STRATEGY
EXPERIENCE
TECHNOLOGY

Beschreibung der technisch-organisatorischen Maßnahmen

Stand: 30.06.2023

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

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 entsprechende technischen und organisatorischen Maßnahmen unterliegen:

- Verschlüsselung von Datensätzen
- Pseudonymisierung: Trennung der Zuordnungsdatei
- Weitergabe von Daten in anonymisierter und pseud. Form

Zugangskontrolle

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

- Alarmanlage
- Automatisches Zugangskontrollsystem
- Personenkontrolle
- Schließsystem
- Schlüssel- Chipregelung
- Videoüberwachung
- Protokollierung der Besucher
- Auswahl von externen DL Inhouse /Reinigung /Wachdienst ..
- Lichtschranken und Bewegungsmelder

Datenträgerkontrolle

- sperren von ext. Schnittstellen
- Verschlüsselung von Laptop/Notebook
- Verschlüsselung von Smartphone Inhalten
- Verschlüsselung von Datenträger
- SmartphoneAdminSoftware MDM

Speicherkontrolle

- Anti Viren Software
- Hardware-Firewall
- Software-Firewall

Benutzerkontrolle

- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- VPN - Technologie

Zugriffskontrolle

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

- Erstellen eines Berechtigungskonzept
- Authentifizierung mit Name und Passwort
- Anzahl der Admin auf “Notwendigkeit” reduziert
- Passwortvergabe und Richtlinie
- Protokollierung von Zugriffen /Eingabe/Änderung/Löschung
- Aufbewahrung von Datenträgern
- Ordnungsgemäße Entsorgung Datenträger/Dokumente
- Einrichtung einer Standleitung
- E-Mail Verschlüsselung
- Dokumentation Empfänger von Daten und Zeitspannen
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

Trennbarkeit

- physisch getrennte Speicherung auf ges. Systeme /Datenträger
- Festlegung von Datenbankrechten
- logische Mandantentrennung
- Trennung von Produktiv- und Testsystem

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

Eingabekontrolle

- Protokollierung der Eingabe / Änderung / Löschung von Daten
- Nachvollziehbarkeit der Eingabe / Änderung / Löschung
- Vergabe von Rechten zur E/Ä/L - Berechtigungskonzept
- Übersicht über Applikationen zur E/Ä/L
- Aufbewahrung von Formularen zur automatisierten Verarb.

Transportkontrolle

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

- Sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- Beim physischen transportsichere Transportbehälter

Datenintegrität

- Festlegung sicherheitskritischer Systeme
- Safety & Security

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

Verfügbarkeit

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; onsite/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne:

- USV
- Überwachung von Temperatur und Feuchtigkeit im S-Raum
- Klimaanlage im Serverraum
- Feuer und Rauchmeldung
- Alarmierung bei unberechtigten Zutritt Serverraum
- Notfallplan
- Sicherheitskonzept
- Alarmsicherung (Feuerlöscher - Alarmzentrale usw)
- Position Serverraum (bauseits intern wie extern)

Wiederherstellbarkeit

- Datensicherung Art / Umfang / Auslagerung
- Backup und Recoverykonzept

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

Datenschutz-Management

Datenschutz Mitarbeiter Vereinbarungen, Verschlüsselung, Passwörter

- Zutrittskontrolle, TOM´s, Aktualisierung des Verfahrensverzeichnisses, Verfügbarkeitsprüfung

Incident-Response-Management (Vorfalls Risiko)

Mitarbeiterschulung Risiko- und Folgenabschätzung, Schadeneindämmung, Ausmerzung der Ursache, Wiederherstellung betroffener Systeme, Dokumentation, Analyse

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

Privacy by Design - datenschutzkonforme Konzeption und Entwicklung von IT-Systemen Privacy by Default - Datenbanken und Benutzer Gruppenrechte

Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, wie Nachkontrollen der technischen und organisatorischen Maßnahmen.

- Auswahl des Auftragnehmers
- Auftragsverarbeitung Art. 28
- Wirksame Kontrollrechte / Vertragsstrafe Art.32
- Unterweisung Mitarbeiter Art 29
- Sicherstellung der Vernichtung/Löschung von Daten nach Beendigung
- Laufende Überprüfung des Auftragnehmers / Tätigkeiten