Technische und organisatorische Maßnahmen (TOM)

Anlage 1 zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO · TK ENTERPRISES LTD, Paphos, Zypern · Version 3.0, Stand: 07.11.2026

Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik und des Risikos für die Betroffenen folgende Maßnahmen nach Art. 32 DSGVO.

1. Vertraulichkeit

Zutritt: Die Server sind eigene Hardware des Auftragnehmers im Rechenzentrum Maincubes FRA01, Frankfurt am Main (Colocation über Klauke Enterprises GmbH & Co. KG). Das Rechenzentrum ist nach ISO/IEC 27001 zertifiziert und verfügt über mehrstufige Zutrittskontrollen, Videoüberwachung und Sicherheitspersonal rund um die Uhr. Arbeiten vor Ort (Remote Hands) erfolgen ausschließlich durch Klauke Enterprises im Auftrag des Auftragnehmers.

Zugang:

- Administration ausschließlich über verschlüsselte Verbindungen
- SSH-Zugang ausschließlich per Schlüssel, keine Passwort-Anmeldung
- Zwei-Faktor-Authentifizierung für Admin- und Kundenpanel

Zugriff: Administrativer Zugriff nur für wenige, festgelegte Personen. Alle Personen mit Zugriff sind zur Vertraulichkeit verpflichtet.

Trennung: Jede Website läuft unter einem eigenen Systembenutzer in einer vollständig isolierten Umgebung. Ein Zugriff auf andere Websites oder Bereiche des Systems wird technisch verhindert.

2. Integrität

- Datenübertragungen bei der Administration und zu Backup-Systemen erfolgen verschlüsselt
- Regelmäßige Updates von Betriebssystem und PHP
- Serverseitige Web Application Firewall mit umfangreichen Blacklists
- Tägliche Sicherheitsprüfungen und Malware-Scans

3. Verfügbarkeit und Belastbarkeit

- Rechenzentrum mit redundanter Strom- und Klimaversorgung sowie Brandfrüherkennung und Löschanlage
- Automatische Backups der Kundenwebsites auf dem Server sowie verschlüsselt auf einem separaten Backup-Server
- Überwachung der Systeme mit automatischer Alarmierung

4. Wiederherstellbarkeit

Daten können bei einem physischen oder technischen Zwischenfall aus den Backups wiederhergestellt werden.

5. Löschung

- Automatische Backups werden nach 7 Tagen gelöscht
- Manuelle Backups und alle übrigen Daten werden nach Ablauf der Abruffrist von 30 Kalendertagen nach Vertragsende gelöscht
- Defekte oder ausgemusterte Datenträger werden vor der Entsorgung sicher gelöscht oder physisch vernichtet

6. Weisungen, Unterauftragnehmer und Überprüfung

- Verarbeitung ausschließlich nach Weisung des Auftraggebers gemäß Auftragsverarbeitungsvertrag
- Unterauftragnehmer werden sorgfältig ausgewählt und vertraglich nach Art. 28 DSGVO verpflichtet
- Die Maßnahmen werden regelmäßig sowie anlassbezogen überprüft und an den Stand der Technik angepasst