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

Der Auftragnehmer 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 nachfolgenden Maßnahmen werden ergriffen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- Der Zutritt zum ausschließlich von GDI genutzten Betriebsgebäude erfolgt über einen zentralen Eingang mit Pforte
- Die Eingangstür ist stets verschlossen
- Besucher müssen klingeln und werden persönlich in Empfang genommen
- Die Ausgabe der Schlüssel erfolgt ausschließlich an Mitarbeiter und wird entsprechend dokumentiert
- Der Serverraum ist mit einer separaten elektronischen Schließanlage gesichert
- Es gibt einen Sicherheitsdienst sowie eine Alarmanlage
- Mobile Geräte werden bei Nichtbenutzung in verschlossenen Räumen aufbewahrt
- Die Nutzung mobiler Geräte durch die Mitarbeiter ist besonders geregelt und unterliegt strengen Voraussetzungen

1.2 Zugangskontrolle

Die nachfolgenden Maßnahmen werden ergriffen, um zu gewährleisten, dass Datenverarbeitungssysteme von Unbefugten nicht genutzt werden können:

- Der Zugang zu den Systemen erfolgt auf Basis eines festgelegten Berechtigungskonzeptes
- Für die Anmeldung an sämtlichen Computern wird ein Benutzername und ein Passwort benötigt
- Hardwarefirewall
- Aktueller Virenschutz
- Der Zugang zu den Systemen des Auftraggebers erfolgt ausschließlich über eine gesicherte VPN-Verbindung
- System verfügt über aktuelle Sicherheitspatches, die regelmäßig aktualisiert werden

- Es gibt eine Passwortrichtlinie, deren Durchsetzung auch technisch erzwungen wird
- Bei Abwesenheit oder Inaktivität wird der Bildschirm automatisch gesperrt
- Zu vernichtende Unterlagen bzw. Daten werden datenschutzkonform vernichtet bzw. gelöscht

1.3 Zugriffskontrolle

Die nachfolgenden Maßnahmen werden ergriffen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Benutzernamen werden nur an einzelne natürliche Personen unter Beachtung des zugrundeliegenden Berechtigungskonzeptes vergeben
- Es gibt keine Gruppenkennungen
- Trennung von Zugangsbereichen über entsprechende Berechtigungssysteme
- Hardwarefirewall
- Aktueller Virenschutz

1.4 Trennungskontrolle

Die nachfolgenden Maßnahmen werden ergriffen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Sofern der Auftraggeber dem Auftragnehmer Daten zur Verarbeitung übermittelt, werden die Daten des Auftraggebers werden ausschließlich vom jeweils zuständigen Mitarbeiter bearbeitet und danach sofort gelöscht
- Nutzung eines mandantenfähigen Systems
- Systemseitige logische Trennung von zu unterschiedlichen Zwecken verarbeiteten Daten

1.5 Pseudonymisierung (Art. 32 Abs. 1 a) DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten erfolgt soweit erforderlich in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

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

2.1 Weitergabekontrolle

Die nachfolgenden Maßnahmen werden ergriffen, um zu gewährleisten, dass personenbezogene Daten bei einer elektronischen Übertragung oder während ihres Transports oder auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt

werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Gesicherte Übertragung per SSL (FTPS)
- Möglichkeit der verschlüsselten Weitergabe von personenbezogenen Daten
- Beim Transport von Datenträgern werden diese verschlüsselt

2.2 Eingabekontrolle

Die nachfolgenden Maßnahmen werden ergriffen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung im internen System

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

3.1 Verfügbarkeitskontrolle

Die nachfolgenden Maßnahmen werden ergriffen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Regelmäßige Datensicherungen in Bezug auf die eigenen Systeme
- Unterbrechungsfreie Stromversorgung (APC Smart UPS 700)
- Überwachung des Serverraums
- Die eingesetzten externen Server sind nach DIN 27001 zertifiziert
- Der Auftraggeber ist für die Verfügbarkeit seiner Daten selbst verantwortlich, der Auftragnehmer erhält für die Verarbeitung lediglich Kopien

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

Die nachfolgenden Maßnahmen werden ergriffen, um die Verfügbarkeit von personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen:

- Wiederherstellung durch Backup-Software von NAS oder Band
- In Bezug auf die rasche Wiederherstellbarkeit von Daten des Auftraggebers liegt die Verantwortlichkeit beim Auftraggeber

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

4.1 Auftragskontrolle

Die nachfolgenden Maßnahmen werden ergriffen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Kontrolle durch Vorgesetzte unter Einbeziehung des Datenschutzbeauftragten

- Mitarbeiter handeln nur nach ausdrücklicher Weisung und unter Aufsicht des Auftraggebers
- Eindeutige Festlegung der Befugnisse durch entsprechende Vertragsgestaltung
- Interne Regelungen zur Sicherstellung der weisungsgebundenen Auftragsverarbeitung durch die Mitarbeiter
- Unterauftragnehmer werden nur bei Zustimmung des Auftraggebers eingesetzt

4.2 Datenschutzmanagement

Die nachfolgenden Maßnahmen werden ergriffen, um zu gewährleisten, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird:

- Die Mitarbeiter sind auf das Datengeheimnis verpflichtet
- Es ist ein Datenschutzbeauftragter schriftlich bestellt
- Stellenbeschreibungen zur Festlegung von Aufgaben
- Zentrale Löschung von nicht mehr benötigten Daten des Auftraggebers wird regelmäßig geprüft und überwacht

4.3 Incident-Response-Management

Die nachfolgenden Maßnahmen werden ergriffen, um zu gewährleisten, dass der Auftragnehmer seinen Plichten aus dem Datenschutzrecht zeitnah und effektiv nachkommt:

- Standardisierte Abläufe für die Erfüllung von Betroffenenrechten
- Notfallplan
- Richtlinien zum Datenschutz

4.4 Datenschutzfreundliche Voreinstellungen

Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass durch Voreinstellung nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist.