Technische und organisatorische Maßnahmen

Diese technischen und organisatorischen Maßnahmen (TOMs) werden von MPMX implementiert, um die sichere und rechtmäßige Verarbeitung von personenbezogenen Daten gemäß dem anwendbaren Datenschutzrecht sicherzustellen. MPMX pflegt diese Maßnahmen und entwickelt sie kontinuierlich weiter, um dem Stand der Technik, der Art und dem Umfang der Verarbeitung sowie den Risiken für die Rechte und Freiheiten natürlicher Personen Rechnung zu tragen.

1. Vertraulichkeit

1.1 Zutrittskontrolle

MPMX implementiert Maßnahmen, die den unbefugten physischen Zugang zu Räumlichkeiten und Systemen, in denen personenbezogene Daten verarbeitet werden, verhindern sollen, einschließlich – soweit anwendbar:

- kontrollierter Bürozutritt und gesicherte Liegenschaften
- Besucherregistrierungsverfahren
- gesicherte Serverumgebungen, die von vertrauenswürdigen Infrastrukturanbietern betrieben werden
- kontrollierter Zugang zu Geräten und Arbeitsplätzen

Soweit Cloud-Infrastruktur eingesetzt wird, wird die physische Sicherheit durch den jeweils zertifizierten Cloud-Anbieter gewährleistet.

1.2 Zugangskontrolle

MPMX implementiert Maßnahmen, die den unbefugten digitalen Zugriff auf Systeme, die personenbezogene Daten verarbeiten, verhindern sollen, einschließlich:

- individuelle Benutzerkonten
- starke Passwortrichtlinien
- Multi-Faktor-Authentifizierung, soweit angemessen
- verschlüsselte Mitarbeitergeräte
- zentrales Identity- und Access-Management
- Firewall-Schutz und Netzwerksegmentierung
- Monitoring und Protokollierung von Systemzugriffen

1.3 Zugriffs- und Nutzungskontrolle

Der Zugriff auf personenbezogene Daten ist strikt nach dem Need-to-Know-Prinzip auf autorisiertes Personal beschränkt.

Maßnahmen umfassen:

- rollenbasierte Zugriffskontrolle
- dokumentierte Berechtigungsverfahren
- regelmäßige Überprüfung der Zugriffsrechte
- Protokollierung administrativer Tätigkeiten
- Beschränkung der Nutzung privilegierter Konten
- sichere Löschverfahren für physische und digitale Aufzeichnungen

1.4 Datenminimierung und Zweckbindung

MPMX wendet Grundsätze an, die unnötige Verarbeitungen von personenbezogenen Daten minimieren sollen, einschließlich:

- Beschränkung der Verarbeitung auf das für die Leistungserbringung Erforderliche
- Pseudonymisierung oder Maskierung, soweit technisch umsetzbar
- Beschränkung der Verwendung von Produktivdaten in Testumgebungen

1.5 Trennung von Umgebungen

MPMX gewährleistet die logische und betriebliche Trennung zwischen:

- Produktivumgebungen
- Entwicklungsumgebungen
- Testumgebungen

Kundenumgebungen sind, soweit anwendbar, logisch voneinander getrennt.

2. Integrität

2.1 Sichere Datenübertragung

MPMX implementiert Maßnahmen, die sicherstellen sollen, dass personenbezogene Daten während der Übertragung nicht unbefugt gelesen, verändert oder entfernt werden können, einschließlich:

- verschlüsselte Netzwerkkommunikation unter Verwendung branchenüblicher Protokolle
- sichere Fernzugriffsmechanismen
- verschlüsselte Verbindungen für administrative Zugriffe
- Verbot unsicherer Datenübertragungsverfahren

2.2 Nachvollziehbarkeit und Eingabekontrolle

MPMX unterhält Mechanismen, die eine nachträgliche Überprüfung der Verarbeitungstätigkeiten ermöglichen, einschließlich:

- systemseitige Protokollierung von Nutzeraktivitäten
- Nachvollziehbarkeit von Kontoänderungen
- Monitoring administrativer Ereignisse
- Audit-Trails, soweit angemessen

2.3 Auftragsverarbeiter-Governance

MPMX beauftragt Unterauftragsverarbeiter nur nach angemessener Due-Diligence-Prüfung und Risikobewertung.

Maßnahmen umfassen:

- schriftliche Datenschutzvereinbarungen mit Unterauftragsverarbeitern
- vertragliche Vertraulichkeitspflichten
- Überprüfung von Sicherheits- und Compliance-Anforderungen
- dokumentierte Onboarding-Verfahren

3. Verfügbarkeit und Belastbarkeit

MPMX implementiert Maßnahmen, die personenbezogene Daten vor versehentlicher Zerstörung oder Verlust schützen und die Belastbarkeit der Services sicherstellen sollen, einschließlich:

- redundante Cloud-Infrastruktur, soweit anwendbar
- Backup-Verfahren und Disaster-Recovery-Mechanismen
- Monitoring von Systemzustand und Performance
- Schwachstellenmanagement und Patching-Prozesse
- Malware-Schutz und Endpoint-Security
- Schutz der Rechenzentrumsinfrastruktur durch zertifizierte Anbieter

4. Verfahren zur regelmäßigen Überprüfung und Bewertung

MPMX unterhält Verfahren, die die fortlaufende Wirksamkeit der Sicherheitsmaßnahmen gewährleisten sollen, einschließlich:

- regelmäßige Sicherheitsüberprüfungen und Risikobewertungen
- Schulungen der Mitarbeitenden zu Sicherheit und Datenschutz
- dokumentierte interne Richtlinien und Verfahren
- unabhängige Audits durch Dritte, soweit anwendbar
- regelmäßige Überprüfung von Sicherheitsstandards und Best Practices
- Incident-Response-Verfahren

5. Aktualisierungen

5.1 MPMX kann diese technischen und organisatorischen Maßnahmen von Zeit zu Zeit aktualisieren, um technologischen Entwicklungen, betrieblichen Änderungen oder sich verändernden Sicherheitsrisiken Rechnung zu tragen.

5.2 Solche Aktualisierungen verringern das Gesamtschutzniveau für personenbezogene Kundendaten nicht wesentlich.

Diese technischen und organisatorischen Maßnahmen (TOMs) gelten ab dem Datum ihrer Veröffentlichung. Letzte Aktualisierung: 01. Juni 2026.