

Anlage 1

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

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

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen ist zu reduzieren.

>> Zutrittskontrolle

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

Technische und organisatorische Maßnahmen:

- Alarmanlage
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder- oder manuelles Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal

>> Zugangskontrolle

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

Technische und organisatorische Maßnahmen:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall bei allen mobilen Arbeitsplätzen

>> Zugriffskontrolle

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

Technische und organisatorische Maßnahmen:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

>> Trennungskontrolle

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

Technische und organisatorische Maßnahmen:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

>> 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.

Technische und organisatorische Maßnahmen:

- Im Rahmen der Dienstleistungserbringung, treffen wir zusätzlich zu Maßnahmen die durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden, keine weiteren Maßnahmen zur Pseudonymisierung."

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

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren.

>> Weitergabekontrolle

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

Technische und organisatorische Maßnahmen:

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen

>> Eingabekontrolle

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

Technische und organisatorische Maßnahmen

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.

>> Verfügbarkeitskontrolle

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.

Technische und organisatorische Maßnahmen:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen

>> Belastbarkeit der Systeme

Datenverarbeitungssysteme & – Dienste müssen auch belastbar sein. Dies bedeutet einerseits, dass etwa ein Webserver auch bei kurzfristig starker Beanspruchung durch viele gleichzeitige Anfragen zuverlässig die angeforderten Daten liefert, als auch die Fähigkeit, externen Angriffen etwa durch Hacker zu widerstehen bzw. diese zu überstehen, z.B. Skalierende Systeme, Denial of Service – Abwehrtechniken, RAID-Systeme, Virenschutz, Firewall.

Technische und organisatorische Maßnahmen:

- Skalierende Systeme
- Denial of Service - Abwehrtechniken,
- RAID-Systeme
- Virenschutz
- Firewall.

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

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

>> Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Technische und organisatorische Maßnahmen:

- Es wird keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen durchgeführt.

>> Innerbetriebliche Organisation**Technische und organisatorische Maßnahmen:****a. Datenschutzmanagement**

- Nur Mitarbeiter die auf die Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet wurden, dürfen die für ihren Aufgabenbereich entsprechenden Daten verarbeiten
- Es existieren interne Verhaltensrichtlinien sowie ein Datenschutz Handbuch
- Alle Mitarbeiter werden in regelmäßigen Abständen (min. Jährlich) zum Thema Datenschutz per E-Learning geschult und sensibilisiert.
- In einem Organigramm sowie in Stellenbeschreibungen sind Verantwortlichkeiten und Befugnisse der einzelnen Mitarbeiter festgelegt und im Unternehmen bekannt gemacht.
- Dieses wird in regelmäßigen Abständen von der obersten Leitung im Rahmen der ISO 9001 Zertifizierung überprüft.

b. Störfallmanagement

- Die Einhaltung der technisch- organisatorischen Maßnahmen werden jährlich (Audit) durch den Datenschutzbeauftragten überprüft und gegebenenfalls angepasst.

c. Datenschutzes durch Technikgestaltung

- Auswahl datenschutzfreundlicher Technologie