Technical and organizational measures (TOM)

Contents

Technical and organizational measures (TOM)

1. Vertraulichkeit

1.1 Access control on side

Office premises measures:

- Video surveillance
- Doors with knob on the outside
- Visitor regulations
- Visitor escort by employees
- Contractual protection for service personnel (cleaning)
-

Data center measures:

- Video surveillance
- Separation systems
- Electronic locking system with authorisation management
- Biometric access locks
- Restrictive access guidelines
- Security guards
- Visitor escort exclusively by authorised employees
- Entrance alarm system
- Contractual security with service providers (maintenance)
- Security locks

1.2 Remote access control

Measures:

- Strict remote access guidelines
- Two-factor authentication where possible
- Firewall
- Regular review of authorisations

- Mandatory encryption of data connections
- Comprehensive behavioural guidelines and further training for employees in dealing with sensitive data
- Password guidelines
- Centralised password management
- Restrictive authorisation rules for particularly sensitive data
- Mobile and teleworking policy

1.3 Access control

Measures:

- Professional, external destruction of data carriers
- Logging of access to applications, specifically when entering, changing and deleting data
- deletion of data
- Use of authorisation concepts
- Minimum number of administrators
- Behavioural guidelines for administrators
- Management of user guidelines by administrators

1.4 Separation control

Measures:

- Separation of productive and test environment
- Physical separation (systems / databases / data carriers)
- Multitenancy of relevant applications
- Control via authorisation concept
- Definition of database rights
- Restrictive authorisation concept

Technical and organizational measures (TOM)

1.5 Pseudonymisation

Measures:

- Internal guidance for anonymizing/pseudonymizing personal data in case of disclosure or after the statutory deletion period has lapsed
- Pseudonymisation of personal data for analytical purposes in cooperation with third parties

Technical and organizational measures (TOM)

2. Integrity
2.1 Transfer control

Measures:

- VPN
- Logging of accesses and retrievals
- Encrypted transmission of data
- Documentation of the data recipients and the duration of the planned transfer and the deletion periods
- Forwarding in anonymised or pseudonymised form

3. Availability and resilience
3.1 Availability control

Measures:

- Fire and smoke detection system
- Automatic fire extinguishing system
- Climate monitoring server rooms
- UPV (uninterruptible power supply)
- Emergency power generator
- Redundant power supply
- RAID systems
- Video surveillance
- Alarm system
- Backup and recovery concept (business continuity policy)
- Monitoring systems
- Detailed emergency planning
- Redundant network supply
- Regular review and testing of emergency plans
- Incident management policy

4. Procedure for regular review, assessment and evaluation

4.1 Data protection measures

Measures:

- Regular review of the effectiveness of the technical protection measures
- Internal data protection officer
- Data protection policy for employees and awareness training
- Sensitisation of employees
- CISO / internal information security officer
- External audits

4.2 Incident-Response-Managment

Measures:

- Use of firewall
- Regular updates
- Regular checks for security vulnerabilities
- Risk management
- Spam filter
- Virus scanner
- Documented process for recognising and reporting
- security incidents / data breaches
  (also with regard to the obligation to notify the supervisory authority)
- Documented procedure for dealing with security incidents
- Incident management policy

4.3 Data protection-friendly default settings

Measures:

- The amount of personal data collected does not exceed the amount required for the respective purpose

4.4 Order control

Measures:

- Prior review of the security measures taken by the contractor and their documentation
- Selection of the contractor from a due diligence perspective (especially regarding data protection and data security)
- In the case of long-term cooperation: Ongoing review of the contractor and its level of protection
- Diligence in the selection of suppliers