# TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

## 1. VERTRAULICHKEIT

### 1.1 Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: geregelte Schlüsselverwaltung, Magnet- oder Chipkarten, elektrische Türöffner, Sicherheitstüren, Portier, Sicherheitspersonal, Beaufsichtigung von Fremdpersonal, Alarmanlagen, Videoanlagen, gesicherte Aufbewahrung von Unterlagen

### 1.2 Zugangskontrolle

Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, Virtual Private Network (VPN), Protokollierung von Benutzeranmeldungen, Maßnahmen bei vergeblichen Anmeldeversuchen, eindeutige Benutzerkennung

### 1.3 Zugriffskontrolle

Zugriff auf Daten durch Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten bei Verarbeitung und Nutzung der personenbezogenen Daten und nach der Speicherung kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Festlegung der Befugnis für die Eingabe, Kenntnisnahme, Veränderung und Löschung von Daten, Standardprozess für Berechtigungsvergabe, Netzsegmentierung, Teilzugriffsberechtigungen, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten, Virenschutzkonzept, sorgfältige Aufbewahrung der Datenträger

### 1.4 Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

### 1.5 Klassifikationsschema für Daten

Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

## 2. VERFÜGBARKEIT UND BELASTBARKEIT

### 2.1 Verfügbarkeitskontrolle

Schutz personenbezogener Daten vor zufälliger Zerstörung oder Verlust z.B.: Objektsicherungsmaßnahmen, Notfallplan, Bestandsicherung (Datensicherung, Speichernetzwerke), Backup- und Recovery-Konzept, Software- und Hardwareschutz, Sachkundiger Einsatz von Schutzprogrammen [Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter] Datensicherungsschränke, Tresore.)

### 2.2 Rasche Wiederherstellbarkeit

## 3. INTEGRITÄT

3.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport und Nachvollziehbarkeit, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen sind z.B.: Verschlüsselung, Virtual Private Networks (VPN), ISDN Wall, Content Filter für ein- und ausgehende Daten, elektronische Signatur, Protokollierung (Übergabeprotokoll/Empfangsbestätigung), abgesicherter Datenträgertransport (verschließbare Transportbehälter);

3.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement, Verwendung von elektronischen Signaturen bei Eingabe/Löschung/Änderung, Regelungen der Zugriffsberechtigungen;

3.3 Trennungsgebot

Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten, z.B.: Verwendung getrennter Datenbanken, Mandantentrennung, Dateiseparierung, Trennung von Test- und Produktionssystemen, physikalische Trennung von Kundenservern, mandantenfähige Applikationen.

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

4.1 Datenschutz-Management;

4.2 Incident-Response-Management;

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

4.4 Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.