



Technical and Organizational Measures

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

Physical access control (Zutrittskontrolle)

Measures suitable for denying unauthorized persons entry to data processing facilities used to process or use personal data.

- ✓ Alarm system
- ✓ Locking system with code lock
- ✓ Key management (key issuance, etc.)
- ✓ Visitor reception
- ✓ Careful selection of personnel (cleaning, gatekeeping, etc.)
- ✓ Structural measures (burglar-resistant windows, etc.)
- ✓ Documented rules for physical access control
- ✓ Division of buildings into security zones
- ✓ Securing of building shafts/ducts
- ✓ Chip card / transponder locking system
- ✓ Manual locking system
- ✓ Security locks
- ✓ Person checks at gatekeeper / reception
- ✓ Established control mechanisms (spot checks of key management, etc.)

System access control (Zugangskontrolle)

Measures suitable for preventing data processing systems from being used by unauthorized persons.

- ✓ Assignment of user rights
- ✓ Password policy (complex passwords)
- ✓ Authentication with username / password
- ✓ Case/housing locking
- ✓ Blocking of external interfaces
- ✓ Use of intrusion detection systems
- ✓ Use of intrusion prevention systems
- ✓ Encryption of smartphone content
- ✓ Use of anti-virus software
- ✓ Network segmentation
- ✓ Logging of access
- ✓ Evaluation of log files

Data access control (Zugriffskontrolle)

Measures ensuring that persons authorized to use a data processing system can access only the data covered by their access authorization, and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

- ✓ Number of administrators limited to the necessary minimum
- ✓ Logging of access
- ✓ Use of external service providers for destruction of data media
- ✓ Secure storage of data media
- ✓ Rights management by the system administrator

- ✓ Proper destruction of data media (ISO/IEC 21964)
- ✓ Logging of destruction
- ✓ Documentation of authorization assignment

Separation control (Trennungskontrolle)

Measures ensuring that data collected for different purposes can be processed separately.

- ✓ Logical multi-tenant separation
- ✓ Data separation through network segmentation
- ✓ Separation of development, test and production systems
- ✓ Physical separation of data

Pseudonymization

Measures suitable for hindering or preventing the identification of the data subject.

- ✓ Managed by the data controller

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

Transfer control (Weitergabekontrolle)

Measures ensuring that personal data cannot be read, copied, modified or removed without authorization during electronic transmission, transport or storage on data media, and that it can be verified and established to which recipients a transmission of personal data is intended by means of data transmission facilities.

- ✓ Controlled destruction of data media by a certified disposal company
- ✓ Disclosure to third parties only after review of the legal basis
- ✓ Written specification of transfers to third countries
- ✓ Secure transmission of data deliveries (SFTP, VPN)
- ✓ Restriction of the group of persons authorized to transmit
- ✓ Logging of data retrieval or transmission
- ✓ Secure transport of data media (e.g. backups, tapes)

Input control (Eingabekontrolle)

Measures ensuring that it can subsequently be verified and established whether and by whom personal data has been entered into, modified in, or removed from data processing systems.

- ✓ Assignment of write rights by user
- ✓ Assignment of logins to data-processing employees
- ✓ Logging of the input, modification and deletion of personal data

3. Availability and Resilience (Art. 32(1)(b), (c) GDPR)

Availability control (Verfügbarkeitskontrolle)

Measures ensuring that personal data is protected against accidental destruction or loss.

- ✓ Data backup concept with regular backups
- ✓ Regular inspection of the condition and labeling of data media and backups
- ✓ Operation and regular testing of UPS, emergency power, surge protection
- ✓ Security precautions for server rooms
- ✓ Fire / smoke detection system
- ✓ Monitoring of operating parameters in server rooms
- ✓ Redundant storage of personal data

- ✓ Offsite storage of data media for backup
- ✓ Alarm system for server rooms
- ✓ Air conditioning in server rooms
- ✓ Fire extinguishers for server rooms
- ✓ Documented emergency plan

4. Procedures for Regular Review, Assessment and Evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

Data protection management

Measures intended to ensure the lawfulness, appropriateness and effectiveness of data protection.

- ✓ Establishment of a data protection organization
- ✓ Data protection officer appointed
- ✓ Record of processing activities
- ✓ Privacy-friendly default settings
- ✓ Data protection training
- ✓ Internal monitoring of compliance
- ✓ Reporting channels for security incidents

Commissioned processing control (Auftragskontrolle)

Measures ensuring that personal data processed on behalf of a controller can be processed only in accordance with the controller's instructions.

- ✓ Selection of the contractor with due diligence (particularly regarding data security)
- ✓ Written instructions to the contractor (e.g. via a data processing agreement) within the meaning of Art. 28 GDPR
- ✓ Contractor has appointed a data protection officer
- ✓ Control rights vis-à-vis the contractor agreed
- ✓ Prior review and documentation of the security measures taken at the contractor
- ✓ Obligation of the contractor's employees to confidentiality / secrecy
- ✓ Ongoing review of the contractor and its activities

Subprocessor / Hosting Provider Measures

The following measures apply to the subprocessors and hosting providers engaged.

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

Physical access control (Zutrittskontrolle)

Measures suitable for denying unauthorized persons entry to data processing facilities used to process or use personal data.

- ✓ Alarm system
- ✓ Automatic access control
- ✓ Locking system with code lock
- ✓ Light barriers / motion detectors
- ✓ Key management (key issuance, etc.)
- ✓ Logging of visitors
- ✓ Careful selection of personnel (cleaning, gatekeeping, etc.)
- ✓ Structural measures (burglar-resistant windows, etc.)
- ✓ Division of buildings into security zones
- ✓ Chip card / transponder locking system
- ✓ Video surveillance of access points
- ✓ Person checks at gatekeeper / reception
- ✓ Documented rules for physical access control
- ✓ Established control mechanisms (spot checks of key management, etc.)

System access control (Zugangskontrolle)

Measures suitable for preventing data processing systems from being used by unauthorized persons.

- ✓ Assignment of user rights
- ✓ Password policy (complex passwords)
- ✓ Authentication with username / password
- ✓ Blocking of external interfaces
- ✓ Logging of visitors
- ✓ Use of intrusion detection systems
- ✓ Use of anti-virus software
- ✓ Use of a hardware firewall
- ✓ Network segmentation
- ✓ Logging of access
- ✓ Four-eyes principle for granting authorizations
- ✓ Evaluation of log files
- ✓ Use of penetration tests
- ✓ Creation of user profiles
- ✓ Assignment of user profiles to IT systems
- ✓ Use of VPN technology
- ✓ Encryption of mobile data media
- ✓ Encryption of data media in mobile devices
- ✓ Use of MDM software

- ✓ Use of a software firewall
- ✓ Regular password changes
- ✓ Account lockout after failed login attempts
- ✓ Automatic screen lock after a defined time interval

Data access control (Zugriffskontrolle)

Measures ensuring that authorized persons can access only the data covered by their access authorization, and that personal data cannot be read, copied, modified or removed without authorization.

- ✓ Creation of an authorization concept
- ✓ Number of administrators limited to the necessary minimum
- ✓ Logging of access
- ✓ Physical deletion of data media before reuse
- ✓ Use of external service providers for destruction of data media
- ✓ Encryption of data media

Separation control (Trennungskontrolle)

Measures ensuring that data collected for different purposes can be processed separately.

- ✓ Logical multi-tenant separation
- ✓ Creation of an authorization concept and assignment by roles
- ✓ Data separation through network segmentation
- ✓ Physical separation of data
- ✓ Separation of development, test and production systems

Pseudonymization

Measures suitable for hindering or preventing the identification of the data subject.

- ✓ Pseudonymization in the product “active avis” upon request

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

Transfer control (Weitergabekontrolle)

Measures ensuring that personal data cannot be read, copied, modified or removed without authorization during electronic transmission, transport or storage on data media, and that it can be verified to which recipients a transmission is intended.

- ✓ Controlled destruction of data media by a certified disposal company
- ✓ Disclosure to third parties only after review of the legal basis
- ✓ Written specification of transfers to third countries
- ✓ Secure transmission of data deliveries (SFTP, VPN)
- ✓ Use of shared networks
- ✓ Disclosure in anonymized or pseudonymized form
- ✓ Encryption of data deliveries (mobile data media)
- ✓ Restriction of the group of persons authorized to transmit
- ✓ Documentation of retrieval and transmission programs
- ✓ Logging of data retrieval or transmission
- ✓ Secure transport of data media (e.g. backups, tapes)
- ✓ Creation of accompanying documents during transport

Input control (Eingabekontrolle)

Measures ensuring that it can subsequently be verified whether and by whom personal data has been entered, modified or removed.

- ✓ Assignment of write rights by roles / organizational units
- ✓ Assignment of logins to data-processing employees
- ✓ Logging of the input, modification and deletion of personal data
- ✓ Regular review of log data

c) Availability and Resilience (Art. 32(1)(b), (c) GDPR)

Availability control (Verfügbarkeitskontrolle)

Measures ensuring that personal data is protected against accidental destruction or loss.

- ✓ Data backup concept with regular backups
- ✓ Regular inspection of the condition and labeling of data media and backups
- ✓ Operation and regular testing of UPS, emergency power, surge protection
- ✓ Security concept for server rooms
- ✓ Operation and testing of emergency plans
- ✓ Fire / smoke detection system
- ✓ Business continuity planning
- ✓ Documented disaster recovery plan
- ✓ Monitoring of operating parameters in server rooms
- ✓ Redundant storage of personal data
- ✓ Regular testing of restore capability
- ✓ Offsite storage of data media for backup
- ✓ Alarm system for server rooms
- ✓ Air conditioning in server rooms
- ✓ Fire extinguishers for server rooms

d) Procedures for Regular Review, Assessment and Evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

Data protection management

Measures intended to ensure the lawfulness, appropriateness and effectiveness of data protection.

- ✓ Establishment of a data protection organization
- ✓ Data protection officer appointed
- ✓ Security concepts
- ✓ Privacy-friendly default settings
- ✓ Reporting channels for security incidents
- ✓ Data protection training
- ✓ Internal monitoring of compliance
- ✓ External monitoring of compliance

Commissioned processing control (Auftragskontrolle)

Measures ensuring that personal data processed on behalf of a controller can be processed only in accordance with the controller's instructions.

- ✓ Selection of the contractor with due diligence (particularly regarding data security)

- ✓ Written instructions to the contractor (e.g. via a data processing agreement) within the meaning of Art. 28 GDPR
- ✓ Contractor has appointed a data protection officer
- ✓ Prior review and documentation of the security measures taken at the contractor
- ✓ Obligation of the contractor's employees to data secrecy / confidentiality
- ✓ Ensuring destruction of data after completion of the contract
- ✓ Ongoing review of the contractor and its activities
- ✓ Effective control rights vis-à-vis the contractor agreed
- ✓ Partial contractual penalties in the event of violations