Technical and Organizational Measures

These **Technical and Organizational Measures (TOMs)** are implemented by MPMX to ensure the secure and compliant Processing of Personal Data in accordance with applicable Data Protection Law. MPMX maintains and continuously updates these measures to reflect the state of the art, the nature and scope of Processing, and the risks to the rights and freedoms of natural persons.

1. Confidentiality

1.1 Physical Access Control

MPMX implements measures designed to prevent unauthorized physical access to facilities and systems where Personal Data may be processed, including where applicable:

- controlled office access and secured premises
- visitor registration procedures
- secured server environments operated by trusted infrastructure providers
- controlled access to equipment and workstations

Where cloud infrastructure is used, physical security is ensured by the respective certified cloud provider.

1.2 System Access Control

MPMX implements measures designed to prevent unauthorized digital access to systems processing Personal Data, including

- individualized user accounts • strong password policies
- multi-factor authentication where appropriate
- encrypted employee devices
- centralized identity and access management
- firewall protection and network segmentation
- monitoring and logging of system access

1.3 Authorization and Usage Control

Access to Personal Data is limited to authorized personnel strictly on a need-to-know basis.

Measures include:

- role-based access control
- documented authorization procedures
- periodic access reviews
- logging of administrative actions
- restriction of privileged account usage
- secure deletion procedures for physical and digital records

1.4 Data Minimization and Purpose Limitation

MPMX applies principles designed to minimize unnecessary Processing of Personal Data, including:

- limiting Processing to what is required for service delivery
- pseudonymization or masking where technically feasible
- restricting use of production data in testing environments

1.5 Separation of Environments

MPMX maintains logical and operational separation between:

- production environments
- development environments
- testing environments

Customer environments are logically separated where applicable.

2. Integrity

2.1 Secure Data Transmission

MPMX implements measures designed to ensure Personal Data cannot be read, altered, or removed by unauthorized persons during transmission, including:

- encrypted network communication using industry-standard protocols
- secure remote access mechanisms
- encrypted connections for administrative access

- prohibition of insecure data transfer methods

2.2 Traceability and Input Control

MPMX maintains mechanisms enabling retrospective verification of Processing activities, including:

- system logging of user actions
- traceability of account changes
- monitoring of administrative events
- audit trails where appropriate

2.3 Processor Governance

MPMX engages Subprocessors only after appropriate due diligence and risk assessment.

Measures include:

- written data protection agreements with Subprocessors
- contractual confidentiality obligations
- security and compliance verification
- documented onboarding procedures

3. Availability and Resilience

MPMX implements measures designed to protect Personal Data against accidental destruction or loss and to ensure service resilience, including:

- redundant cloud infrastructure where applicable
- backup procedures and disaster recovery mechanisms
- monitoring of system health and performance
- vulnerability management and patching processes
- malware protection and endpoint security
- protection of data center infrastructure by certified providers

4. Procedures for Regular Testing and Evaluation

MPMX maintains procedures designed to ensure ongoing effectiveness of security measures, including:

- regular security reviews and risk assessments
- employee security and privacy training
- documented internal policies and procedures
- independent third-party audits where applicable
- periodic review of security standards and best practices
- incident response procedures

5. Updates

5.1 MPMX may update these Technical and Organizational Measures from time to time to reflect technological developments, operational changes, or evolving security risks.

5.2 Such updates will not materially reduce the overall level of protection for Customer Personal Data.

These Technical and Organizational Measures (TOMs) are effective as of the date of publication. Last updated: 01 May 2026.