Anlage: Technische und organisatorische Maßnahmen (TOM)

zur Anlage zum Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

Stand: 05.01.2026

Diese Anlage beschreibt die vom Auftragsverarbeiter ergriffenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Die Maßnahmen orientieren sich an den Grundsätzen der ISO/IEC 27001 und sind auf ein B2B-SaaS-Geschäftsmodell zugeschnitten.

---

1. Zutrittskontrolle

Ziel: Verhinderung des unbefugten physischen Zugangs zu Datenverarbeitungsanlagen.

Maßnahmen:

- Betrieb der Server ausschließlich in professionellen Rechenzentren innerhalb Deutschlands
- Zutrittskontrollen mittels Chipkarten-/Schließsystemen
- Videoüberwachung und Sicherheitsdienst im Rechenzentrum
- Besucherregistrierung und -begleitung

---

2. Zugangskontrolle

Ziel: Verhinderung der Nutzung von IT-Systemen durch Unbefugte.

Maßnahmen:

- Benutzerkonten mit individuellen Zugangsdaten
- Starke Passwortrichtlinien
- Zwei-Faktor-Authentifizierung für administrative Zugänge
- Automatische Sperrung nach mehrfachen Fehlversuchen

---

3. Zugriffskontrolle

Ziel: Sicherstellung, dass berechtigte Nutzer ausschließlich auf die für sie freigegebenen Daten zugreifen können.

Maßnahmen:

- Rollen- und Berechtigungskonzepte (Least-Privilege-Prinzip)
- Trennung von Produktiv-, Test- und Entwicklungssystemen
- Protokollierung administrativer Zugriffe

---

4. Weitergabekontrolle

Ziel: Schutz personenbezogener Daten vor unbefugter Offenlegung bei Übertragung oder Speicherung.

Maßnahmen:

- Verschlüsselte Datenübertragung (TLS/HTTPS)
- Verschlüsselte Speicherung sensibler Daten
- Keine Weitergabe personenbezogener Daten an Dritte ohne Weisung

---

5. Eingabekontrolle

Ziel: Nachvollziehbarkeit, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht wurden.

Maßnahmen:

- Protokollierung relevanter System- und Administrationsvorgänge
- Zeitstempel und Benutzerzuordnung bei Änderungen

---

6. Auftragskontrolle

Ziel: Verarbeitung personenbezogener Daten ausschließlich gemäß Weisung des Verantwortlichen.

Maßnahmen:

- Verarbeitung nur im Rahmen der vertraglichen Vereinbarungen (AGB, AVV)
- Regelmäßige Schulung der Mitarbeiter zu Datenschutz und IT-Sicherheit
- Verpflichtung der Mitarbeiter auf Vertraulichkeit

---

7. Verfügbarkeitskontrolle

Ziel: Schutz personenbezogener Daten vor zufälliger Zerstörung oder Verlust.

Maßnahmen:

- Regelmäßige Datensicherungen (Backups)
- Redundante Systeme und Monitoring
- Notfall- und Wiederherstellungskonzepte

---

8. Trennungsgebot

Ziel: Getrennte Verarbeitung von Daten für unterschiedliche Kunden.

Maßnahmen:

- Mandantenfähige Systemarchitektur
- Logische Trennung von Kundendaten

---

9. Integrität und Vertraulichkeit

Ziel: Schutz der Daten vor unbefugter Veränderung oder Offenlegung.

Maßnahmen:

- Einsatz aktueller Sicherheitsupdates und Patches
- Regelmäßige Sicherheitsprüfungen
- Zugriff auf Produktivsysteme nur für autorisiertes Personal

---

10. Überprüfung und Weiterentwicklung

Die technischen und organisatorischen Maßnahmen werden regelmäßig überprüft und bei Bedarf angepasst, um ein angemessenes Schutzniveau dauerhaft sicherzustellen.