# Anlage 3 – Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO:

## 1. Vertraulichkeit

### Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Alarmanlage mit Bewegungs- und Einbruchmeldern sowie Anschluss an Wachdienst
- Videoüberwachung der Zugänge
- Elektronisches Zugangskontrollsystem mit Schließsystem und Sicherheitsschlössern
- Restriktive Schlüsselregelung
- Personenkontrolle beim Pförtner / Empfang
- Sorgfältige Auswahl von Reinigungspersonal [1]
- Sorgfältige Auswahl von Sicherheits-/Wachpersonal [1]
- Protokollierung von Besuchern [1]

[1] Besucher und fremde Dienstleister dürfen sich nur in Begleitung von Personal in den relevanten Räumlichkeiten aufhalten.

### Zugangskontrolle

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

- Authentifikation für Mitarbeiter nur mit Benutzername und Passwort
- Strenge Passwortregeln für Mitarbeiter
- Umfassende Protokollierung
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls und IDS
- Einsatz von Verschlüsselung und VPN-Technologien
- Getrennte Netzbereiche für Administrations- und Wartungszwecke

### 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.

- Restriktive Berechtigungsregelungen
- Umfassende Protokollierung
- Einsatz von Aktenvernichtern
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern
- Sichere Löschung von Datenträgern vor Wiederverwendung

#### Trennung

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Firmen-Daten von Kunden-Daten strikt getrennt
- Trennung von Produktiv- und Testsystemen

#### Pseudonymisierung & Verschlüsselung

Maßnahmen, die sicherstellen, dass Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr oder schwer einer spezifischen betroffenen Person zugeordnet werden können.

- Kurze Vorhaltezeiten von Log-Dateien
- Reduktion von Log-Dateien auf das Nötigste

### 2. Integrität

#### 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.

- Berechtigungssystem sowie Protokollierung der Eingabe, Änderung und Löschung von Daten

#### 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.

- Einsatz von Verschlüsselung und VPN-Technologien

- Authentifizierung

## 3. Verfügbarkeit und Belastbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Notstromdiesel-Aggregat
- Feuer- und Rauchmeldeanlage mit Anschluss an Wachdienst
- Feuerlöschgeräte in Serverräumen
- Geräte zur Überwachung von Temperatur in Serverräumen
- Klimaanlage in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Backup- und Recovery-Strategie
- Notfallpläne
- Serverräume über der Wassergrenze
- Automatische Überwachungssysteme (Monitoring) kritischer Systeme
- Incident Management

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

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

- Verpflichtung der Mitarbeitern und Subunternehmern auf die EU-DSGVO
- Maßnahmen gemäß 2., 3. und 4. der TOM sowie des AV-Vertrages
- Verarbeitung ausschließlich in der Bundesrepublik Deutschland, einem Mitgliedsstaat der

  Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum