

Technische und Organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

1. Pseudonymisierung & Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Alle Datenübertragungen erfolgen verschlüsselt (HTTPS/TLS, SFTP).
 - Schlüssel und Zertifikate werden intern verwaltet.
 - Backups sind vollständig verschlüsselt.
 - Mobile Endgeräte sind über Festplattenverschlüsselung abgesichert.
-

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

- Nutzung von Microsoft Azure Germany West Central; keine eigenen Serverräume.
- Bürozugang über mechanische Schlüssel mit protokollierter Ausgabe.
- Besucher werden begleitet; Besucherbuch wird geführt.

2.2 Zugangskontrolle

- Definierter Freigabeprozess für Benutzerkennungen und Berechtigungen.
- Individuelle Kennungen, Passwortregeln (Sonderzeichen, vorgegebene Gültigkeitsdauer), technische Durchsetzung.
- Auto-Logout nach Inaktivität.
- Begrenzung fehlgeschlagener Loginversuche.
- 2-Faktor-Authentifizierung bei Fernzugriff.

2.3 Zugriffskontrolle

- Zentrale Rollen- und Rechteverwaltung; Protokollierung von Änderungen.
- Firewall mit regelmäßigen Updates; Administration durch externen Dienstleister über 4-Augen-Prinzip.

2.4 Weitergabekontrolle

- Datenübermittlung ausschließlich verschlüsselt (TLS, SFTP).
- Kein Einsatz privater Datenträger; ausschließliche Nutzung firmeneigener Medien.
- Verschlüsselter Versand sensibler Unterlagen.

2.5 Trennbarkeit

- Getrennte Entwicklungs-, Test- und Produktionsumgebungen.
-

3. Integrität & Verfügbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

3.1 Integrität

- Patch-Management-Prozess vorhanden; regelmäßige Software-Updates.
- Virenschutz, Anti-Spyware und Spamfilter, betrieben durch externen Dienstleister.

3.2 Verfügbarkeit

- Nutzung hochverfügbarer Azure-Cloud-Infrastruktur in Deutschland.
- Redundante Netzwerkanbindung; Backup-Verbindungen für Mitarbeitende.

3.3 Backup- und Notfallkonzept

- Backupkonzept vorhanden; regelmäßige Wiederherstellungstests.
- Backups als Echtzeit-Spiegelung auf redundanten Servern an separatem Standort.
- Verschlüsselte Backups; Aufbewahrung in getrennten Brandabschnitten.
- Notfallkonzept für Ausfälle, Hardwaredefekte, Brand, Totalverlust.