VOXR - Technical and Organisational Measures according to Art. 32 GDPR

0. Usage of an external computer centre

VoxR has been using Hetzner's many years of experience and reputation for the physical protection of data and information security since 2015. There is a DPA including TOM according to GDPR.

Hetzner has neither access to the event data of VOXR, the database, the server software, nor even the admin interface of the Hetzner stationed singular (dedicated) VOXR servers.

1. Confidentiality

1.1. Risk minimization in operations

- Minimization of the collected data volume and storage duration. Beyond the level required by the GDPR, VOXR always agrees extremely short storage periods for personal data with VOXR users, namely a maximum of 10 days.
- VOXR prevents the public display of personal data where they are specifically entered by event participants and thus collected and stored, especially in the function of the email collector (also called lead generator).
- VOXR will advise clients prior to signing the contract of use of the service of the legal requirements for the intention to collect personal information, as well as in the event of unintentional collection and/or storage, and will specify responsibilities in the contract of use.

1.2. Access control regarding hardware is granted by the computer centre (for this and other TOMs see the corresponding TOMs of the computer centre)

1.3. Access control regarding data

- Policy for strong passwords for server, database and all software environments (minimum length, character complexity and regular renewal)
- Regular security updates
- Binding authorisation procedure
- Data medium control by data center, additional health status monitoring by VOXR.

1.4. Separation control

- VOXR event data is stored physically and logically separate from VOXR customer data, except for the VOXR administrator's email address, which is stored logically separate from VOXR event data.
- Data backup is also stored logically separate from VOXR event data.

2. integrity (Art. 32 para. 1 lit. b GDPR)

2.1. Transfer control

- All employees who come into contact with personal data are instructed in accordance with Article 32 Paragraph 4 of the GDPR and are obliged to ensure that personal data is handled in compliance with data protection regulations.
- To further minimize risk, part of every contract for the use of VOXR is the obligation to delete personal data by the user within 10 days. Deletion from daily backups will occur after 30 days at the latest.

2.2. Input control

- The control of the input of event data, if necessary including personal data, is the sole responsibility of the person responsible. VOXR, by its nature, has no control over this information and assumes no responsibility for the legality of its collection and/or storage.

3. Availability and resilience (Art. 32 § 1 lit. b GDPR)

- VOXR has an automatic monitoring of the server, which immediately informs the necessary departments in case of a temporary unavailability.
- All relevant data is backed up logically separated daily, the backup is kept for a maximum of 30 days. Personal data may be deleted after 10 days.
- VOXR servers are regularly checked for the latest operating and protection programs and updated if necessary.
- VOXR servers run in hard disk mirroring mode.
- About the data center exists:
  - Use of uninterruptible power supply, backup power system.
  - Permanently active DDoS protection.
- An escalation process is defined, which specifies who is to be informed in the event of an error in order to restore the system as quickly as possible.

4. procedures for regular inspection, assessment and evaluation (Art. 32 § 1 lit. d GDPR; Art. 25 § 1 GDPR)

4.1. Combined data protection management system and information security management system as DIMS (Data Protection Information Security Management System) by computer centre (for the parts located there), as well as internal VOXR manual: Data and Information Security Protection, as well as contract components for data and information security management.

4.2. Incident-Response-Management: By data center (for the parts located there), as well as internal VOXR manual: Procedure in case of data protection incidents, imminent or detected data loss.

4.3. Data protection-friendly default settings are taken into account in the development of VOXR (Art. 25 § 2 GDPR).

4.4. Order control

- Employees of VOXR are regularly instructed in data protection law and are familiar with the procedural instructions and user guidelines for data processing on behalf of the client, also with regard to the right of instruction of the respective client. The same applies to sub-processors.
- The computer center has appointed a company data protection officer and an information security officer. Both are integrated into the relevant operational processes through the data protection organization and the information security management system.
- VOXR also appoints a data protection officer, as well as legally required.
- Other subcontractors also appoint a data protection officer, as required by law.
- VOXR checks the existing data protection, data security and information security contracts with, as well as the TOM from the subcontractor before the beginning of the cooperation, in case of changes in the legal situation regarding data protection, or indications of misconduct, and additionally every year without reason and adjusts them if necessary.

- VOXR monitors the availability of the servers at sub-processors and their connection quality every second and takes appropriate measures up to the change of the data center in case of failures above the norm.
- VOXR ensures that sub-processors do not create, modify or delete contractor data unless instructed to do so by VOXR.
- VOXR does not use mobile data carriers for order processing, neither in relation to the person responsible nor in relation to sub-processors.
- VOXR will ensure that any changes to the algorithm will not result in a change in the processing of personal data and will require sub-processors to do so. If an algorithm change is found to alter personal data, VOXR will notify the Privacy Officer.
- Data processing by VOXR software is checked for availability every second and daily for function.
- In the event that unauthorized persons have gained knowledge of personal data or secret information, the data controller will be notified immediately. VOXR requires subcontractors to do the same in relation to VOXR.
- Subcontractors will be selected so that VOXR's own contracts can be fulfilled. In particular, only those subcontractors will be employed who provide VOXR with an effective right of control.
- The correctness of subcontractors' performance is guaranteed by a technical monitoring system, which checks and reports errors every second.
- Subcontractors are bound to data secrecy according to Art. 5, 28, 29, 32 GDPR.
- VOXR contractually obliges responsible parties to delete all personal data within 10 days of their entry, or at the end of the contract, whichever is the shorter.