Technische und organisatorische Massnahmen (TOM)

Inhaltsverzeichnis

Technische und organisatorische Massnahmen (TOM)

1. Vertraulichkeit

1.1 Zutrittskontrolle

Massnahmen Büroräumlichkeiten:

- Videoüberwachung
- Türen mit Knauf Aussenseite
- Besucherregelung
- Besucherbegleitung durch Mitarbeitende
- Vertragliche Absicherung Servicepersonal (Reinigung)

Massnahmen Rechenzentren:

- Videoüberwachung
- Vereinzelungsanlagen
- Elektronisches Schliesssystem mit Berechtigungsmanagement
- Biometrische Zugangssperren
- Restriktive Zugangsrichtlinien
- Wachpersonal
- Besucherbegleitung ausschliesslich durch berechtigte Mitarbeitende
- Alarmsystem Eingänge
- Vertragliche Absicherung mit Dienstleistern (Wartung)
- Sicherheitsschlösser

1.2 Zugangskontrolle

Massnahmen:

- Strikte Fernzugriffsrichtlinien
- Wo möglich Zwei-Faktor-Authentifizierung
- Firewall
- Regelmässige Überprüfung von Berechtigungen

Technische und organisatorische Massnahmen (TOM)

- Verpflichtende Verschlüsselung von Datenverbindungen
- Umfassende Verhaltensrichtlinien und Weiterbildung für Mitarbeitende im Umgang mit schützenswerten Daten
- Passwortrichtlinien
- Zentrales Passwortmanagement
- Restriktive Berechtigungsregelung für besonders schützenswerte Daten
- Mobile und Telearbeit Policy

1.3 Zugriffskontrolle

Massnahmen:

- Professionelle, externe Vernichtung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
- Einsatz Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Verhaltensrichtlinien Administratoren
- Verwaltung Benutzerrichtlinien durch Administratoren

1.4 Trennungskontrolle

Massnahmen:

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Mandantenfähigkeit relevanter Anwendungen
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten
- Restriktives Berechtigungskonzept

Technische und organisatorische Massnahmen (TOM)

1.5 Pseudonymisierung

Massnahmen:

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist zu anonymisieren / pseudonymisieren
- Pseudonymisierung personenbezogenen Daten zu analytischen Zwecken in Zusammenarbeit mit Dritten

Technische und organisatorische Massnahmen (TOM)

2. Integrität
2.1 Weitergabekontrolle

Massnahmen:

- VPN
- Protokollierung der Zugriffe und Abrufe
- Verschlüsselte Übertragung von Daten
- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Weitergabe in anonymisierter oder pseudonymisierter Form

3. Verfügbarkeit und Belastbarkeit
3.1 Verfügbarkeitskontrolle

Massnahmen:

- Feuer- und Rauchmeldeanlage
- Automatisches Feuerlöschsystem
- Klimaüberwachung Serverräume
- USV
- Notstromgenerator
- Redundante Stromversorgung
- RAID Systeme
- Videoüberwachung
- Alarmanlage
- Backup- und Recoverykonzept (Business Continuity Policy)
- Monitoringsysteme
- Detaillierte Notfallplanung
- Redundante Netzzuleitung
- Regelmässige Überprüfung und Tests der Notfallpläne
- Incident-Management-Policy

Technische und organisatorische Massnahmen (TOM)

4. Verfahren für regelmässige Überprüfung, Bewertung und Evaluierung

4.1 Datenschutzmassnahmen

Massnahmen:

- Regelmässige Überprüfung der Wirksamkeit der technischen Schutzmassnahmen
- Interner Datenschutzbeauftragte
- Datenschutzpolicy für Mitarbeitende und Awarenesstraining
- Sensibilisierung der Mitarbeitenden
- CISO / interner Informationssicherheitsbeauftrage
- Externe Audits

4.2 Incident-Response-Managment

Massnahmen:

- Einsatz von Firewall
- Regelmässige Aktualisierung
- Regelmässige Überprüfung nach Sicherheitslücken
- Risikomanagement
- Spamfilter
- Virenscanner
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen
  (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Incident-Management-Policy

Technische und organisatorische Massnahmen (TOM)

4.3 Datenschutzfreundliche Voreinstellungen

Massnahmen:

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

4.4 Auftragskontrolle

Massnahmen:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmassnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
- Sorgfalt bei Auswahl von Lieferanten