Technical and organizational measures (TOM)

Table of Contents

Technical and organizational measures (TOM)

Information Security and Data Protection Standards – Technical and Organizational Measures (TOM)

For all data processing activities in accordance with Art. 9 FADP

MOUNT10 ensures, in the interest of the integrity, traceability, availability, and confidentiality of processed personal data, a level of data security appropriate to the risk through suitable technical and organisational measures (TOM).

Within the framework of the agreed contracts and General Terms and Conditions, the customer provides MOUNT10, at their own discretion and on their behalf, with personal data and/or confidential data for processing. These measures apply to all activities related to the service in which employees of the contractor or third parties commissioned by the contractor may come into contact with the controller's personal data.

The current TOM can be found at: https://mount10.ch/en/tom/

Technical and organizational measures (TOM)

Access Control – Data Centers

(Measures to prevent unauthorized physical access to data processing systems)

Technical Measures	Organisational Measures
☑ Access control systems (mantraps)	☑ Personal identification
☑ Video surveillance	☑ Logging of access
☑ Electronic locking system with authorization management	☑ Contractual safeguards (NDA) with service providers (maintenance)
☑ Alarm system	☑ Careful selection of personnel and suppliers
☑ Security locks	☑ ID badges for employees and visitors
	☑ Security personnel
	☑ Restrictive access policies
	☑ Visitors accompanied exclusively by authorized staff

Technical and organizational measures (TOM)

System Access Control (Measures to prevent unauthorized access to data processing systems)	
Technical Measures	**Organisational Measures**
☑ User authentication ☑ Two-factor authentication (2FA) ☑ Use of firewall clusters ☑ Use of VPN technologies	☑ Authorization concept ☑ Regular review of user permissions ☑ Centralized password management ☑ Password policies ☑ Logging of access ☑ IT usage policy for employees ☑ Home office policy ☑ Comprehensive awareness and continuous training of employees in cyber security and data protection

Technical and organizational measures (TOM)

Data Access Control

(Authorized users may only access data within their authorization – need-to-know principle)

Technical Measures	Organisational Measures
☑ Logging of access ☑ Professional physical destruction of data carriers	☑ Minimal number of administrators ☑ User permissions managed by administrators ☑ Accounts of departing employees are deactivated immediately All administrative access is logged

Separation Control

(Personal data collected for different purposes must be processed separately.)

MOUNT10 AG has no access to customer data, as it is encrypted with the customer's key.

Technical Measures	Organisational Measures
☑ Physical and virtual separation (systems / databases / storage) ☑ Separation of production and test environments ☑ Multi-client capability of relevant applications	☑ Authorization and access concept ☑ Restrictive authorization concept

Technical and organizational measures (TOM)

Data Transfer Control

(Measures ensuring that data cannot be read, copied, modified, or removed without authorization during transmission or storage.)

MOUNT10 AG has no access to customer data, as it is encrypted with the customer's key.

Technical Measures	Organisational Measures
☑ Encrypted data transmission ☑ Encrypted data storage ☑ No transfer of pseudonymized data to third parties	☑ Documentation of data recipients and retention periods or deletion deadlines in accordance with the GTC

Availability and Resilience Control

Technical Measures	Organisational Measures
☑ Uninterruptible power supply (UPS) ☑ Protection against fire, smoke, flooding, humidity, etc. ☑ Climate monitoring of server rooms ☑ Emergency power generator ☑ Redundant power supply ☑ Redundant storage ☑ Video surveillance ☑ Alarm system ☑ Monitoring systems	☑ Backup concept ☑ Business Continuity Management (BCM) ☑ Testing of recovery processes ☑ Regular review and testing of emergency plans ☑ Security Incident Management policy

Technical and organizational measures (TOM)

Regular Review, Assessment and Evaluation	
Technical Measures	**Organisational Measures**
☑ Employee access to internal policies	☑ External Data Protection Advisor (DSB) ☑ External Chief Information Security Officer (CISO) ☑ Employee training in cyber security and data protection ☑ Regular review of the effectiveness of technical safeguards ☑ External audits

Technical and organizational measures (TOM)

Security Incident Response Management

Technical Measures	Organisational Measures
☑ Use of firewall clusters, regularly updated ☑ Use of spam filters, regularly updated ☑ Use of antivirus software, regularly updated ☑ Regular updates of operating systems and applications	☑ Process for detecting and reporting security incidents ☑ Documented procedures for handling data security incidents ☑ Involvement of the Data Protection Advisor (DSB) ☑ Involvement of the Chief Information Security Officer (CISO) ☑ Documentation of security incidents ☑ Process and responsibility for remediation of security incidents ☑ Cyber Security Incident Management concept

Privacy-Friendly Default Settings: Privacy by design / Privacy by default

Technical Measures	Organisational Measures
☑ Collection of personal data only when necessary and with consent	☑ Right of access is guaranteed at all times