Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragnehmer in seiner Funktion als Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

1. Vertraulichkeit

1.1 Zutrittskontrolle

Der Auftragnehmer wird angemessene Maßnahmen treffen, um das Risiko zu reduzieren, dass Unbefugte Zutritt zu Datenverarbeitungssystemen, mit denen die personenbezogenen Daten des Auftraggebers verarbeitet und genutzt werden, erhalten.

Technische Maßnahmen:

- Automatisches Zugangskontrollsystem,
- Kontrolle des Zugangs durch Pförtnerdienste und Alarmsysteme
- Chipkarten / Transpondersysteme

Organisatorische Maßnahmen:

- Schlüsselregelung (Schlüsselabgabe etc.)
- Besucher in Begleitung durch Mitarbeiter
- Sorgfältige Auswahl von Reinigungspersonal

1.2 Zugangskontrolle

Auftragnehmer wird angemessene Maßnahmen treffen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Hierzu trifft der Auftragnehmer folgende Vorkehrungen:

Technische Maßnahmen:

- Login mit Benutzername + Passwort
- Verschlüsselung von Smartphones
- Verschlüsselung von Firmen Laptops
- Fernverwaltung von Laptop
- Einsatz von Anti-Viren-Software für Server
- Einsatz von Anti-Virus-Software für Laptops

Organisatorische Maßnahmen:

- Verwalten von Benutzerberechtigungen

- Erstellen von Benutzerprofilen
- Richtlinien für die Nutzung von Firmenhardware
- Allg. Richtlinie Datenschutz und / oder Sicherheit

1.3 Zugriffskontrolle

Der Auftragnehmer wird angemessene Maßnahmen treffen, um sicherzustellen, dass die zur Benutzung der Datenverarbeitungssysteme Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass personenbezogene Daten des Auftraggebers bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Hierzu trifft der Auftragnehmer folgende Vorkehrungen:

Technische Maßnahmen:

- Löschung von Datenträgern auf Notebooks vor Wiederverwendung
- Protokollierung von Zugriffen auf wichtige Dokumente, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Aktenschredder (mind. Stufe 3, cross cut)

Organisatorische Maßnahmen:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Reduzierung der Anzahl an Administratoren
- Abgeschlossener Bereich für sensible Dokumente

1.4 Trennungskontrolle

Der Auftragnehmer wird angemessene Maßnahmen treffen, um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten des Auftraggebers getrennt verarbeitet werden können. Hierzu trifft der Auftragnehmer folgende Vorkehrungen:

Technische Maßnahmen:

- Getrennte Speicherung auf unterschiedlicher Software

Organisatorische Maßnahmen:

- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten

2. Integrität

2.1 Weitergabekontrolle

Der Auftragnehmer wird angemessene Maßnahmen treffen, um das Risiko zu reduzieren, dass personenbezogene Daten des Auftraggebers bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Hierzu trifft der Auftragnehmer folgende Vorkehrungen:

Technische Maßnahmen:

- Email-Verschlüsselung
- Protokollierung der Zugriffe und Abrufe wichtiger Dokumente und Daten
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https

2.2 Eingabekontrolle

Der Auftragnehmer wird angemessene Maßnahmen treffen, um sicherzustellen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten des Auftraggebers in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Hierzu trifft der Auftragnehmer folgende Vorkehrungen:

Technische Maßnahmen:

- Möglichkeit der technischen Protokollierung der Eingabe, Änderung und Löschung personenbezogener Daten

Organisatorische Maßnahmen:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung personenbezogener Daten durch individuelle Benutzernamen
- Aufbewahrung von Formularen, von denen personenbezogene Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung personenbezogener Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Der Auftragnehmer wird angemessene Maßnahmen treffen, um sicherzustellen, dass personenbezogene Daten des Auftraggebers gegen zufällige Zerstörung oder Verlust geschützt sind. Hierzu trifft der Auftragnehmer folgende Vorkehrungen:

Technische Maßnahmen:

- Feuer- und Rauchmeldeanlagen
- Sorgfältige Auswahl des Hostingdienstleisters

Organisatorische Maßnahmen:

- Regelmäßige Kontrolle des Hostingdiensleisters

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Auftragnehmer implementiert Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

4.1 Datenschutz-Management

Organisatorische Maßnahmen:

- Zentrale Dokumentation aller Verfahrensweisen, Regelungen und Richtlinien zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird regelmäßig durchgeführt
- Mitarbeiter geschult und auf Vertraulichkeit verpflichtet
- Sensibilisierung der Mitarbeiter durch Schulungen

4.2 Incident-Response-Management

Organisatorische Maßnahmen:

- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Regelung zu Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvor-fällen und Datenpannen
- Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO); Privacy by design / Privacy by default

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.