General description of the technical and organizational measures in accordance with Art. 32 para. 1 GDPR

Taking into account the nature, scope, context and purposes of processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures set out below to ensure and demonstrate that the processing is carried out in accordance with the applicable GDPR. These measures shall be reviewed and updated as necessary.

1 Confidentiality (Art. 32 para. 1 b) GDPR)

1.1 Physical access control

The prevention of unauthorized persons from entering the building and individual secured areas within the building is ensured by the following measures:

- Alarm system
- Light barriers and motion detectors
- Security locks with manual locking system
- Locking system with chip card / transponder system
- Securing of building accesses
- Intercom system
- Key management / key book
- Video surveillance of the entrances
- Careful selection of cleaning and security personnel

1.2 Logical access control

Sufficient protection of the IT systems is ensured by:

- Authentication with username & password
- Two-factor authentication
- Pre-boot password
- Use of firewalls
- Use of Mobile Device Management
- Use of VPN technology
- Auto start of external data carriers is prevented
- WLAN password protected
- Unused network sockets not patched
- Network physical / logical (VLAN) segmented, WLAN guest network
- Technical password policy (forced by the system)
- Authorization concept
- Personal user profiles (no function profiles)
- Organizational password policy

1.3 Data access control

Systems that are used by different users are secured by data access controls. This is a general access protection around server and network:

- Secure deletion of data carriers before external transfer
- Proper destruction of data carriers
- Use of document shredders
- Number of administrators reduced to the minimum
- Separate administrator accesses with separate login
- Authorization concept
- Administration of user rights by system administrators
- Secure storage of data carriers

1.4 Separation control

Separate processing of data collected for different purposes

- Separation of production and test system
- Separation of private and business data (MDM)
- Authorization concept
- Separation of private and business data (prohibition of private use)

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

2.1 Data transfer control

These measures serve to protect against unauthorized access to files via the Internet and e-mail:

- Setting up VPN connections
- Careful selection of transport personnel and vehicles
- Ensuring that only authorized recipients receive data

2.2 Input control

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

- Assignment of rights to enter, change and delete data based on an authorization concept
- Traceability of entries, changes to and deletion of data through individual usernames

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

3.1 Availability control

A comprehensive security concept is used to protect business-critical data from accidental or deliberate destruction:

- Fire and smoke detection systems
- Air conditioning in server rooms
- Equipment for monitoring temperature and humidity in server rooms
- Protective socket strips in server rooms
- Uninterruptible Power Supply (UPS)
- Separate redundant circuits
- Redundancies
- Alarm message for unauthorized access to server rooms
- Store backup data in a secure, outsourced location
- Backup & recovery concept
- Regular tests of data recovery
- IT emergency plan

3.2 Rapid recoverability (Art. 32 para. 1 c) GDPR)

A comprehensive data backup strategy has been developed to prevent data loss:

- Data backups
- Recovery system
- IT emergency plan (business-critical)
- Restart plan
- Incident management
- IT documentation on the current status

4 Process for regularly testing, assessing and evaluating (Art. 32 para. 1 d) GDPR; Art. 25 para. 1 GDPR)

4.1 Order control

Ensuring that personal data processed on behalf of the client are only processed according to the client's instructions:

- Selection of the contractor under due diligence aspects
- Ongoing review of the contractor and his activities
- Ensuring the destruction / return / deletion of data after completion of the order
- Obligation of the contractor's employees to maintain data secrecy
- Effective rights of control over the contractor
- Prior examination of the safety measures taken by the contractor and corresponding documentation

4.2 Data protection management

Ensuring that the internal organization meets the special requirements of privacy:

- Data protection officer
- Obligation of employees to maintain data secrecy
- Standardized guidelines and other written regulations on how to proceed in certain privacy cases

4.3 Incident response management

Ensuring that security incidents are detected at an early stage and that immediate action can be taken to minimize serious consequences:

- Security incidents trigger alarm
- Emergency manual and/or emergency concept
- Documentation of incidents

4.4 Privacy-friendly default settings

Ensuring that only personal data whose processing is necessary for the respective specific processing purpose are processed by default settings

- Deactivation of privacy-unfriendly default settings
- Compliance with deletion periods
- Privacy-friendly arrangement of contracts with service providers
- Regular review of the sample contracts used