Anhang zum Verarbeitungsverzeichnis

TOM

(technisch-organisatorische-Maßnahmen)

1. Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

- manuelles Schließsystem, Videoüberwachung, Bewegungsmelder im Treppenhaus und vor dem Haus, Schlüsselregelung Beschäftigte (Schlüsselkartei), Personenkontrolle am Empfang

1.2 Zugangskontrolle

- Erstellen von Benutzerprofilen mit unterschiedlichen Berechtigungen
- Pflicht zur Passwortnutzung
- Authentifikation durch Benutzername und Passwort
- Verriegelungen an Rechnergehäusen (Server)
- Einsatz von VPN-Technologie bei Zugriff von außen auf die internen Systeme
- Einsatz von Intrusion-Detektion-Systemen
- Begrenzung der Fehlversuche bei Anmeldung am System

1.3 Zugriffskontrolle

- Nutzer-Berechtigungskonzept
- Verwaltung der Nutzerrechte durch Systemadministrator
- Anzahl der Administratoren auf das Notwendigste reduziert (1 Person + GF)
- Verwenden einer Passwortrichtlinie
- Protokollierung von Zugriffen auf Anwendungen
- ordnungsgemäße Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern
- Aufbewahrung von Datenträgern in abschließbaren Schränken
- Aufbewahrung von Aktenordnern in abschließbaren Schränken

1.4 Trennungsgebot

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Datensätze mit Zweckattributen/Datenfeldern
- Trennung der Zuordnungsdaten und der eigentlichen Daten auf einem getrennten System bei Pseudonymisierung
- Festlegung von Datenbankrechten durch Vorgaben im Berechtigungskonzept

2. Gewährleistung und Integrität

2.1 Eingabekontrollen

- Protokollierung der Eingabe, Änderung und Löschung von Daten im System
- individuelle Benutzernamen für Nutzer
- sichere Aufbewahrung von Papierunterlagen, von denen Daten ins EDV-System übernommen wurden
- Nachvollziehbarkeit durch Berechtigungskonzept

2.2 Weitergabekontrollen

- verschlüsselte E-Mail-Übertragung (SSL/TLS)
- vertraglich vereinbarte Rechte und Pflichten in Bezug auf die Datenweitergabe

3. Gewährleistung der Verfügbarkeit

3.1 Verfügbarkeitskontrollen

- Klimaanlage in Serverräumen
- Feuer- bzw. Rauchmeldeanlagen
- Feuerlöschgeräte an mehreren, entsprechend gekennzeichneten Stellen im Gebäude
- Datensicherungs-Konzept
- regelmäßiges Testen der Funktionsweise der Datensicherung
- Notfallkonzept
- Aufbewahrung von Datensicherung an sicherem, ausgelagertem Ort
- Serverräume nicht in Hochwasser gefährdeten Kellerräumen

4. Gewährleistung der Belastbarkeit der Systeme

4.1 Belastbarkeiten der IT-Systeme:

- Antiviren-Software, Hardware-Firewall, Software-Firewall, Intrusion-Detektion-System
- sorgfältige Auswahl des externen IT-Dienstleisters

5. Wiederherstellung der Verfügbarkeit

5.1 Wiederherstellbarkeit von IT-Systemen:

- sorgfältig ausgewählter interner System-Administrator
- Vorhaltung von Ersatz-Hardware / Server
- Vorhaltung von Ersatz-Hardware / Arbeitsplätze
- sorgfältig ausgewählter IT-Dienstleister

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

6.1 Informations-Sicherheits-Management-System (ISMS):

- regelmäßige Prüfung der TOM (mind. 1x jährlich) durch Geschäftsführer und System-Administrator.