VOXR

Technical and Organisational Measures (TOMs)

Pursuant to Art. 32 GDPR

Version: 2026 · Available at: voxr.com/tom

Data Processing Agreement (DPA): voxr.com/avv

0. Use of an External Data Centre

Since 2015, VOXR has relied on the expertise and reputation of Hetzner GmbH, Gunzenhausen, Germany, for the physical protection of data and information security. A DPA including TOMs pursuant to the GDPR is in place.

Hetzner has no access to VOXR event data, the database, server software, or the administration interface of the dedicated VOXR servers hosted at their facility.

1. Confidentiality

1.1 Risk minimisation in operations

- Data minimisation and short retention periods. Beyond the GDPR minimum, VOXR contractually requires its users to delete personal data within 10 days of the event.
- All data is transmitted in encrypted form only (TLS 1.2 / 1.3). Sensitive database fields are additionally encrypted at rest.
- VOXR prevents the public display of personal data collected via the Email Collector feature.
- VOXR informs customers of their data protection obligations before contract conclusion.

1.2 Physical access control

Managed by Hetzner GmbH (see Hetzner's own TOMs for details).

1.3 System access control

Managed by Hetzner GmbH and VOXR internally: two-factor authentication for all administrative access; passwords complying with current minimum standards (length, complexity, regular renewal).

1.4 Data access control

- Secure password policy for servers, database, and all software environments.
- Regular security updates for the operating system and all software components.
- Mandatory permission assignment process based on the need-to-know principle.
- Data stored exclusively on server-internal drives; no external removable media.

1.5 Separation control

- VOXR event data is stored physically and logically separate from VOXR customer account data.
- Data of different customers is logically separated via separate database structures (multi-tenancy).
- Backups are also stored in logically separate locations.

2. Integrity (Art. 32(1)(b) GDPR)

2.1 Data transfer control

- All staff with access to personal data are trained and obligated in accordance with Art. 32(4) GDPR.
- Data transfers to external services (particularly AI services) are carried out solely on the basis of appropriate legal grounds (SCCs under Art. 46 GDPR) and only with the Controller's explicit opt-in.

2.2 Input control

Control over the entry of event data, including any personal data, rests exclusively with the Controller. VOXR has no influence over this and accepts no responsibility for the lawfulness of data collection.

3. Availability and Resilience (Art. 32(1)(b) GDPR)

- Automated server monitoring alerts the relevant parties immediately in case of unavailability.
- All relevant data is backed up daily in logically separate storage. Backups are retained for a maximum of 30 days and then permanently and completely deleted.
- VOXR servers are regularly updated with the latest operating system and security patches.
- VOXR servers operate in RAID (mirrored disk) configuration.
- The data centre provides: uninterruptible power supply (UPS), emergency generator, permanent DDoS protection.
- An escalation chain defines who must be notified in case of failure to restore the system as quickly as possible.

4. AI Services and Third-Country Data Transfers

VOXR offers optional AI-powered features (e.g. AI summaries, event chat, machine translation). These features use external services that may process data outside the EU.

4.1 AI services used

- OpenAI, L.L.C. (USA): For AI summaries and event chat. Legal basis for third-country transfer: Standard Contractual Clauses (SCCs) under Art. 46 GDPR, as part of the OpenAI Data Processing Agreement.
- DeepL SE (Germany): For machine translation. Processing within the EU/EEA.

4.2 Data protection principles for AI processing

- Privacy by Default: All AI features are disabled by default. Data is only transferred to AI services when the Controller actively enables a feature.
- Data minimisation: Requests to AI services are limited to the minimum necessary for the respective function.
- No training data retention: VOXR uses API settings that exclude data from being used for model training (Zero Data Retention where available).
- Transparency: The Controller is informed about data sharing and third-country transfers when activating an AI feature.

5. Regular Review and Evaluation (Art. 32(1)(d) GDPR)

5.1 Data protection management

Combined data protection and information security management system through the data centre (for hosted components) and via VOXR's internal data protection handbook.

5.2 Incident response management

Managed by the data centre and via VOXR's internal incident response handbook. In case of a data breach, the Controller will be notified by VOXR within 48 hours (see DPA §7(8)).

5.3 Privacy by Design and Privacy by Default

Privacy-friendly defaults are considered throughout VOXR’s development process (Art. 25(2) GDPR). New features are subject to regular data protection impact assessment screening.

5.4 Processor control

- VOXR staff receive regular data protection training.
- VOXR appoints a Data Protection Officer where required by law.
- VOXR reviews its DPAs with sub-processors every two years and whenever legislation changes.