Technisch-organisatorische Maßnahmen

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

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

a. Zutrittskontrolle des Gebäudes Tag/Nacht

1. Haupteingang
- Kurze Beschreibung

2. Weitere Zugänge
- Kurze Beschreibung

b. Besucherkontrolle

Besucherregelung:

c. Schutzmaßnahmen des Gebäudes Tag/Nacht

d. Zutrittskontrolle für den Serverraum (falls im Haus betrieben)

e. Zutritt zu sensiblen Abteilungen (Personal / IT / o. vgl.)

Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

a. Zugang zu Datenverarbeitungsstationen und Systemen

b. Allgemeine Passwortrichtlinie

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

Allgemeine Richtlinie: Zugriff nur gemäß den weisungsgemäßen Befugnissen

a. Berechtigungskonzept Laufwerke

b. Berechtigungskonzept ERP

c. Berechtigungskonzept CRM

d. Berechtigungskonzept weiterer eingesetzte Systeme

d. Organisatorische Regelungen zum Speichern von Daten

e. Zugriff auf und aus dem Wifi Netzwerk

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

a. Trennung von Test- und Produktivumgebung

b. Sandboxing

c. Mandantentrennung

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

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

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

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

a. Lokale Schnittstellen an Datenverarbeitungsstationen

b. Virenschutz, Firewall und Proxy

c. Regelungen zum Email-Versand

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

a. Protokollierung

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

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

a. Back-Up System

b. Redundantes Serversystem

c. Mobile Datenverarbeitungsstationen

b. Unterbrechungsfreie Stromversorgung

c. Klimatisierung

d. Feuer/Rauchmelder

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

Datenschutz-Management

Maßnahmen, die dem kontinuierlichen Schutz von personenbezogenen Daten dienen / Datenschutzkonzept.

Incident-Response-Management

Organisatorischer und technischer Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist.

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.

a. Datenschutzkonforme Verträge mit Dienstleistern vorhanden?

- Bereits auf EU-DSVGO umgestellt?

b. Hinreichend dokumentierte TOMs der Dienstleister vorhanden?

- Haben die Dienstleister ihre TOMs bereits auf EU-DSVGO umgestellt?