# Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Version: 20220601

## Präambel

Der Verantwortliche hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert.

Der allgemeine Teil beschreibt technische und organisatorische Maßnahmen die unabhängig von den jeweiligen Dienstleistungen und Services, Standorten und Kunden gelten. In den Anhängen sind Maßnahmen beschrieben, die über die im allgemeinen Teil dokumentierten Maßnahmen hinaus gelten.

## 1. Vertraulichkeit

## 2. Intergrität

Vertraulichkeit ist die Eigenschaft, dass personenbezogene Daten unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.

**Zugangskontrolle**

• Formale Benutzer- und Berechtigungsverfahren

• Login nur mit Benutzername, Passwort und wo erforderlich 2-Faktor-Authentifizierung

• Systemisch forcierte Passwortrichtlinien

• VPN bei Remote-Zugriff und durch vom Verantwortlichen verwaltete Geräte

• Mobile Device Management

**Zugriffskontrolle**

• Führen von Assetregistern und Ableitung von Maßnahmen anhand der Datenklassifikation

• Nutzung kryptografischer Verfahren (z.B. Verschlüsselung)

• Umsetzung von Berechtigungskonzepten nach dem Need-to-Know-Prinzip

• Trennung von Anwendungs- und Administrationszugängen

• Protokollierung von Zugriffsversuchen

• Minimale Anzahl an Administratoren

**Pseudonymisierung**

• Sofern möglich oder erforderlich werden personenbezogene Daten pseudonymisiert verarbeitet (Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System)

**Trennungskontrolle**

• Trennung von Entwicklungs-, Test- und Produktivumgebung

• Personenbezogene Daten dürfen nicht für Testzwecke verwendet werden

• Mandantenfähigkeit / logische Trennung von Daten bei relevanten Anwendungen: Separate Datenbanken, Schema-Trennung in Datenbanken, Berechtigungskonzepte und/oder strukturierte Dateiablage

## 2. Integrität

Die Integrität personenbezogener Daten ist dann gewahrt, wenn sie richtig, unverändert und vollständig sind.

**Weitergabekontrolle**

• Bereitstellung von Daten über verschlüsselte Verbindungen (z.B. SFTP)

• Weitergabe von personenbezogenen Daten im Sinne des Need-to-Know / Need-to-Do Prinzips

• Personenbezogene Daten werde nach ihrem Schutzbedarf klassifiziert, wobei vertrauliche Daten nur über sichere Kommunikationswege übertragen werden dürfe

• Wo möglich wird E-Mail-Verschlüsselung eingesetzt

• Wo möglich werden personenbezogene Daten nur in pseudonymisierter oder anonymisierter Form übermittelt

• Dokumentation der Weitergabe von physischen Speichermedien

• Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag

**Eingabekontrolle**

• Technische Protokollierung der Eingabe, Änderung und Löschung von personenbezogenen Daten sowie Kontrolle der Protokolle

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

• Rollenbasiertes Berechtigungskonzept (Lese-, Schreib-, und Löschrechte)

• Protokollierung von administrativen Änderungen

## 3. Verfügbarkeit und Belastbarkeit

Die Verfügbarkeit von personenbezogenen Daten ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

• Einsatz von Firewalls

• Notfallhandbücher für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust

• Durchführung von Wiederherstellungstests

• Wo notwendig Nutzung redundanter Systeme (z.B. RAID)

• Regelmäßiger Test von Datensicherungen

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

**Datenschutz-Management**

• Ein Datenschutzbeauftragte ist benannt

• Alle Mitarbeiter sind auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet und werden auf das Telekommunikationsgeheimnis hingewiesen

• Mitarbeiter sind im Umgang mit personenbezogenen Daten sensibilisiert

• Neue Mitarbeiter erhalten Informationsmaterial bezüglich dem Umgang mit personenbezogenen Daten

• Ein Verzeichnis von Verarbeitungstätigkeiten wird gepflegt und Datenschutzfolgenabschätzungen werden bei Bedarf durchgeführt

• Prozesse zur Wahrnehmung von Betroffenenrechten sind etabliert

**Auftragskontrolle**

• Daten, die im Auftrag verarbeitet werden, werden nur nach Weisungen des Auftraggebers verarbeitet

• Auftragnehmer werden im Hinblick auf getroffene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sorgfältig ausgewählt

• Weisungen zum Umgang mit personenbezogenen Daten werden in Textform dokumentiert

• Sofern erforderlich werden Auftragsverarbeitungsvereinbarungen bzw. geeignete Garantien zur Übermittlung von Daten an Drittländer geschlossen

**Datenschutzfreundliche Voreinstellungen**

• Es wird prozessual sichergestellt, dass Systeme und Produkte datenschutzfreundlich entwickelt werden

• Es werden nur diejenigen personenbezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind

**Incident-Response-Management**

• Etablierter Prozess zur Erkennung, Meldung und Dokumentation von Datenschutzverletzungen unter Einbindung des Datenschutzbeauftragten

• Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen unter Einbindung der Verantwortlichen