Informationssicherheitsmaßnahmen

Diese Informationssicherheitsmaßnahmen beschreiben die administrativen, technischen, physischen und organisatorischen Schutzvorkehrungen, die von MPMX im Zusammenhang mit der Bereitstellung der Services umgesetzt werden. Diese Maßnahmen sind Bestandteil der ToS und der Data Processing Terms und können von Zeit zu Zeit aktualisiert werden, um technologischen Entwicklungen, betrieblichen Verbesserungen oder sich verändernden Sicherheitsrisiken Rechnung zu tragen, sofern das Gesamtschutzniveau nicht wesentlich verringert wird. Die Sicherheitsdokumentation ist beschreibender Natur und begründet keine Garantien für bestimmte technische Konfigurationen.

1. Informationssicherheitsprogramm

MPMX unterhält ein umfassendes Informationssicherheitsprogramm, das darauf ausgerichtet ist:

- die Vertraulichkeit, Integrität und Verfügbarkeit von Kundendaten sicherzustellen
- vor unbefugtem oder unrechtmäßigem Zugriff oder unrechtmäßiger Verarbeitung zu schützen
- einen versehentlichen Verlust, eine Zerstörung oder Beschädigung zu verhindern
- Cybersicherheitsrisiken zu mindern

MPMX überprüft und aktualisiert sein Informationssicherheitsprogramm regelmäßig und führt regelmäßig interne Sicherheitsschulungen für seine Mitarbeitenden durch.

2. Zertifizierungen und Standards

MPMX unterhält ein Informationssicherheits-Managementsystem, das an international anerkannten Sicherheitsstandards ausgerichtet ist. Auf zumutbare Anfrage und unter Beachtung von Vertraulichkeitspflichten kann MPMX eine Bestätigung über seinen Zertifizierungsstatus bereitstellen.

3. Verschlüsselung

MPMX setzt branchenübliche Verschlüsselungsmaßnahmen zum Schutz von Kundendaten ein, einschließlich:

- verschlüsselte Kommunikationskanäle für den Zugriff auf die Services
- Verschlüsselung von Kundendaten im Ruhezustand, soweit von der zugrunde liegenden Infrastruktur unterstützt
- sichere Speicherung von Zugangsdaten, Authentifizierungs-Secrets und Schlüsseln
- Zugriffskontrollen, die das Schlüsselmanagement auf autorisiertes Personal beschränken

MPMX kann Verschlüsselungsverfahren entsprechend Branchenstandards und technologischen Entwicklungen aktualisieren.

4. Plattform-Sicherheitsmaßnahmen

MPMX implementiert Sicherheitsmaßnahmen, die unbefugten Zugriff auf die Services verhindern sollen, einschließlich:

- logisch getrennte Produktiv- und interne Geschäftsumgebungen
- sichere administrative Zugriffsverfahren
- Überwachung auf unbefugte Aktivitäten und Sicherheitsereignisse
- zentrale Protokollierung sicherheitsrelevanter Tätigkeiten
- sichere Praktiken im Software-Entwicklungslebenszyklus
- Schutz vor Malware und bekannten Branchenbedrohungen

MPMX bringt nicht wissentlich Schadcode in die Services ein.

5. Infrastruktur- und Hosting-Sicherheit

Die Services können auf zertifizierten Cloud-Infrastruktur-Anbietern von Dritten gehostet werden. Solche Anbieter halten physische und umgebungsbezogene Sicherheitsmaßnahmen vor, die umfassen können:

- kontrollierter physischer Zugang zu Rechenzentren
- Besucher-Identifikationsverfahren
- Überwachungs- und Monitoring-Systeme
- Branderkennungs- und Brandbekämpfungssysteme
- redundante Strom- und Umgebungskontrollen
- Klimaregelungen

MPMX stellt sicher, dass mit solchen Infrastruktur-Anbietern angemessene vertragliche Sicherheitspflichten bestehen.

6. Authentifizierung, Autorisierung und Access-Management

MPMX implementiert Maßnahmen, die sicherstellen sollen, dass der Zugriff auf Kundendaten ausschließlich autorisiertem Personal vorbehalten ist, einschließlich:

- individuelle Benutzerkonten
- rollenbasierte Zugriffskontrollen
- Anwendung des Least-Privilege-Prinzips
- sichere Authentifizierungsverfahren
- Multi-Faktor-Authentifizierung für administrative Zugriffe, soweit angemessen
- Protokollierung und Überprüfung privilegierter Zugriffe

MPMX beschränkt den dauerhaften Zugriff auf Produktivumgebungen auf solches Personal, das einen derartigen Zugriff aus betrieblichen Gründen benötigt.

7. Change-Management und Systempflege

MPMX unterhält Change-Management-Verfahren, die sicherstellen sollen, dass Updates, Patches und Systemänderungen vor dem Rollout ordnungsgemäß geprüft, getestet und freigegeben werden. Sicherheitsupdates und die Beseitigung von Schwachstellen erfolgen gemäß internen risikobasierten Verfahren.

8. Backup, Business Continuity und Disaster Recovery

MPMX unterhält Backup- und Recovery-Verfahren, die die Verfügbarkeit und Belastbarkeit der Services sicherstellen sollen, einschließlich:

- automatisierte Backup-Routinen
- redundante Speichermechanismen, soweit angemessen
- dokumentierte Disaster-Recovery-Verfahren
- regelmäßige Tests der Wiederherstellungsprozesse

9. Security Monitoring, Testing und Schwachstellenmanagement

MPMX führt ein Security Monitoring durch und unterhält Verfahren zur Identifikation von Schwachstellen und potenziellen Bedrohungen. Diese Verfahren können umfassen:

- automatisierte Monitoring-Werkzeuge
- Schwachstellenbewertungen
- Patch-Management-Prozesse
- regelmäßige interne Sicherheitsüberprüfungen

MPMX kann qualifizierte externe Sicherheitsspezialisten mit der Durchführung von Bewertungen oder Tests beauftragen, soweit dies angemessen ist.

10. Management von Sicherheitsvorfällen

MPMX unterhält einen Incident-Response-Prozess, der Sicherheitsvorfälle erkennen, darauf reagieren und sie eindämmen soll. Tritt ein bestätigter Sicherheitsvorfall ein, der Kundendaten wesentlich betrifft, benachrichtigt MPMX den Kunden unverzüglich und stellt die verfügbaren Informationen bereit, die nach dem anwendbaren Datenschutzrecht erforderlich sind.

11. Personalsicherheit und administrative Schutzvorkehrungen

MPMX implementiert administrative Schutzvorkehrungen, einschließlich:

- Vertraulichkeitsverpflichtungen für Mitarbeitende
- Zugriffsverfahren für Onboarding und Offboarding
- regelmäßige Schulungen zum Sicherheitsbewusstsein
- dokumentierte interne Sicherheitsrichtlinien

Hintergrundüberprüfungen können dort durchgeführt werden, wo dies angemessen und rechtlich zulässig ist.

12. Verantwortlichkeiten des Kunden

Der Kunde bleibt verantwortlich für:

- die Verwaltung von Benutzerzugriffen und Zugangsdaten
- die Konfiguration der in den Services verfügbaren Sicherheitsfunktionen
- die Sicherstellung der rechtmäßigen Erhebung und des rechtmäßigen Uploads von personenbezogenen Daten
- die Pflege angemessener Backups der vom Kunden kontrollierten Datenquellen
- den Schutz der Infrastruktur und Endgeräte auf Seiten des Kunden

Diese Informationssicherheitsmaßnahmen gelten ab dem Datum ihrer Veröffentlichung. Letzte Aktualisierung: 01. Juni 2026.