Appendix 1: Technical and organizational measures

Confidentiality

Access control

The following measures have been implemented to restrict or prevent unauthorized access to premises where personal data is processed.

- Closed doors and windows
- Security locks
- Securing the building shafts
- Controlled key allocation
- Accompanying visitors

Access control

The following measures have been implemented to prevent data processing equipment from being used by unauthorized persons.

- Use of an up-to-date firewall
- Use of up-to-date virus protection
- Use of individual user IDs
- Use of complex passwords
- Use of biometric procedures
- Two-factor authentication
- Automatic screen lock
- Encryption of data during transmission and storage

Access control

The following measures have been implemented to ensure that access to personal data is only possible in accordance with the assigned authorizations. In addition, it is ensured that personal data cannot be processed without authorization, i.e. that it cannot be recorded, read, copied, changed or deleted without authorization.

- Application-related authentication and authorization
- Logging of user access
- Encryption of data during transmission and storage
- Document shredder according to DIN 66399 level P-4 or higher
- Profilery enables the customer to configure a specific role and rights management system with a differentiated authorization concept and data-related access separation.

Pseudonymization

Where necessary, the following measures are implemented to prevent personal data from being attributed to a specific data subject without the use of additional information.

- Pseudonymization takes place as early as possible in the processing procedure

Separation control

The following measures have been implemented to ensure that data collected for different purposes is processed separately.

- Customer data is stored within a system by means of customer separation
- Separation of production and test systems
- No processing of production data in test environment

Integrity

Transfer control

The following measures have been implemented to ensure data integrity, which generally contribute to protection against unauthorized or unlawful processing, destruction or unintentional damage.

- Encrypted transmission of data
- Logging
- E-mail encryption on request

Input control

The following measures have been implemented to ensure that it is possible to check and determine by whom personal data has been entered, changed or removed.

- Logging of successful and failed login attempts
- Logging the collection, modification and deletion of personal data
- Traceability of entries, changes and deletions through individual user IDs
- Monitoring and logging of automated data processing
- Automated control of log files
- Securing log data against loss and modification

Order control

The following measures have been implemented to ensure that personal data processed on behalf of the customer can only be processed in accordance with the customer's instructions.

- Careful selection of processors from an information security perspective

- Concluded order processing contract
- Documentation of processing activities
- Regular monitoring of contract performance
- Destruction of data after completion of the order

Availability and resilience

The following measures have been implemented to ensure that personal data is protected against accidental destruction or loss and that the system and services are sufficiently resilient.

- Fire and smoke detection systems, fire extinguishers
- Uninterruptible power supply
- Regular and automated patch management
- Use of redundant systems
- Concept for data backup and recovery
- Regularly check the data backup
- Monitoring availability and capacity utilization

Procedures for regular review, assessment and validation

The following measures have been implemented to ensure that the technical and organizational measures for the protection of personal data are regularly assessed and evaluated with regard to their effectiveness.

- Appointment of a data protection officer
- Obligation of employees involved in data processing to ensure data protection and confidentiality
- Regular training of employees involved in data processing
- Regular auditing of procedures
- Regular review of the state of the art in accordance with Article 32 DSGVO

Privacy-friendly default settings

The following measures have been implemented to ensure that personal data is only collected and processed if this is actually necessary for the result to be achieved.

- Products are developed and operated according to the "privacy by design" principle
- Personal data is collected and processed for specific purposes
- Personal data is processed in a transparent and comprehensible manner

Emergency management

The following measures have been implemented to ensure that data protection incidents can be detected, reported, and remedied:

- Documented procedure for identifying and reporting data protection incidents
- Immediate notification of the controller in the event of data breaches pursuant to Art. 33 (2) GDPR
- Recovery procedures to ensure the availability of personal data in accordance with Art. 32 (1)(c) GDPR

Version: 2026-03-10