Anlage 1 zur Vereinbarung zur Auftragsdatenverarbeitung:

Technische und organisatorischen Maßnahmen (§ 9 BDSG und Anlage)

Entsprechend den Erfordernissen des Gesetzgebers in § 11 Abs. 2 Nr. 3 BDSG sind vom Auftragnehmer im Rahmen der Verarbeitung der Daten des Auftraggebers die nach § 9 BDSG (und Anlage) zu treffenden technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes festzulegen.

Diese Anlage zur zwischen den Parteien bestehenden Vereinbarung zur Auftragsdatenverarbeitung kommt diesen Erfordernissen nach und konkretisiert die Anforderungen der Ziff. 6 der Vereinbarung zur Auftragsdatenverarbeitung.

1. Zutrittskontrolle:

Welche Maßnahmen ergreifen Sie, um Unbefugten den Zutritt zu Datenverarbeitungs-anlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren?

Ergriffene Maßnahmen:

- Festlegung der zugangsberechtigten Personen
- Revisionsfähigkeit der Zugangsberechtigungen
- Einsatz eines Zugangskontrollsystems, Schlüsselregelung und aktuelle Schlüsselliste
- Protokollierung der Zu- und Abgänge
- Empfang / Pförtner
- Closed Shop-Betrieb (Kein Besucherverkehr im Server-Bereich)

2. Zugangskontrolle:

Welche Maßnahmen ergreifen Sie, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

Ergriffene Maßnahmen:

- Festlegung der nutzungsberechtigten Personen
- Identifikation und Authentifizierung der Benutzer
- Verschlüsselung der zu übertragenden Daten
- Protokollierung der Benutzer und deren Aktivitäten
- Passwortrichtlinie (bzgl. Länge, Änderungsintervall, etc.)
- Verwendung von passwortgeschützten Bildschirmschonern
- Regelungen / Voraussetzungen zur Telearbeit

3. Zugriffskontrolle:

Welche Maßnahmen ergreifen Sie, um dafür Sorge zu tragen, 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?

Ergriffene Maßnahmen:

- Identifikation und Authentifizierung der Benutzer
- Maschinelle Überprüfung der Berechtigungen
- Einführung zugriffsbeschränkender Maßnahmen (z. B. nur Leseberechtigung)
- Einsatz von Verschlüsselungsverfahren
- Zentrale Vergabestelle von Benutzerrechten

4. Weitergabekontrolle:

Welche Maßnahmen ergreifen Sie, um dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist,

Ergriffene Maßnahmen:

- Festlegung der nutzungsberechtigten Personen
- Identifikation und Authentifizierung der Benutzer
- Verschlüsselung der zu übertragenden Daten
- Passwortrichtlinie (bzgl. Länge, Änderungsintervall, etc.)
- Verwendung von passwortgeschützten Bildschirmschonern
- Regelungen / Voraussetzungen zur Telearbeit

5. Eingabekontrolle:

Welche Maßnahmen ergreifen Sie, um dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind?

Ergriffene Maßnahmen:

- Protokollierung der Eingaben, Veränderungen und Löschungen
- Speicherung des Veranlassers

6. Auftragskontrolle:

Welche Maßnahmen ergreifen Sie, um dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können?

Ergriffene Maßnahmen:

- Klare Vertragsgestaltung und -ausführung
- Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
- Sorgfältige Auswahl des Auftragnehmers

7. Verfügbarkeitskontrolle:

Welche Maßnahmen ergreifen Sie, um dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind?

Ergriffene Maßnahmen:

- Backup-Systeme zur Wiederherstellung verlorener Daten
- Testen der Wiederherstellung
- Notfallkonzept mit Wiederanlaufplan
- USV (Unterbrechungsfreie Stromversorgung)
- Redundante Leitungsversorgung
- Notstromaggregat
- Brandmelder
- Brandschutz- und Katastrophenordnung
- Dokumentiertes Datensicherungskonzept
- Zentrale Datensicherung
- Räumlich getrennte Aufbewahrung der erstellten Datensicherungen
- Objektsicherung insb. der Serverräume
- Virenschutzkonzept
- Klimatisierung

8. Trennungskontrolle:

Welche Maßnahmen ergreifen Sie, um dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können?

Ergriffene Maßnahmen:

- Datenspeicherung wird mit dem Zweck der Datenerhebung versehen (z. B. durch Dateibezeichnung)
- Mandantentrennung - Logische Trennung der Daten (z. B. unterschiedliche Dateiverzeichnisse)

_____

Ort, Datum

_____

Unterschrift Auftragnehmer