mooncare

Unsere Sicherheitsverfahren

Wir legen grössten Wert darauf, ein vertrauenswürdiger Partner für unsere Kunden zu sein. Sicherheit ist daher ein grundlegendes Thema für tipee AG.

Sämtliche Software von tipee wird als Software-as-a-Service (SaaS) angeboten. Das heisst, wir übernehmen die Verantwortung für alle mit der Nutzung der Applikationen verbundenen Aspekte der Datensicherheit und Verfügbarkeit.

1. Gesetzeskonformität

Als Anbieter von Applikationen für seine Kundschaft übernimmt tipee die Rolle eines Auftragsbearbeiters im Sinne des Bundesgesetzes über den Datenschutz (DSG). tipee verpflichtet sich, die nach diesem Gesetz zu erfüllenden Anforderungen einzuhalten, und erklärt hier im Sinne der Transparenz die getroffenen organisatorischen und technischen Sicherheitsmassnahmen. In der «Vereinbarung über die Bearbeitung von Personendaten», die auf seiner Website verfügbar ist, wird genau beschrieben, wie tipee in seiner Eigenschaft als Auftragsbearbeiter mit Personendaten umgeht.

2. Entwicklung und Hosting in der Schweiz

Die Applikationen von tipee werden von den eigenen Entwicklern des Unternehmens in der Schweiz entwickelt. Die Lösungen und die darin enthaltenen Personendaten werden in Rechenzentren von ISO 27001-zertifizierten Dienstleistern in der Schweiz oder in Europa gehostet.

3. Datensicherheit

Die Daten werden während der Übertragung mithilfe des TLS-Protokolls verschlüsselt. Statische Daten, Benutzerkennungen und Back-ups werden ebenfalls mittels geeigneter Technologien verschlüsselt, die stets auf dem neuesten Stand gehalten werden.

4. Vertraulichkeit

Die Daten werden streng voneinander getrennt, um zu gewährleisten, dass die Informationen jeder Kundin und jedes Kunden vertraulich behandelt werden. Die Architektur unserer Applikationen garantiert, dass die Daten mittels spezieller Datenbanken und spezifisch abgegrenzter Bereiche geschützt werden. Ohne ausdrückliche Zustimmung unserer Kundinnen und Kunden werden keine Informationen an Dritte übertragen oder weitergegeben.

Unsere Mitarbeitenden sind vertraglich zur Wahrung des Berufsgeheimnisses verpflichtet.

5. Verfügbarkeit

Alle Bestandteile unserer Infrastruktur sind aufgrund der Redundanz unserer Systeme ausfallsicher. Unsere Dienste werden an 365 Tagen im Jahr rund um die Uhr von unserem Supportteam überwacht. Warnmeldungen werden Tag und Nacht umgehend bearbeitet. Unsere Systemwiederherstellungsverfahren versetzen uns in die Lage, unsere Dienste nach einem grösseren Vorfall rasch wiederherzustellen.

6. Zugriffskontrolle

Der Zugriff unserer Kundinnen und Kunden auf die Applikationen ist durch eine Kombination aus Benutzername und Passwort geschützt. Darüber hinaus führen wir in unseren verschiedenen Applikationen nach und nach die 2-Faktor-Authentifizierung (2FA) ein.

Mit den von tipee entwickelten Applikationen kann genau festgelegt werden, auf welche Daten jede Benutzerin und jeder Benutzer zugreifen kann. Es liegt in der Verantwortung unserer Kundinnen und Kunden, Richtlinien für die Verwaltung von Passwörtern zu formulieren sowie deren ordnungsgemässe Anwendung und die angemessene Konfiguration der Benutzerberechtigungen sicherzustellen.

Der Zugriff der Mitarbeitenden auf die verschiedenen Systeme von tipee wird systematisch durch 2-Faktor-Authentifizierung geschützt. Ausserdem wird der Zugriff durch Anwendung des Least-Privilege-Prinzips – d. h. Mitarbeitende erhalten nur die Berechtigungen, die sie wirklich benötigen – beschränkt.

7. Back-ups

Um das Risiko eines Datenverlusts weitestgehend zu mindern, wird stündlich ein Back-up der Datenbanken unserer Applikationen durchgeführt und die Wiederherstellung wird regelmässig getestet.

Die Back-ups werden an verschiedenen Standorten gespeichert und gemäss unserer Richtlinie zur Datenspeicherung aufbewahrt.

8. Systemupdates

Unsere Systeme werden durch Updates laufend aktualisiert. Dank der Redundanz unserer Systeme sowie unserer Verfahren können Wartungsarbeiten im Allgemeinen ohne Betriebsunterbruch durchgeführt werden. Ist eine Abschaltung unserer Systeme unvermeidbar, werden unsere Kundinnen und Kunden vorab per E-Mail benachrichtigt.

9. Interne Organisation

tipee hat Sicherheitsrichtlinien und -verfahren festgelegt, mit denen sich alle Mitarbeitenden vertraut machen müssen. Neu eingestellte Mitarbeitende müssen eine Schulung zum Thema Cybersicherheit absolvieren. Zudem werden alle Mitarbeitenden regelmässig über bewährte Vorgehensweisen auf diesem Gebiet aufgeklärt.

Der Beauftragte für IT-Sicherheit ist unmittelbar der Geschäftsleitung unterstellt. Ausserdem wurde ein Datenschutzbeauftragter ernannt.

10. Pflichten von tipee

Gemäss den gesetzlichen Datenschutzanforderungen führt tipee ein Verzeichnis seiner Bearbeitungstätigkeiten sowie ein Verzeichnis von Sicherheitsvorfällen.

Die Grundsätze des **Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen** werden auf sämtliche neu entwickelte Software angewendet. Falls erforderlich, werden auch Datenschutz-Folgenabschätzungen durchgeführt.