Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO

Der Verantwortliche hat unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen die im Folgenden aufgeführten geeigneten technischen und organisatorischen Maßnahmen umgesetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der geltenden DS-GVO erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

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

1.1 Zutrittskontrolle

Die Verhinderung des Zutritts nicht berechtigter Personen in das Gebäude sowie einzelner abgesicherter Bereiche innerhalb des Gebäudes wird durch folgende Maßnahmen gewährleistet:

- Alarmanlage
- Lichtschranken und Bewegungsmelder
- Sicherheitsschlösser mit manuellem Schließsystem
- Schließanlage mit Chipkarten- / Transponder-System
- Absicherung von Gebäudezugängen
- Gegensprechanlage
- Schlüsselverwaltung / Schlüsselbuch
- Videoüberwachung der Zugänge
- Sorgfältige Auswahl von Reinigungs- und Sicherheitspersonal

1.2 Zugangskontrolle

Ein ausreichender Schutz der IT-Systeme wird gewährleistet durch:

- Authentifikation mit Benutzernamen & Passwort
- 2-Faktor-Authentifizierung
- Pre-Boot-Passwort
- Einsatz von Firewalls
- Einsatz von Mobile Device Management
- Einsatz von VPN-Technologie
- Autostart von externen Datenträgern wird verhindert
- WLAN passwortgeschützt
- Ungenutzte Netzwerkdosen nicht gepatcht
- Netzwerk physisch / logisch (VLAN) segmentiert, WLAN-Gastnetz
- Technische Passwortrichtlinie (vom System erzwungen)
- Berechtigungskonzept
- Persönliche Benutzerprofile (keine Funktionsprofile)
- Organisatorische Passwortrichtlinie

1.3 Zugriffskontrolle

Systeme, die von unterschiedlichen Benutzern verwendet werden, werden durch Zugriffskontrollen abgesichert. Dabei handelt es sich um einen allgemeinen Zugriffsschutz rund um Server und Netzwerk:

- Sichere Löschung von Datenträgern vor deren externer Weitergabe
- Ordnungsgemäße Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern
- Anzahl der Administratoren auf das Mindestmaß reduziert
- Getrennte Administratorenzugänge mit separatem Login
- Berechtigungskonzept
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Sichere Aufbewahrung von Datenträgern

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- Trennung von Produktiv- und Testsystem
- Trennung von privaten und geschäftlichen Daten (MDM)
- Berechtigungskonzept
- Trennung von privaten und geschäftlichen Daten (Privatnutzungsverbot)

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

2.1 Weitergabekontrolle

Diese Maßnahmen dienen dem Schutz vor unberechtigten Zugriffen auf Dateien via Internet und E-Mail:

- Einrichtung von VPN-Verbindungen
- Sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- Sicherstellen, dass nur berechtigte Empfänger Daten erhalten

2.2 Eingabekontrolle

Maßnahmen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

3.1 Verfügbarkeitskontrolle

Zur Sicherung geschäftskritischer Daten wird ein umfassendes Sicherheitskonzept eingesetzt, welches vor zufälliger oder mutwilliger Zerstörung schützt:

- Feuer- und Rauchmeldeanlagen
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte redundante Stromkreise
- Redundanzen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Backup- & Recoverykonzept
- Regelmäßige Tests der Datenwiederherstellung
- IT-Notfallplan

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 c) DS-GVO)

Um Datenverlust zu vermeiden ist eine umfangreiche Datensicherungsstrategie entwickelt worden:

- Datensicherungen
- Wiederherstellungs-System
- IT-Notfallplan (geschäftskritisch)
- Wiederanlaufplan
- Incident Management
- IT-Doku auf aktuellem Stand

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

4.1 Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Sicherstellung der Vernichtung / Rückgabe / Löschung von Daten nach Beendigung des Auftrags
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer
- Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation

4.2 Datenschutzmanagement

Gewährleistung, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird:

- Datenschutzbeauftragter
- Verpflichtung der Arbeitnehmer auf das Datengeheimnis
- Standardisierte Richtlinien und sonstige schriftliche Regelungen zum Vorgehen in bestimmten datenschutzrechtlichen Fallgestaltungen

4.3 Incident-Response-Management

Gewährleistung, dass Sicherheitsvorfälle frühzeitig erkannt werden und hierauf unmittelbar reagiert werden kann, damit schwerwiegende Folgen möglichst begrenzt werden:

- Sicherheitsvorfälle lösen Alarm aus
- Notfallhandbuch und/oder Notfallkonzept
- Dokumentation von Vorfällen

4.4 Datenschutzfreundliche Voreinstellungen

Gewährleistung, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden

- Deaktivierung von datenschutzunfreundlichen Voreinstellungen
- Einhaltung von Löschfristen
- Datenschutzfreundliche Gestaltung von Verträgen mit Dienstleistern
- Regelmäßige Überprüfung der verwendeten Vertragsmuster