Anlage 3 – Technische und organisatorische Maßnahmen / Datenschutzkonzept

Technische und organisatorische Maßnahmen zur Datensicherheit

Der Auftragsnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

1.) Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- Alarmanlage mit Aufschaltung auf ein Sicherheitsunternehmen
- Regelung für die Vergabe von Zutrittsberechtigungen
- Elektronisches Zugangskontrollsystem
- Für die Mitarbeiter gelten abgestufte Zutrittsregelungen
- Besucher dürfen nur in Begleitung von berechtigten Mitarbeitern in die Sicherheitsbereiche eintreten
- Protokollierung der Besucher
- Wartungstechniker arbeiten grundsätzlich unter Aufsicht
- Reinigung der Sicherheitsbereiche erfolgt unter Aufsicht

2.) Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Funktions- und Rollenkonzept
- Userbezogene Passwortvergabe
- Passwortrichtlinien (Mindestens 8 Zeichen, Kombination aus Buchstaben, Sonderzeichen, Ziffern, sowie die Nutzung von Groß- und Kleinschreibung)
- Externer Zugang für Mitarbeiter nur über gesicherte und verschlüsselte VPN-Anbindung
- Regelmässiger Passwortwechsel
- Identifikation und Authentifikation von Benutzern
- Sperrung bei Fehlversuchen

3.) **Zugriffskontrolle**

Maßnahmen, die 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:

- Berechtigungskonzept
- Getrennte Benutzerkonten für Administratoren und Sachbearbeitung
- Hinterlegte Notfallpasswörter
- Akten- und Datenträgervernichtung durch ein zertifiziertes Unternehmen mit Entsorgungsnachweis
- Protokollierung der Systemnutzung

4.) **Weitergabekontrolle**

Maßnahmen, die gewährleisten, 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.

- Festgelegte Wege und Verfahren der Übermittlung
- Abgesicherte Übermittlung
- Sichere Datenübertragung zwischen Server und Clients
- Verschlüsselte Ablage von Daten

5.) **Eingabekontrolle**

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

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Aufbewahrungsfristen für Revision und Nachweiszwecke

6.) **Auftragskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Regelungen der Zuständigkeiten und Verantwortlichkeiten
- Auswahl der Auftragnehmers unter Sorgfallsgesichtspunkten
- Dokumentation aller Aufträge

7.) **Verfügbarkeitskontrolle**
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in den Serverräumen
- Virenschutz
- Firewalls
- Lizenzüberwachung
- Brandschutzeinrichtungen, Rauchverbot
- Regelmäßige Datensicherung, Backup-Konzept
- Plan für zu ergreifende Sofortmaßnahmen bei einem Notfall

8.) **Trennungsgebot**
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Trennung von Produktiv- und Testsystemen
- Berechtigungskonzept

Unsere Technische und organisatorische Maßnahmen (TOM) sind jederzeit einzusehen unter:

https://www.set.de/datenschutz