Technische und Organisatorische Maßnahmen (TOMs)

gem. Art. 32 DSGVO

Die im Folgenden beschriebenen technischen und organisatorischen Maßnahmen (TOMs) gelten für alle von der Beppler Ventures UG (haftungsbeschränkt) (fortan „Seatti“) bereitgestellten Standard-Serviceangebote, es sei denn, der Kunde ist für die Sicherheits- und Datenschutz-TOMs verantwortlich. Die beschriebenen Maßnahmen richten sich insbesondere nach Art. 28 Abs. 3 lit. c & Art. 32 DSGVO sowie nach Kapitel 3 (Technische und Organisatorische Maßnahmen) u. 5 (Qualitätssicherung und sonstige Pflichten des Auftragnehmers) dieses Vertrags, welche die Rahmenvorgaben der DSGVO aufgreifen. Die Struktur der Maßnahmen orientiert sich nach dem Vorschlag der Aufsichtsbehörden und leitet sich direkt aus den Maßgaben des Art. 32 DSGVO ab. Diese sind unterteilt in Maßnahmen zur Sicherstellung der

- Vertraulichkeit
- Integrität
- Verfügbarkeit und Belastbarkeit
- Regelmäßigen Überprüfung, Bewertung und Evaluierung

Risikoermittlung

Seatti implementiert den Grundsatz Privacy by Design von Beginn an. Das Design der Prozesse und Systeme richtet sich insbesondere nach den Prinzipen der Pseudonymisierung und Minimierung. Daten werden lediglich im für die Erbringung der spezifischen Dienstleistung minimal erforderlichen Ausmaß und Detailgrad zweckgebunden erhoben und pseudonymisiert.

Die Nutzungsdaten (Workspace Buchungen) der Seatti Services werden lediglich im Zusammenhang mit einer pseudonymisierten User ID gespeichert und verarbeitet. Eine Zuordnung personenbezogener Daten findet ausschließlich innerhalb der Client-Systeme statt und ist für Seatti nicht einsehbar. Eingabedaten aus der Arbeitsplatzplanung werden lediglich mit dieser User ID verknüpft und geben keinen weiteren Aufschluss über personenbezogene Daten.

Der Service wird als Cloud-gehostete Software zur Verfügung gestellt. Jegliche Infrastruktur zur Datenverarbeitung ist physisch ausgelagert an AWS als unterstützenden Nebendienstleister i.S.v. Kapital 7.6 des vorliegenden Vertrags. Dabei wird jeweils sichergestellt, dass die Datenspeicherung im Territorium der EU stattfindet und genutzte Server entsprechend stationiert sind (Frankfurt a.M.). AWS garantiert in deren Data Processing Addendum (DPA), dass ausschließlich die gewählte Serverregion für Datenverarbeitungen genutzt werden, solange nicht aktiv anders vom Auftraggeber initiiert. Das DPA dient außerdem zur DSGVO-konformen Ergänzung der Standardvertragsklauseln für die Zusammenarbeit mit US-Dienstleistern und entspricht aktueller Empfehlungen der EuGH Rechtsprechung, um auch nach Aussetzen des US-Privacy-Shields durch den EuGH maximal möglichen Schutz der Daten zu gewährleisten.

Seatti Mitarbeiter fungieren vollkommen remote. Da personenbezogene Daten niemals auf lokalen Endgeräten gespeichert werden oder direkt einsehbar sind, stellen unbefugten physische Übergriffe ein geringes Risiko dar.

Alle im Folgenden aufgeführten technischen und organisatorischen Maßnahmen werden zentral dokumentiert und allen Mitarbeitern zur Verfügung gestellt.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Seatti verfügt nicht über eigene physische Einrichtungen zur Speicherung oder Verarbeitung von Daten. Datenverarbeitungsanlagen werden wie zuvor beschrieben von etablierten Drittanbietern in Anspruch genommen. Es werden niemals personenbezogene Daten auf anderen Geräten als diesen der Drittanbieter gespeichert. Daher ist der physische Zutritt zu Endgeräten oder jeglicher anderer Hardware im Hoheitsbereich von Seatti nicht relevant für den Schutz personenbezogener Daten.

AWS als Datencenter bietet umfangreiche Sicherheitsvorkehrungen zur Compliance mit der DSGVO. Dabei sind mehrere Standards implementiert, u.a. ISO 27001 für technische Maßnahmen, ISO 27017 für Sicherheit in der Cloud und ISO 27018 für Datenschutz in der Cloud. Im AWS GDPR DPA gibt AWS zudem weitere Zusicherungen:

- Daten werden ausschließlich in der exakt instruierten Weise verarbeitet
- AWS pflegt ausführliche technische und organisatorische Maßnahmen
- Bei Sicherheitsvorfällen werden AWS Kunden unmittelbar nach Kenntnisnahme über Vorfälle informiert

Die Zutrittskontrolle zu AWS Rechenzentren sowie alle weiteren von AWS implementierten technischen und organisatorischen Maßnahmen sind detailliert unter https://aws.amazon.com/de/compliance/data-center/controls/ aufgeführt.

1.2. *Zugangskontrolle*

Digitale Zugänge zu den Speichermedien der personenbezogenen Daten sind generell vor fremden Zugriffen mittels passwortgeschützter Zugänge und von einem verschlüsselten Passwort-Manager zufällig generierter Passwörter zu schützen. Zugangsdaten und insb. Passwörter dürfen niemals lokal, sondern ausschließlich in einem SOC2-zertifizierten Passwort-Management Tool gespeichert werden. Auch das Teilen von neu angelegten oder gemeinsamen Zugängen erfolgt niemals unverschlüsselt über Standard-Kommunikationskanäle, sondern ausschließlich mittels der eingesetzten Passwort-Management Software. So werden Benutzerzugänge zentral verwaltet, dokumentiert und deren Gültigkeit regelmäßig überprüft. Grundsätzlich müssen Initialpasswörter, direkt nach deren Erhalt geändert und in einem privaten Passwort-Container in dem zertifizierten Passwort-Management Tool gespeichert werden. E-Mails werden lediglich über die zum Unternehmen gehörende und TLS-verschlüsselte Domain versendet und gelesen. Zudem werden Bildschirmarbeitsplätze nach zwei Minuten automatisch gesperrt und müssen durch erneute Authentifizierung entsperrt werden.

1.3. Zugriffskontrolle

Eine für den Betrieb erforderliche, auf ein Minimum reduzierte Anzahl an Administratoren, welche Benutzerzugänge und -rollen verwalten können, soll einen minimal möglichen Zugriffsumfang garantieren. Zudem werden für unterschiedliche Aufgabenprofile dezidierte Nutzerrollen erstellt, mit denen einzelnen Nutzern nur die minimal erforderlichen Nutzungs- und Zugangsberechtigungen erteilt werden. Generell sollen keinerlei personenbezogene und vertrauliche Daten lokal oder in Papierform überführt oder aufbewahrt werden. Der Zugriff auf Datenbanken sowie die Eingabe, Änderung und Löschung von Daten werden mittels Amazon aws Sevices Log protokolliert und sind nur durch Administratoren einsehbar.

1.4. Trennungskontrolle

Seatti Software ist mandantenfähig und alle kundenbezogenen Daten werden in einem eigenen Mandanten in einem zentralen Datenverarbeitungssystem verwaltet. Datensätze sind dabei mit einer Mandanten-ID versehen, welche zur Authentifizierung und eindeutigen Abgrenzung dienen. Mandanten können ausschließlich für sie authentifizierte Daten in ihrer Benutzeroberfläche einsehen und ggf. in dem zur Verfügung gestellten Umfang bearbeiten.

1.5. Pseudonymisierung

Grundsätzlich werden nur die minimal erforderlichen Daten zur Erbringung unserer Services erhoben (Privacy by Design). Die gespeicherten Daten sind keiner natürlichen Person zuordenbar, da das einzige Mittel zur Identifikation eine pseudonymysierte User ID ist. Diese ist niemals mit anderen von Seatti gespeicherten Daten auf eine Person zurückführbar. Zuordnungsdaten, welche eine eindeutige Identifizierung zulassen könnten, werden ausschließlich vom Auftraggeber und / oder seiner Partner verwaltet. Jede Übermittlung von Daten zwischen diesen Parteien und Seatti unterliegt der TLS Verschlüsselung. Sollten Daten jeglicher Art zu Analysezwecken in andere Datenverarbeitungssysteme transferiert werden, werden diese zuvor vollständig anonymisiert.

2. Integrität

2.1. Weitergabekontrolle

Personenbezogene Daten sollen die aws Cloud grundsätzlich nicht verlassen. Auch für Analysezwecke werden die Daten in der Cloud Umgebung ausgewertet oder vor einer Übertragung vollständig anonymisiert. Falls dies erforderlich ist, muss eine Weitergabe zuvor mit dem Datenschutzbeauftragten abgesprochen werden, entsprechende Maßnahmen zur Verschlüsselung getroffen werden und die Übertragung protokolliert und dokumentiert werden.

2.2. Eingangskontrolle

Die Bearbeitung von Daten wird im aws System Log protokolliert und ist jederzeit für die Systemadministratoren einsehbar. Lediglich die benannten Systemadministratoren sind zur Datenbearbeitung berechtigt. Diese haben nur über individuelle Zugänge Zugriff, wodurch protokollierte Aktivitäten eindeutig zugeordnet werden können. Weitere Leserechte, die über den für den automatisierten Betrieb erforderlichen Rahmen hinausgehen, werden nur im minimal benötigten Ausmaß und nach Einsicht des Datenschutzbeauftragten vergeben.

3. Verfügbarkeit und Belastbarkeit

Ein zentralisierter Cloud Backup Plan inkl. konfigurierter Sicherheitsrichtlinie garantiert regelmäßige und automatisierte Backups über alle aws Services hinweg und erstellt Sicherheitskopien aller Anwendungen sowie Snapshots der genutzten Datenbanken. Logging und Monitoring erlauben zusätzlich die regelmäßige Überprüfung der Backup-Sicherung. Die elektrischen Anlagen unseres Datenzentrums von AWS sind so gestaltet, dass diese vollständig redundant und mit einer Notstromversorgung ausgestattet sind, um rund um die Uhr unbeeinträchtigt von Ausfällen sind.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Maßnahmen

Die hier aufgeführten Maßnahmen werden jährlich, gemeinsam mit einem Datenschutzexperten einer unabhängigen Anwaltskanzlei auf deren Aktualität und Wirksamkeit überprüft. Nach jeder Prüfung werden die TOMs entsprechend angepasst und alle Mitarbeiter über die Anpassungen informiert. Datenschutzrichtlinien sowie TOMs werden zentral dokumentiert und sind für alle Mitarbeiter jederzeit zugänglich. Ebenfalls werden die Zugänge der Systemadministratoren und alle weiteren Benutzerzugänge und deren jeweilige Zugriffsberechtigungen zentral dokumentiert.

4.2. Incident-Response-Management

Sicherheitsvorfälle können zu jeder Zeit telefonisch oder per Mail beim Datenschutzbeauftragten (siehe 4.5 TOMs) gemeldet werden. Dieser leitet die Meldung unverzüglich an die nach 4.1 (TOMs) dokumentierten Systemadministratoren weiter, um direkt Maßnahmen einleiten.

4.3. Datenschutzfreundliche Voreinstellungen

Daten werden nur in einem Ausmaß erhoben, welches für den jeweiligen Zweck der Erbringung unserer Dienstleitungen nötig ist. Zusätzlich werden Daten stets pseudonymisiert gespeichert und lediglich in Klienten-Systemen mit Zuordnungsdaten verknüpft.

4.4. Auftragskontrolle

Unterauftragnehmer im Sinne von Kapitel 6 des AV werden nur nach Unterzeichnung eines AV und nach Einsicht in die technischen und organisatorischen Maßnahmen des jeweiligen Auftragnehmers zur Datenverarbeitung zugelassen. Eine weitere Voraussetzung ist die Sicherstellung eines erreichbaren Datenschutzbeauftragten des Auftragnehmers. Des Weiteren wird nach Beendigung eines Auftrags sichergestellt, dass alle zuvor übergebenen Daten vollständig gelöscht werden.

4.5. Datenschutzbeauftragter

Gem. des Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU ist die Bestellung eines Datenschutzbeauftragten erst ab 20 Mitarbeitern, welche mit der Datenverarbeitung betraut sind, erforderlich. Dazu zählen wir alle in Voll- und Teilzeit beschäftigten Mitarbeiter unseres Unternehmens. Aktuell wird diese Grenze nicht erreicht und somit kein Datenschutzbeauftragter gestellt. Sobald die Grenze in Zukunft überschritten wird, werden Vertragspartner umgehend über den dann zu bestellenden Datenschutzbeauftragten informiert.

Für jegliche datenschutzbezogene Themen steht zur Verfügung:

Johannes Eppler
Sendlinger Str. 35
D-80331 München
johannes@seatti.co
+49 1512 108 97 43