

## Anlage – Technisch-organisatorische Maßnahmen

### 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  - manuelles Schließsystem
  - Sicherheitsschlösser
  - Schlüsselregelung
  - Transponder-Schließsystem
  - Sorgfältige Auswahl von Reinigungspersonal
  
- Zugangskontrolle
  - Verwaltung von Berechtigungen
  - Erstellen von Benutzerprofilen
  - Passwortvergabe und Passwortkomplexität
  - Einsatz von Passwortmanagementlösung
  - Authentifikation mit Benutzername / Passwort
  - Einsatz von starker Authentifizierung
  - Einsatz von VPN-Technologie
  - Einsatz von AV-Software
  - Einsatz einer zentralen Smartphone Administrations Software (z.B. für Fernlöschung)
  - Verschlüsselung von Datenträgern bei Notebooks
  - Einsatz einer Hardware-Firewall
  - Einsatz von Intrusion-Detection-Systemen
  - Einsatz von Systemen zu Schwachstellenüberwachung
  - Nutzerprotokollierung
  
- Zugriffskontrolle
  - Verwaltung von Berechtigung
  - Regelmäßige Kontrolle von Berechtigungen mit Hilfe von Softwaretool
  - Protokollierung von Zugriffen
  - Einsatz von Aktenvernichtern
  - Physische Lösung von Datenträgern
  
- Trennungskontrolle
  - Berechtigungskonzept
  - Logische Mandantentrennung (softwareseitig)
  - Trennung von Produktiv-und Testsystem

## 2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  - Einrichtung von Standleitungen bzw. VPN-Tunneln
  - Bei physischem Transport sorgfältige Auswahl von Transportpersonal und Fahrzeugen
  - Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarten Löschfristen
  - E-Mail-Transport-Verschlüsselung
  - Nutzung eines verschlüsselten Datenaustauschportals
  
- Eingabekontrolle
  - Vergabe von Rechten zur Eingabe, Änderung und Löschung auf Basis eines Berechtigungskonzeptes
  - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  - Einsatz von USV-Systemen
  - Einsatz von Klimaanlage in Serverräumen
  - Technologie zur Überwachung von Serverdiensten
  - Technologie zur Überwachung von Temperatur in Serverräumen
  - CO2-Feuerlöscher im Serverraum
  - Reglm. Wiederherstellungstest
  
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
  - Standortunabhängiges Backupkonzept
  - Reglm. Wiederherstellungstest

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle  
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.