Allgemeine technische und organisatorische Maßnahmen (TOM) DS-GVO und Anlage

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- ⇨ Zutrittskontrollsystem, zentrales Schließsystem, Zutritt nur über Empfangsbereich mit Klingel, Codeschlösser
- ⇨ Schlüssel / Schlüsselvergabe:
  Zentrales Schließsystem, inkl. Schlüsseldokumentation, besondere Bereiche (insbes. IT) mit Codeschlössern geschützt
- ⇨ Türsicherung: alle Eingangstüren mit Codeschlössern/Schließanlage
- ⇨ Wachschutz
- ⇨ Überwachungseinrichtung: Alarmanlage

1.2. Zugangskontrolle

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- ⇨ Authentifikation mit Benutzername/Passwort (Alphanumerisch inkl. Sonderzeichen, mind. 8 Zeichen, min. 1 Buchstabe, min. 1 Sonderzeichen, keine Trivialkennworte)
- ⇨ Automatische Sperrung bei mehrmaliger Falscheingabe, zwangsweise Aktivierung des Bildschirmschoners
- ⇨ Sperrung externer Schnittstellen (USB usw.), keine externen Laufwerke (CD, Disk.) bzw. Zugriff ausschließlich für Administratoren
- ⇨ Einrichtung eines Benutzerstammsatzes pro User
- ⇨ Firewall, Virenscanner, Intrusion-Protection-System
- ⇨ Verschlüsselung mobiler Datenträger

1.3. Zugriffskontrolle

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- ⇨ Differenziertes Berechtigungskonzept (Profile, Rollen, Transaktionen und Objekte)
- ⇨ Rechteverwaltung durch Systemadministrator
- ⇨ Protokollierung des Zugriffs (insbes. bei Eingabe, Änderung, Löschung von Daten)
- ⇨ Einsatz von Aktenvernichtern/entsprechenden Dienstleistern
- ⇨ Passwortrichtlinien insbes. Kennwortlänge (s.o.), Zeichensatz (s.o.), Gültigkeitsdauer
- ⇨ Auswertung der entsprechenden Protokolle

1.4. Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- ⇨ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ⇨ Logische Mandantentrennung (softwareseitig)
- ⇨ Berechtigungskonzept

1.5. Pseudonymisierung gem. Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifisch betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

- ⇨ Im Falle der Pseudonymisierung Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen
- ⇨ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2. Integrität gem. Art. 32 Abs.1 lit b. DSGVO

2.1. Weitergabekontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- ⇨ Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- ⇨ Email-Verschlüsselung
- ⇨ Protokollierung
- ⇨ Transportsicherung
- ⇨ Bereitstellung über verschlüsselte Verbindungen wie SFTP, HTTPS
- ⇨ Dokumentation der Datenempfänger
- ⇨ Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge
- ⇨ Weitergabe nach Möglichkeit in anonymisierter und pseudonymisierter Form
- ⇨ Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen

2.2. Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- ⇨ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ⇨ Manuelle oder automatisierte Kontrolle der Protokolle
- ⇨ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ⇨ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ⇨ Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

3.1. Verfügbarkeitskontrolle

Maßnahmen zur Datensicherung (physikalisch / logisch):

- ⇨ Regelmäßiges Backup
- ⇨ Regelmäßiges Testen der Daten-Wiederherstellung
- ⇨ Spiegeln von Festplatten, z.B. RAID-Verfahren
- ⇨ Unterbrechungsfreie Stromversorgung (USV)
- ⇨ Getrennte Aufbewahrung
- ⇨ Virenschutz / Firewall
- ⇨ Notfallplan
- ⇨ Feuerwarnanlagen / Klimaanlagen in Serverräumen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO

4.1. Datenschutz-Management

- ⇨ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf / Berechtigung
- ⇨ Mind. Jährliche Überprüfung der Technischen Schutzmaßnahmen
- ⇨ Externer Datenschutzbeauftragter
- ⇨ Mitarbeiter geschult und auf Datengeheimnis verpflichtet
- ⇨ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener

4.2. Incident-Response-Management

- ⇨ Einsatz von Firewall und regelmäßige Aktualisierung
- ⇨ Spamfilter
- ⇨ Virenscanner
- ⇨ Intrusion Detection System
- ⇨ Intrusion Prevention System

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

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

4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

⇨ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation

⇨ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten insbes. In Bezug auf Datenschutz und Datensicherheit

⇨ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung

⇨ Schriftliche Weisungen an den Auftragnehmer

⇨ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)

⇨ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer

⇨ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

⇨ Externer Datenschutzbeauftragter bestellt

⇨ Kontrolle der Vertragsausführung