

## **Allgemeine technische und organisatorische Maßnahmen der Invitario GmbH nach Art. 32 Abs. 1 DSGVO**

Der Auftragnehmer betreibt den Betrieb der Internet-Dienstleistung Invitario ausschließlich auf der Infrastruktur des auf externes Server-Hosting spezialisierten Sub-Auftragsverarbeiters Amazon Web Services EMEA SARL (AWS) am Standort Frankfurt am Main. In den Räumlichkeiten des Auftragnehmers selbst werden keine personenbezogenen Daten von Teilnehmern gespeichert oder verarbeitet.

- **Informationen zu den TOM für das externe Server-Hosting sind abrufbar unter:**  
<https://aws.amazon.com/de/compliance/data-center/controls/>
- **Die von Invitario eingesetzten Sub-Auftragsverarbeiter sind abrufbar unter:**  
<https://support.invitario.com/portal/kb/articles/sub-auftragsverarbeiter>

Der Auftragnehmer verschlüsselt sämtliche personenbezogenen Daten in der Internet-Dienstleistung Invitario mit Hilfe des AWS Key Management System sicher (256bit), so dass ein unberechtigter Zugriff auf diese Daten ausgeschlossen ist.

### **Darüber hinaus ergreift der Auftragnehmer folgende Maßnahmen:**

#### **1. Zutrittskontrolle**

Maßnahmen, um zu verhindern, dass Unbefugte räumlichen Zutritt zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden:

- Schlüsselvergabe an Mitarbeiter mit Übergabeprotokoll
- Türsicherung (elektrische Türöffner, in Boden und Decke verbautes Balkenschloss
- Doppeltes Sicherheitsschloss an der Bürotür
- Sorgfältige Auswahl von Dienstleistern und Sub-Auftragsverarbeitern

#### **2. Zugangskontrolle**

Maßnahmen, um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können:

- Alle Systeme sind passwortgeschützt
- Abgesicherter Zugang des Entwicklungs- und Verwaltungsbereichs mit einem Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge)
- Organisatorische Maßnahmen bei Beendigung eines Dienstverhältnisses mit einem Mitarbeiter (Zugang wird gelöscht)
- Einrichtung eines Benutzerstammsatzes pro Anwender
- Die Übertragung von Daten erfolgt über eine per SSL verschlüsselte Verbindung

#### **3. Zugriffskontrolle**

Es besteht eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung.

#### **4. Weitergabekontrolle**

Maßnahmen, dass personenbezogene Daten bei der elektronischen Übertragung oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.

Der Austausch von personenbezogenen Daten erfolgt ausschließlich innerhalb der Systeme des Auftragnehmers sowie ggf. deren Sub-Auftragsverarbeiter. Zwischen den einzelnen Systemen werden die Daten entweder lokal oder über eine per SSL verschlüsselte Datenverbindung übertragen.

Personenbezogene Daten werden im Zuge der Weitergabe und Verarbeitung nicht verändert und bleiben unversehrt, vollständig und aktuell. Der Auftragnehmer unternimmt alles Notwendige, um zu verhindern, dass Daten verfälscht werden oder falsche Daten verarbeitet werden. Gleichzeitig ist gewährleistet, dass Änderungen an Daten nachvollzogen werden können.

## **5. Eingabekontrolle**

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind. Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet und nur vom Teilnehmer, dem Auftraggeber (und dessen Anwendern) sowie durch den Anwender-Support von Invitario erstellt und/oder bearbeitet werden. Jede Veränderung wird mit dem Nutzer sowie einem Zeitstempel dokumentiert. Darüber hinaus erfolgt die Protokollierung über Logfiles.

## **6. Auftragskontrolle**

Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer. Der Auftragnehmer gewährleistet durch die nachstehenden Maßnahmen, dass die im Auftrag zu verarbeitenden Daten nur entsprechend der Auftragsbestätigung verarbeitet werden:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsbestätigung)
- Kriterien zur Auswahl des Auftragnehmers
- Vertraulichkeits- und Datenschutzvereinbarung mit Dienstleistern

## **7. Verfügbarkeitskontrolle**

Maßnahmen, um personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen, sind hier abrufbar: <https://aws.amazon.com/de/security/>

## **8. Trennungskontrolle**

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken: Die Systeme des Auftragnehmers werden von mehreren Mandanten gleichzeitig genutzt (Mandantenfähigkeit) und gewährleisten eine logische Trennung der Daten der Mandanten. Gleichzeitig besteht eine physikalische Trennung der Systeme nach Funktion in Entwicklungssystem, Testsystem und Produktivsystem.

Daten der Zahlungsabwicklung werden vom Auftragnehmer nicht verarbeitet oder gespeichert. Die Verarbeitung erfolgt ausschließlich über das durch den Käufer ausgewählte Zahlungsmittel. Invitario speichert lediglich Zeitpunkt sowie den Status der Transaktion