centron

Technical and organizational measures in accordance with Article 32 GDPR

Description of the technical and organizational measures

(Art. 32 Abs. 1 lit. d, Art 15 Abs. 1 DS-GVO)

January 2025

General Measures

- ISO 27001 certificate based on IT-Grundschutz

An **ISMS** is operated on the basis of **ISO 27001**

Initial certification:	**Validity**:
04/04/2020	04/07/2026

TrustedCloud certification: 06/14/2014

- The information security, IT usage, and data protection guidelines are accessible to all employees and are updated regularly or as required
- A data protection officer is provided and reports directly to the management
- A risk management system is established and reports to the management
- An emergency plan and a recovery plan have been established
- An incident management system has been established
- All employees are obliged to observe data protection and confidentiality

Confidentiality

Access Control (physical)

Measures to deny unauthorized access to data processing systems with which the personal data is processed and used:

- Access control system
  - Door security in the office building (electric door opener with access logging as well as logged key allocation according to key management).
  - Additional biometric access security to the data center and electronic door security for the purpose of two-stage access control.
- Establishment of protection zones and definition of access rules.
- Visitor regulations
  - Logging of all visitors
  - Visits and suppliers are subject to continuous supervision depending on the protection zone.
- All-round video surveillance of the building exterior with sabotage detection and recording. Seamless video surveillance of the data center interior.
- Intrusion alarm system with activation of the security service.

Access Control (digital)

Measures to prevent data processing systems from being used by unauthorized persons:

- Granting of authorizations according to the role and authorization concept as required
- Determination of authorizations by the technical management and management
- Logged allocation of authorizations by the technical management
- Workplace PCs are protected by employees' local passwords
- In the intranet, password guidelines are implemented by MS-AD (including special characters, minimum length, regular change of password)

- The local systems of the employees are updated regularly when updates appear
- Automatic blocking (e.g. password or pause)
- Upstream connection of a physical firewall with IDS and IPS
- Use of virus scanners
- Physical separation of networks
- Monitoring of network traffic

Access Control (internal access)

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, changed, or removed without authorization during processing, use, and after storage:

- The password is only issued by authorized personnel to persons named by the client
- The communication of instructions takes place on the part of the contractor via an ITIL-compliant ticket system
- The authorization to process personal data is controlled and logged by the Active Directory
- Logging of the logins on the systems
- Destruction of data carriers according to the data carrier destruction concept
- If the customer processes personal data on his systems, the customer is primarily responsible for securing the data. If this responsibility is assigned, the security mechanisms are to be checked by the customer at irregular intervals and, if necessary, to be criticized.

Separation Control

Measures to ensure that data collected for different purposes can be processed separately:

- Due to the way they are stored, all data can be processed separately from one another. Exclusive use of software that provides multi-tenancy
- Separation of the processing systems
- Separation of the systems in production and test environment
- Customers have no mutual access to other customer systems

Integrity

Transfer control

Measures to ensure that personal data cannot be read, copied, changed, or removed by unauthorized persons during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and determine to which bodies a transfer of personal data by institutions for data transfer is provided:

- A transfer of personal data takes place only at the request of authorized persons or institutions
- If personal data is transferred to authorized persons or institutions, it is encrypted, and unencrypted at the express request of the customer

Data carriers that contain personal data are cleaned several times using different erasure methods when the data carrier is disposed of, then the data carrier is destroyed and properly disposed of.

Input control

Measures to ensure that it can be subsequently checked and determined whether and by whom personal data has been entered, changed, or removed in data processing systems:

- Logging of the system activities by a monitoring system
- Semi-automated evaluation of log files
- Logging of all work in the ITIL-compliant ticket system
- New personal data can only be entered by authorized persons

Access to the data processing system is logged (see point access control).

Availability and resilience

Availability control

Measures to ensure that personal data are protected against accidental destruction or loss:

- RAID (redundant data writing on hard drives)
- If commissioned by the client, backup copies are created in the form of backups in accordance with the backup concept
- Rhythm: daily or according to customer requirements
- Retention period: redundant, 1-5 weeks or as requested by the customer
- File format: binary, proprietary encrypted
- The place of storage: Depending on the order, the client's dedicated storage or server systems in their own or third-party data centers or the contractor's global storage systems, which in turn have internal fault tolerance and are provided with access controls
- Depending on the order by the client: Configuration of the server systems with hardware RAID (mirroring of the hard disks), redundant power supply units
- Regular checking of the backups for functionality
- Implementation of the disaster and recovery concept, emergency concept, and recovery plan

Data center: Uninterruptible power supply (UPS), emergency diesel system, redundant air conditioning, early fire detection system, regular fire-fighting training for employees.

Procedures for periodic review, assessment and evaluation

Data protection management

- Annual review of the risk assessment for the processing of personal data
- Annual review of the technical and organizational measures for appropriateness and the state of the art
- Maintaining a central data protection management system
- Regular internal data protection audits
- Regular training courses and awareness-raising measures on the subjects of data protection and information security

Order control

Measures to ensure that personal data that is processed in the order can only be processed in accordance with the instructions of the client (order control):

- Orders by customers who request the processing of personal data are logged in a ticket system; an access control is configured for the ticket system
- Electronic orders are only possible from verified contact addresses (email and fax)
- Orders can also be sent by post in written form only through verified addresses
- Persons who place orders must have been authorized by the contractual partner to place orders