TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Verantwortliche Stelle

Firma	
Straße	
PLZ/Ort	
Telefon	
Fax	
E-Mail	
Internet Adresse (URL)	
Fachverantwortlicher für dieses Verfahren	
Organisationseinheit	G

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

• Zutrittskontrolle:

Abgeschlossene Serverräume bei den Cloud-Dienstleistern

Besucherkontrolle am Eingang (abgeschlossene Türen)

Manuelles Schließsystem

Regelungen für Zutritt zu Serverräumen externer Personen bei den Cloud-Dienstleistern

Zutritt des Rechnerraums nur für bestimmte Personen bei den Cloud-Dienstleistern

TOM der xxxx GmbH & Co.KG Stand: 2021-08-23

• Zugangskontrolle:

Authentifikation mit Benutzer und Passwort

Authentifikation mit biometrischen Daten

Einsatz von Anti-Viren-Software

Einsatz von Firewalls (bei den jeweiligen Clients als auch bei den Servern)

Erstellen von Benutzerprofilen

Passwortvergabe/Passwortregeln

Regelung für den Umgang mit Passwörtern (beschränkt auf den DEV-Bereich)

Verschlüsselung von Datenträgern (beschränkt auf die DEV Umgebung)

W-LAN ist gesichert

• Zugriffskontrolle:

Anzahl der Administratoren auf das Mindeste begrenzt

Passwortrichtlinie inkl. Länge

Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

Sichere Aufbewahrung von Datenträgern (im Rechenzentrum)

Verschlüsselung von Datenträgern (beschränkt auf den DEV-Bereich)

Verschlüsselung von Smartphones

• Trennungskontrolle:

Logische Mandantentrennung (softwareseitig).

Trennung von Produktiv- und Testsystem.

Versehen der Datensätze mit Zweckattributen/Datenfeldern.

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

Eine Pseudonymisierung findet statt.

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

• Weitergabekontrolle:

Verpflichtung der Mitarbeiter auf das Datengeheimnis

Sicherer Verbindungen über https

Regelungen bei Ausscheiden von Mitarbeitern

Regelungen zum datenschutzkonformen Vernichten von Datenträgern

• Eingabekontrolle:

Eingabekontrolldaten sind zweckbestimmt

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Protokollierung der Eingabe, Änderung und Löschung von Daten

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

• Verfügbarkeitskontrolle:

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort von den Cloudsystemen und den Clouddaten.

Sicherungen der Umgebung auf GitHub

Erstellen eines Backup & RecoverykonzeptsBackup-Strategie (offline, online z.B. Cloud)

Erstellen eines Notfallplans

Feste Prozesse zur Datensicherung

Feuer- und Rauchmeldeanlagen

Feuerlöschgeräte in Serverräumen

Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

Testen von Datenwiederherstellung

Zertifizierte Rechenzentren

Zuständige Personen zur Datensicherung sind namentlich benannt

• Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):

Backup Konzept (Offline/Online in der Cloud).

Testen der Wiederherstellungssysteme.

Notfallmanagement inkl. Notfallpläne.

Notfallmanagement Übungen (inkl. worst case).

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

• Datenschutz-Management:

• Incident-Response-Management:

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

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

• Auftragskontrolle:

Begründung für die Auswahl des Auftragnehmers (Cloud-Dienstleister)

Hard- und Softwareprodukte aus seriösen Quellen

Datenschutzberater

Prozesse für Betroffenenrechte

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags