

Technische und organisatorische Maßnahmen (TOMs)

Stand: 25.10.2026

Online-Fassung: <https://vertriebs-ai.de/avv#anlage-2>

Anlage 2 zum Auftragsverarbeitungsvertrag (AVV) der MW Software GbR

Anlage 2 – Technische und organisatorische Maßnahmen (TOMs)

Die nachfolgenden Maßnahmen beschreiben das zum Zeitpunkt der Veröffentlichung dieses AVV bestehende Sicherheitsniveau. Der Auftragsverarbeiter darf die Maßnahmen fortentwickeln, sofern das Schutzniveau nicht unterschritten wird.

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Zutritt zu produktionsrelevanten Systemen nur für autorisierte Personen
- Nutzung etablierter Cloud-Infrastrukturen mit physischen Sicherheitsmaßnahmen des jeweiligen Hosting-Anbieters

1.2 Zugangskontrolle

- Zugriff auf Administrations- und Produktivsysteme nach Berechtigungskonzept
- Verwendung individueller Benutzerkennungen
- Multifaktorauthentifizierung für interne Zugänge, soweit verfügbar und vorgesehen
- Starke Passwortrichtlinien und Zugriffsbeschränkungen für privilegierte Konten

1.3 Zugriffskontrolle

- Rollen- und berechtigungsbasierte Zugriffskonzepte
- Beschränkung des Datenzugriffs nach Need-to-know-Prinzip
- Begrenzte Administrator-Konten
- Trennung von regulären Nutzer- und Administrationsrechten

1.4 Weitergabekontrolle

- Transportverschlüsselung für Datenübertragungen (TLS, mindestens Version 1.2)
- Absicherung externer Schnittstellen und API-Zugriffe
- Drittlandtransfers nur unter Beachtung der Art. 44 ff. DSGVO

1.5 Eingabekontrolle

- Protokollierung relevanter administrativer und sicherheitsbezogener Vorgänge
- Audit-Logging für ausgewählte organisationsbezogene Aktionen
- Nachvollziehbarkeit von Änderungen im Rahmen technischer Protokolle

2. Integrität

- Schutz vor unbefugter Veränderung durch Berechtigungs- und Rollenkonzepte
- Validierungs- und Plausibilisierungsmechanismen in Anwendungs- und Backend-Prozessen
- Teilweise manipulationsnachweisbare Audit-Protokollierung für sicherheitsrelevante Organisationsereignisse

3. Verfügbarkeit und Belastbarkeit

- Betrieb auf skalierbarer Cloud-Infrastruktur
- Maßnahmen zur Systemstabilität, Fehlererkennung und Wiederherstellbarkeit
- Protokollierung technischer Fehler und sicherheitsrelevanter Ereignisse
- Schutzmechanismen gegen Missbrauch und Überlastung im üblichen Betriebsrahmen

4. Verschlüsselung

- Transportverschlüsselung aller Verbindungen mit TLS (mindestens Version 1.2)
- Verschlüsselung gespeicherter Daten mit AES-256 auf Infrastruktur- und Plattformebene (gemäß eingesetztem Cloud-Anbieter)

5. Belastbarkeit und Wiederherstellung

- Einsatz von Cloud-Diensten mit Mechanismen zur Redundanz und Ausfallsicherheit
- Regelmäßige Aktualisierung und Wartung der produktiven Umgebung
- Wiederanlauf und Wiederherstellung im Rahmen der Möglichkeiten der eingesetzten Cloud- und Plattformanbieter

6. Verfahren zur regelmäßigen Überprüfung

- Laufende technische Weiterentwicklung der Sicherheitsmaßnahmen
- Prüfung von Zugriffsrechten und internen Berechtigungen nach Bedarf
- Fehler- und Ereignisüberwachung
- Tests und Qualitätssicherungsmaßnahmen im Rahmen des Entwicklungs- und Release-Prozesses

7. Trennung

- Logische Trennung von Kundendaten über Mandanten-, Organisations- und Rechtekonzepte innerhalb der Anwendung
- Getrennte Verarbeitungskontexte für Entwicklungs-, Test- und Produktivumgebungen, soweit betrieblich vorgesehen

8. Unterstützung bei Betroffenenrechten und Löschung

- Möglichkeiten zur Löschung oder Sperrung von Nutzerkonten und zugehörigen Daten im Rahmen der Produktfunktionen und Backend-Prozesse
- Unterstützung bei Datenexporten, Korrekturen oder Löschungen im Rahmen technischer Möglichkeiten und der vertraglichen Vereinbarungen