



# Technisch-organisatorische Maßnahmen

## I Vertraulichkeit

### 1. Zutrittskontrolle

Für angemietete Server:

Auswahl von Server-Providern, die die Umsetzung strenger TOM garantieren:

- Überwachung und Protokollierung des Zutritts zum Serverraum
- Zutritt zum Serverraum nur durch berechtigte Mitarbeiter des Server-Providers
- Video-Überwachung der relevanten Räumlichkeiten

Für eigene Räumlichkeiten:

- Die Räumlichkeiten sind durch die Verwendung von Sicherheitsschlössern vor dem Zutritt von Unbefugten geschützt.

### 2. Zugangskontrolle

- Verwendung von Netzwerkprotokollen für eine verschlüsselte Übertragung
- Passwortgeschützter Zugang zu den Servern
- Lediglich autorisierte Mitarbeiter haben einen passwortgeschützten Zugang zum Datenserver
- Alle Computer sind passwortgeschützt und werden gesperrt, wenn der Mitarbeiter sich vom Arbeitsplatz entfernt.
- An- und Abmeldevorgänge werden protokolliert.
- Einsatz einer Personal Firewall auf den genutzten Geräten.
- Einsatz eines WLAN-Routers mit Firewall
- Angemietete Server sind mit Hardware-Firewall ausgestattet
- Wir verwenden mobile Arbeitsplätze so, dass kein Unbefugter Einblicke in das System erhält.

### 3. Zugriffskontrolle

- Lediglich autorisierte Mitarbeiter haben einen Zugriff zum Datenserver
- Die verschiedenen Komponenten des Systems sind zusätzlich einzeln passwortgeschützt, insbesondere die Datenbanken.
- Auswahl von Server-Providern, die regelmäßige Sicherheitsupdates durchführen und die  
eine sichere Vernichtung von Daten nach Beendigung der Verarbeitung garantieren
- Verschlüsselung der eingesetzten Festplatten
- Die Vernichtung und Entsorgung von ausgedruckten Inhalten mit personenbezogenen Daten erfolgt datenschutzkonform.

### 4. Trennungskontrolle

- Datensätze werden jederzeit physisch oder logisch voneinander getrennt gespeichert.
- Datensätze eines Auftraggebers können auf dessen Weisung hin in eine eigene Datenbank übertragen werden.

### 5. Pseudonymisierung





- Mitarbeiter-Accounts sind pseudonymisierbar.

## **II Integrität**

### **6. Auftragskontrolle**

- Die Mitarbeiter sind vertraut mit den Datenschutzrichtlinien hinsichtlich DS-GVO und sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.
- Die Verarbeitung personenbezogener Daten erfolgt ausschließlich auf Anweisung des Auftraggebers

### **7. Weitergabekontrolle**

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs. 4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Es findet keine Weitergabe physischer Datenträger statt
- Elektronische Datenübertragung findet ausschließlich per Leitungsverschlüsselung statt

### **8. Eingabekontrolle**

- Daten können nur nach einer benutzerkontogebundenen Authentifizierung bearbeitet oder gelöscht werden.
- Alle Bearbeitungsvorgänge, die Daten von Kunden betreffen, werden mit Verweis auf den Benutzer, der die Bearbeitung vorgenommen hat, protokolliert.

## **III Verfügbarkeit und Belastbarkeit**

### **9. Verfügbarkeitskontrolle**

- Erstellen regelmäßiger Backups aller relevanter Daten
- Auswahl von Server-Providern mit unterbrechungsfreier Stromversorgung und Netzersatzanlage.
- Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter)

### **10. Wiederherstellbarkeit**

- Erstellen regelmäßiger Backups aller relevanter Daten
- Regelmäßige Tests der Wiederherstellbarkeit der Backups

## **IV Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

### **11. Weitere Maßnahmen:**

- Unsere internen Leit- und Richtlinien, Arbeitsanweisungen und Sicherheitskonzepte unterliegen regelmäßiger Kontrolle und ggf. Überarbeitung.





- Alle Benutzerkonten sind zu Beginn stets mit minimalen Zugriffsrechten ausgestattet. Die Zugriffsrechte können daraufhin nur von autorisierten Personen angepasst werden.
- Regelmäßige Updates aller Softwarekomponenten.

