Seatti

Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung

(AV-Vertrag)

gem. Art. 28 DSGVO

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen

und

Seatti UG (haftungsbeschränkt)

vertreten durch

Johannes Eppler
Chief Product Officer Seatti
johannes@seatti.co

im Folgenden: **Auftraggeber**

im Folgenden: **Auftragnehmer**

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer ist Anbieter einer Software für die Verwaltung hybrider Arbeitsplätze, die vom Auftraggeber als cloud-based SaaS-Dienstleistung genutzt wird. Die Parteien haben einen Vertrag über die Nutzung der Software abgeschlossen.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag (im Folgenden „Hauptvertrag“).

2.2 Dauer

Die Verarbeitung beginnt mit Unterschrift des Hauptvertrags und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

3 Art, Zweck und Betroffene der Datenverarbeitung:

3.1 Art der Verarbeitung

Personenbezogene Daten im Sinne der DSGVO werden lediglich in Form einer pseudonymisierten User-ID direkt durch den Auftragnehmer verarbeitet. Jedoch kann der Zugriff auf weitere personenbezogene Daten nicht ausgeschlossen werden. Konkret können bei IT-, Support und Projektmanagement-Aufgaben Tätigkeiten anfallen wie:

- Anlage oder Modifikation von Systembenutzern via Adminclient (direktes Editieren der Tabelle) inkl. Zuweisung von Rollen, Domänen und Gruppen nach Vorgaben des Auftraggebers
- Durchsicht von Logfiles oder Datenbanktabellen im Störungs- oder Präventiv-Wartungsfall, die personenbezogene Daten von Systembenutzern enthalten können
- Arbeiten mit einzelnen Assets im Störungsmeldungsfall (Support-Anfrage), die je nach Verwendung durch den Auftraggeber personenbezogene Informationen enthalten können

Die Verarbeitung und Nutzung der Daten findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Grundsätzlich werden mit US-Dienstleistern, welche in einem Unterauftragsverhältnis i.S.v

Absatz 7 stehen, Datenverarbeitungsabkommen in Ergänzung zu weiterhin gültigen Standardvertragsklauseln abgeschlossen. Dies gilt auch, wenn deren Services zur Datenverarbeitung ausschließlich innerhalb EU-Territorium stattfinden.

3.2 Zweck der Verarbeitung

Der genauere Zweck der Verarbeitung ist in der Leistungsbeschreibung des Hauptvertrages geregelt.

3.3 Art der Daten

Es werden folgende Daten verarbeitet:

- Microsoft Company-ID (pseudonymisiert)
- Microsoft User-ID (pseudonymisiert)
- Input Workspace-Buchungsdaten

Grundsätzlich kann der Zugriff auf personenbezogene Daten von Systembenutzern (Login-Informationen wie Vorname, Nachname, Login-Name, Email-Adresse, auf Wunsch des Auftraggebers auch Titel, Geschlecht und Sprache) bei der Durchführung der im Absatz 3.1 aufgeführten Verfahren nicht ausgeschlossen werden.

3.4 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Systembenutzer der Seatti Services
- Mitarbeiter des Auftraggebers

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei

Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5 Sicherheit der Verarbeitung

(1) Die im Anhang 1 beschriebenen Technischen und Organisatorischen Maßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(4) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

7 Unterauftragsverhältnisse

(1) Wenn und soweit der Auftragnehmer zur Erbringung der vertraglich vereinbarten Leistungen Unterauftragnehmer einsetzen möchte und wenn nicht ausgeschlossen werden kann, dass diese Unterauftragnehmer im Rahmen ihrer Tätigkeit eine Kenntnisnahme-Möglichkeit von Daten des Auftraggebers haben, darf der Auftragnehmer den Unterauftragnehmer nur und erst dann beauftragen und eine Kenntnisnahme von Daten des Auftraggebers ermöglichen, wenn er den Auftraggeber in Textform konkret und im Detail über die Punkte in Punkt 7.2 informiert hat, dem Auftraggeber Gelegenheit zum Einspruch (siehe Punkt 7.3) gegeben hat und der Auftraggeber innerhalb der Einspruchsfrist keinen Einspruch erhoben hat. Unterauftragnehmer, welche bereits zum Zeitpunkt des Vertragsschlusses in einem Unterauftragsverhältnis zu Seatti stehen, sind unter Anlage 2 aufgeführt.

(2) Die Information des Auftragnehmers nach Punkt 7.1 muss mindestens in konkreter und detaillierter Form enthalten:

a. die Identität des Unterauftragnehmers,
b. die spezifischen Leistungen, die der Unterauftragnehmer für den Auftragnehmer erbringen soll, und
c. die Garantien bzw. Versicherungen des Unterauftragnehmers, dass er die Bestimmungen dieses Auftrags entsprechend einhalten wird.

(3) Der Auftraggeber ist berechtigt, innerhalb von 14 Tagen nach Zugang der Informationen gemäß Punkt 7.2 gegen die Beauftragung eines Unterauftragnehmers in Textform Einspruch zu erheben, soweit dies nicht willkürlich erfolgt.

(4) Wenn und soweit dem Unterauftragnehmer Daten des Auftraggebers zugänglich werden, ist der Auftragnehmer verpflichtet, mit dem Unterauftragnehmer vor der erstmaligen Zugänglichmachung von Daten des Auftragnehmers einen Auftragsverarbeitungsvertrag schriftlich zu vereinbaren, der dem Unterauftragnehmer entsprechende Pflichten auferlegt, wie in dieser Vereinbarung geregelt. Der Auftragnehmer hat auf Anfrage des Auftraggebers eine Kopie des Auftragsverarbeitungsvertrags und Nachweise über die Einhaltung der sich daraus ergebenden Pflichten durch den Unterauftragnehmer zu Verfügung zu stellen. Der Auftragnehmer stellt durch Vereinbarung mit seinem Unterauftragnehmer sicher, dass er zur Offenlegung dieser Informationen gegenüber dem Auftraggeber berechtigt ist und dass der Auftraggeber seine Kontrollrechte gemäß 7. auch unmittelbar gegenüber dem Unterauftragnehmer ausüben kann.

(5) Ungeachtet der Regelungen in Punkt 7.1-7.4 ist der Auftragnehmer für den Unterauftragnehmer vollumfänglich verantwortlich und haftet für die Einhaltung der Verpflichtungen des Unterauftragnehmers gegenüber dem Auftraggeber.

(6) Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Bereitstellung von Rechenzentrumsinfrastruktur, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

8 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom

relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11 Beendigung des Auftrags

(1) Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser des nach Wahl des

Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach entsprechender Aufforderung durch den Auftragnehmer zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer mindestens bis zum Ablauf des dritten Kalenderjahres nach Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber übergeben.

12 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner gegenüber der Person, wobei die Haftung für Schäden zwischen dem Auftraggeber und dem Auftragnehmer nach Massgabe des jeweiligen Verschuldens zu tragen ist.

(2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

Unterschriften

Ort, Datum	Ort, Datum
_____	_____
Auftraggeber	Auftragnehmer

Anlage 1 – Technische und Organisatorische Maßnahmen

Die im Folgenden beschriebenen technischen und organisatorischen Maßnahmen (TOMs) gelten für alle von der Seatti 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 Prinzipien 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 persönlichen 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 Services 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 verlassen die aws Cloud grundsätzlich nicht. 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 Dienstleistungen nötig ist. Zusätzlich werden Daten stets pseudonymisiert gespeichert und lediglich in Klienten-Systemen mit Zuordnungsdaten verknüpft.

4.4. Auftragskontrolle

Unterauftragnehmer im Sinne von Kapitel 7 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. Auch gem. Bundesdatenschutzgesetz (§ 4f BDSG) muss kein Datenschutzbeauftragter bestellt werden, wenn höchstens neun Personen mit der Verarbeitung personenbezogener Daten betraut sind. Eine Ausnahme kann gelten, wenn besonders sensible Daten (beispielsweise Daten über die rassische und ethnische Herkunft oder über politische Meinungen) verarbeitet werden. Die Verarbeitung einer pseudonymisierten User-ID entspricht jedoch keiner besonders sensiblen Datenverarbeitung gem. § 3 Abs. 9 BDSG. Sobald die Grenze in Zukunft überschritten wird oder sich die Sensibilität der Daten erhöht, 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

Anlage 2 – Unterauftragnehmer

Unterauftragnehmer 1: Amazon Web Services

Identität: Amazon Web Services Inc. 410 Terry Avenue North, Seattle, WA 98109-5210, USA
Leistungen: Bereitstellung von Rechenzentrumsinfrastruktur

Die Garantien des Unterauftragnehmers basieren auf dem AWS GDPR-Datenverarbeitungszusatz und den darin enthaltenen Standardvertragsklauseln, bis weitere gesetzliche Vorkehrungen zum Schutz des Datentransfers ins Ausland getroffen werden.
Für alle von AWS in Anspruch genommenen Services wird ausschließlich der Serverstandort Frankfurt, DE verwendet.