# Technical and Organizational Measures

This document describes the requirements and implementation of measures for secure and compliant processing of personal data.

## 1. Confidentiality

### 1.1 Entry control

Measures for preventing unauthorized individuals from accessing the premises where personal data are processed:

| | |
|---|---|
| X | Locked building |
| X | Electronic security locking system |
| X | Mechanical security locking system |
| X | Documented key issuance |

| | |
|---|---|
| X | Locked server rooms with entry control |
| X | Locked server cabinets |
| X | Visitor registration and monitoring |
| X | Daily security service for offices and building |

### 1.2. Access control

Measures for preventing unauthorized individuals from accessing the personal data processed digitally:

| | |
|---|---|
| X | Personalized user accounts |
| X | Complex Passwords |
| X | Central authentication |
| X | Access blocked after five incorrect password entries |
| X | Systems access is logged and monitored |

| | |
|---|---|
| X | Encrypted employee laptops |
| X | Secure line connection for external access (VPN) |
| X | Use of an up-to-date firewall |
| X | Multifactor access control |

### 1.3 Usage control

Measures for restricting and monitoring accesses to personal data:

| | |
|---|---|
| X | Role-based authorization process |
| X | Authentication with unique username and password |
| X | Logging user access and data processing |
| X | Allocation of authorizations only after approval by the data owner |

| | |
|---|---|
| X | Protected access to data storage media |
| X | Secure destruction of paper documents |
| X | Encryption of data at rest |
| X | Minimization of superuser access |

### 1.4 Personal data minimization

Measures to minimize the use of personal data:

| | |
|---|---|
| X | Processing of personal data restricted to the minimal required for the defined purpose |

| | |
|---|---|
| X | Pseudonymization of personal data whenever feasible |

### 1.5 Separation control

Measures for separating personal data by means of various storage locations or logical separation:

| | |
|---|---|
| X | Separation of production and test systems |

| | |
|---|---|
| X | Separation of personal data with the data processing systems |

## 2. Integrity

### 2.1 Transmission control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during transmission:

| | |
|---|---|
| X | For data in transit required AES-256 encryption. |
| X | The use of private data storage media is prohibited |

| | |
|---|---|
| X | Special protection when physically transporting data storage media |
| X | Connections to the infrastructure by employees are encrypted end-to-end |

### 2.2 Input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data has been processed:

| | |
|---|---|
| X | Traceability when assigning, changing and deleting user authorizations |

### 2.3 Contractual order control

Measures to ensure that the personal data processing carried out on a subcontracted basis takes place exclusively at the instruction of the Controller:

| | |
|---|---|
| X | Documentation of processing activities |
| X | Careful selection of processors (detailed assessment of provided guarantees) |
| X | No use of processors who have not entered into agreement pursuant to Article 28 GDPR where applicable |

| | |
|---|---|
| X | Written agreement with the processor on the data protection minimum standard |
| X | Assuring compliant destruction or return of data upon completion of the assignment |

## 3. Availability and reliability

Measures for protecting personal data against accidental destruction or loss:

| | |
|---|---|
| X | Regular documented patch management for servers |
| X | Regular documented patch management for endpoint devices |
| X | Mitigate and remediate any confirmed zero-day vulnerabilities |
| X | Recovery procedures are established and tested at least annually |

| | |
|---|---|
| X | Physically separate redundant data storage or backup data |
| X | Uninterrupted power supply |
| X | Early fire detection in office buildings |

## 4. Procedure for routine review, assessment, and evaluation

Measures for monitoring personal data protection and for verifying appropriateness of established technical and organizational measures:

| | |
|---|---|
| X | Appointment of a data protection officer where required |
| X | Regular documented training of employees involved in personal data processing |
| X | Documented procedure for introducing, modifying, and discontinuing procedures |

| | |
|---|---|
| X | Regular audits by independent third parties |
| X | Regular review of the latest technical standards pursuant to Article 32 GDPR |
| X | Regular auditing or other suitable verifications of the processors |