexität der Zeichen und regelmäßige Erneuerung)
- Regelmäßige Sicherheitsupdates
- Verbindliches Berechtigungsvergabeverfahren
- Datenträgerkontrolle durch Rechenzentrum, zusätzliches Health-Status-Monitoring durch VOXR.

1.5. Trennungskontrolle

- VOXR Event-Daten werden physisch und logisch von VOXR Kunden Daten getrennt gespeichert, Ausnahme ist die Email-Adresse des VOXR Administrators, diese wird logisch getrennt von VOXR Event-Daten gespeichert.
- 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.
- Zur weiteren Risiko-Minimierung ist Teil jeden Nutzungsvertrages für die Nutzung von VOXR die Verpflichtung zur Löschung personenbezogener Daten durch den Nutzer binnen 10 Tagen. Die Löschung aus täglichen Backups erfolgt spätestens nach 30 Tagen.

2.2. Eingabekontrolle

- Die Kontrolle der Eingabe von Event-Daten, ggf. einschließlich persönlicher Daten obliegt ausschließlich dem Verantwortlichen. VOXR hat hierauf naturgemäß weder Einfluss noch übernimmt VOXR für die Rechtmäßigkeit der Erhebung und/oder Speicherung irgendeine Verantwortung.

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

- VOXR verfügt über ein automatisches Monitoring des Severs, welcher bei einer eventuellen temporären Nicht-Verfügbarkeit sofort die notwendigen Stellen informiert.
- Alle relevanten Daten werden täglich logisch getrennt gesichert, das Backup wird maximal 30 Tage aufbewahrt. Persönliche Daten dürfen nach 10 Tagen gelöscht werden.
- VOXR Server werden regelmäßig auf die neusten Betriebs- und Schutzprogramme geprüft und ggf. upgedatet.
- VOXR Server laufen im Festplattenspiegelungsbetrieb.
- Über das Rechenzentrum besteht:
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Dauerhaft aktiver DDoS-Schutz.
- Es ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Vereintes Datenschutz-Managementsystem und Informationssicherheits-Managementsystem als DIMS (Datenschutz-Informationssicherheits-Management-System) durch Rechenzentrum (für die dort angesiedelten Teile), sowie internes VOXR Handbuch: Daten- und Informationssicherheitsschutz, sowie Vertragsbestandteile zum Daten- und Informationssicherheits-Management.

4.2. Incident-Response-Management: Durch Rechenzentrum (für die dort angesiedelten Teile), sowie internes VOXR Handbuch: Vorgehen bei Datenschutzvorfällen, drohendem oder festgestelltem Datenverlust.

4.3. Datenschutzfreundliche Voreinstellungen werden bei der Entwicklung von VOXR berücksichtigt (Art. 25 Abs. 2 DS-GVO).

4.4. Auftragskontrolle

- Mitarbeiter von VOXR werden regelmäßigen im Datenschutzrecht unterweisen und sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des jeweiligen Auftraggebers. Gleiches gilt für Unterverarbeiter.
- Das Rechenzentrum hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.
- Auch VOXR bestellt einen Datenschutzbeauftragten, sowie gesetzlich erforderlich.
- Auch weitere Subunternehmern bestellen einen Datenschutzbeauftragten, sowie gesetzlich erforderlich.
- VOXR prüft die bestehenden Datenschutz- Datensicherheit- und Informationssicherheits-Verträge mit, sowie die TOM vom Unterverarbeitern vor Beginn der Zusammenarbeit, bei Änderungen der gesetzlichen Lage zum Thema Datenschutz, oder Hinweisen auf Fehlverhalten, sowie zusätzlich jedes Jahr auch ohne Anlass und passt diese ggf. an.
- VOXR überwacht die Verfügbarkeit der Server bei Unterverarbeitern und deren Anschlussqualität sekündlich und ergreift bei über der Norm liegenden Ausfällen entsprechende Maßnahmen bis hin zum Wechsel des Rechenzentrums.
- VOXR stellt sicher, dass Unterverarbeiter Daten des Auftragnehmers nicht kreieren, ändern oder löschen, es sei denn sie werden vom VOXR dazu angewiesen.
- VOXR setzt keine mobilen Datenträger zur Auftragsbearbeitung ein, weder im Verhältnis zum Verantwortlichen, noch im Verhältnis zu Unterverarbeitern.
- VOXR stellt bei Veränderungen des Algorithmus sicher, dass dieser keine Änderung an der Verarbeitung persönlicher Daten hervorruft und verlangt entsprechendes von Unterverarbeitern. Sollte sich herausstellen, dass eine Algorithmus-Änderung persönliche Daten verändert, so informiert VOXR den Datenschutzbeauftragen.
- Die Datenverarbeitung durch die VOXR Software wird sekündlich auf Verfügbarkeit geprüft und täglich auf Funktion.
- Im Falle, dass unberechtigte Personen Kenntnisse von personenbezogenen Daten oder geheimen Informationen erlangt haben, wird dies dem Verantwortlichen umgehend gemeldet. VOXR verpflichtet Unterauftraggeber, dies im Verhältnis zu VOXR ebenfalls zu tun.
- Unterauftragnehmer werden so ausgewählt, das eigene eingegangene Verträge erfüllt werden können, insbesondere werden nur solche Unterauftragnehmer beschäftigt, welche VOXR ein wirksames Kontrollrecht vertraglich einräumen.
- Die Korrektheit der Leistungen von Unterauftragnehmern wird durch ein technisches Monitoring gewährleistet, welches Fehlleistungen sekündlich prüft und meldet.
- Unterauftragnehmer werden auf das Datengeheimnis nach Art. 5, 28, 29, 32 DS-GVO verpflichtet.

- VOXR verpflichtet Verantwortliche vertraglich auf die Löschung aller persönlicher Daten bis spätestens 10 Tage nach Ihrer Eingabe, oder zum Ablauf des Auftrags je nachdem, was der kürzere Zeitraum ist.