Anlage 3 zum AVV: Technische und organisatorische Maßnahmen (TOMs)

01.08.2026

> Version 1.0 | Gültig seit: 01.08.2026

MBCOM setzt die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DSGVO zu gewährleisten. Die konkrete Ausgestaltung richtet sich nach Schutzbedarf, technischem Stand und Verarbeitungsrisiko. Diese TOMs werden jährlich sowie bei wesentlichen Änderungen der Verarbeitungsprozesse auf ihre Wirksamkeit geprüft, dokumentiert und erforderlichenfalls angepasst.

Die Maßnahmen sind nach den Verantwortungsbereichen MBCOM (Dienstleister) und den Unterauftragsverarbeitern (Rechenzentrumsbetreiber) gegliedert.

1. Maßnahmen der MBCOM IT-Systemhaus GmbH (Plattform & Organisation)

1.1 Maßnahmen zur Vertraulichkeit

1.1.1 Zutrittskontrolle (Gebäude/Büros)

- Einsatz einer Alarmanlage mit internem Meldeweg.
- Besucherkontrolle am Empfang und Begleitung durch Mitarbeiter.
- Einzelschließung für Büros mit sensiblen Daten.
- Schließsystem mit Chipkarten/RFID/Transponder.
- Schlüsselregelung mit lückenloser Dokumentation (Schlüsselbuch).
- Videoüberwachung im Außenbereich zur Diebstahlsicherung (Löschfrist gemäß gesetzlicher Vorgaben).

1.1.2 Zugangskontrolle (Systeme/Netzwerke)

- Firewall mit Intrusion Prevention und Content-Filter.
- Einsatz von Mobile Device Management (MDM).
- On-/Offboarding-Prozess für Mitarbeiter.
- Einsatz von Passwort-Managern mit Verschlüsselung.
- Persönlicher und individueller User-Log-In; Verbot von Shared Accounts.
- Verpflichtende Zwei-Faktor-Authentifizierung (2FA) für privilegierte administrative Zugänge zu Produktivsystemen; technisch nicht 2FA-fähige Notfallzugänge werden auf das notwendige Minimum beschränkt, gesondert geschützt und protokolliert.
- WLAN-Verschlüsselung (WPA3-Standard, wo technisch möglich, mindestens WPA2/AES).

1.1.3 Zugriffskontrolle (Daten/Anwendungen)

- Strenges Berechtigungskonzept nach dem “Need-to-Know”-Prinzip.
- Audit-Logging von Datenzugriffen auf sensiblen Systemen.
- Bildschirmschoner mit automatischer Sperrung nach Inaktivität.
- Einsatz von Aktenvernichtern (Sicherheitsstufe P-4 nach DIN 66399).
- Verschlüsselung von mobilen Endgeräten (Notebooks, Smartphones).

1.1.4 Trennungsgebot (Mandantentrennung)

- Logische Mandantentrennung auf Datenbankebene zur Verhinderung von Cross-Tenant-Access.
- Trennung von Netzwerken (Gast, Verwaltung, Produktion).
- Trennung von Produktiv-, Stage- und Testumgebungen.

1.1.5 Pseudonymisierung & Verschlüsselung

- Datenverschlüsselung “at rest” (auf den Speichermedien) und “in transit” (TLS 1.2 oder höher).
- Absicherung der Fernwartungsverbindungen über gesicherte Tunnel.

1.2 Maßnahmen zur Integrität (Eingabekontrolle)

- Protokollierung von Eingaben, Änderungen und Löschungen durch individuelle Benutzerkennungen.
- Code-Reviews und automatisierte Tests vor Deployment neuer Versionen.

1.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

- Risikobasiertes Patch-Management mit dokumentierter Priorisierung; kritische Sicherheitsupdates werden nach Prüfung von Ausnutzbarkeit, Exposition und Betriebsrisiko unverzüglich innerhalb der intern festgelegten Behebungsfrist eingespielt oder bis dahin durch dokumentierte Schutzmaßnahmen mitigiert.
- Einsatz von Antivirensoftware und Spamfiltern.
- Monitoring der Systemauslastung und Verfügbarkeit (24/7).
- Definierter Incident-Response-Plan (IRP) bei Sicherheitsvorfällen.

1.4 Weitere Maßnahmen (Auftragskontrolle/Management)

- Regelmäßige Datenschutz-Schulungen der Mitarbeiter (mindestens jährlich).
- Verpflichtung der Mitarbeiter auf Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO).
- Benennung eines Datenschutzbeauftragten.
- Einsatz softwaregestützter Tools zur Datenschutzverwaltung (audatis MANAGER).

2. Maßnahmen der Rechenzentrum-Subunternehmer (Cloud-Sicherheit)

MBCOM nutzt für den Betrieb der ConnectCLOUD Rechenzentren der IONOS SE und Hetzner Online GmbH. Die nachfolgend zusammengefassten Kontrollen werden anhand der jeweils aktuellen Vertragsunterlagen, Sicherheitsdokumentationen und verfügbaren Prüfungsnachweise des betreffenden Subunternehmers bewertet:

- **Zutrittskontrolle:** Dokumentierte physische Zutrittsbeschränkungen, Überwachung und Besucherregelungen für Serverbereiche.
- **Verfügbarkeit:** Redundante Energieversorgung sowie Maßnahmen zur Brandfrüherkennung, Löschung und Klimatisierung entsprechend der gebuchten Rechenzentrumsleistung.
- **Integrität/Sicherheit:** Maßnahmen zur Schwachstellenprüfung und Abwehr von Netzwerkangriffen sowie die in den jeweils aktuellen Prüfungsnachweisen ausgewiesenen Zertifizierungen.
- **Auditierung:** MBCOM prüft regelmäßig Gültigkeit, Geltungsbereich und Relevanz der vom jeweiligen Subunternehmer tatsächlich vorgelegten Zertifikate und Prüfungsberichte; eine bestimmte Zertifizierung gilt nur als zugesichert, wenn sie im aktuellen Nachweis für die genutzte Leistung ausgewiesen ist.

Nachweise der Zertifizierungen der Subunternehmer werden dem Auftraggeber auf Anfrage zur Verfügung gestellt.