Anhang A zum Auftragsverarbeitungsvertrag

DATENSICHERHEIT

Dieser Anhang A gilt nur insoweit, als Asensus im Rahmen der Dienstleistungen Kundendaten erlangt.

1. **ÜBERBLICK**

a. Zugang zu Kundendaten. Asensus erkennt an, dass es im Zuge der Erbringung eines Dienstes für den Kunden gemäß den Bedingungen des Vertrags Zugang zu Kundendaten haben oder erhalten kann.

b. Datensicherheitsprogramme. Asensus verpflichtet sich, die in diesem Anhang A aufgeführten administrativen, technischen und physischen Sicherheitsmaßnahmen zu implementieren, um die Kundendaten vor versehentlicher oder unrechtmäßiger Vernichtung, Verlust, Zugriff auf oder Veränderung von Kundendaten im Besitz oder unter der Kontrolle von Asensus zu schützen.

c. Datensicherheitsrichtlinien. Asensus unterhält Richtlinien und Standards für den Schutz von Kundendaten, die aus branchenüblichen Rahmenwerken stammen und einheitliche Sicherheits- und Datenschutzstandards für die Geschäftstätigkeit von Asensus festlegen. Diese Richtlinien müssen mit ISO27001/2 oder einem anderen allgemein anerkannten Industriestandard übereinstimmen, der auf Asensus als Service Provider anwendbar ist.

d. Unterauftragnehmer von Dritten. Asensus ist dafür verantwortlich, dass seine Unterauftragnehmer, die über Kundendaten verfügen, Datensicherheits- und Datenschutzprogramme unterhalten, die mindestens so streng sind wie die eigenen Programme von Asensus in Bezug auf den jeweiligen Service, mit dem der Unterauftragnehmer beauftragt wurde, und die den allgemein anerkannten Industriestandards und -praktiken entsprechen. Asensus unterhält ein Risikomanagementprogramm, das sich auf die Identifizierung, Bewertung und Validierung der Sicherheitskontrollen von Asensus konzentriert.

2. **SICHERHEITSMAßNAHMEN**

Asensus unterhält angemessene Datenschutz- und Sicherheitsmaßnahmen für Kundendaten. Zu diesen Maßnahmen gehören unter anderem die folgenden:

- Identitäts- und Zugriffsmanagementkontrollen (IDAM)
- Kontrollen zur Verhinderung von Datenverlusten (DLP)
- Verschlüsselung & Pseudonymisierung von relevanten Daten
- Formaler Plan zur Reaktion auf Vorfälle (IRP) und Richtlinie zur Meldung von Datenverletzungen
- Richtlinien Management mit regelmäßigen Überprüfungen

Die von Asensus durchgeführten technischen und organisatorischen Maßnahmen sind in Asensus-ScheduleC-TOMs_DE.pdf aufgeführt.