

Anlage 1 zum Vertrag vom DATUM

Zwischen der KUNDE

– Auftraggeber –

und der Philipp Uhl Capital UG (haftungsbeschränkt)

– Auftragnehmer –

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag vom DATUM in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten («Daten») des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorie betroffener Personen
Matrikelnummer	Aufzeichnung zwecks Nachverfolgbarkeit von gemeinsamen Aufenthalten im Rahmen von CoronaSchVO.	Studierende
Personenkürzel	Aufzeichnung zwecks Nachverfolgbarkeit von gemeinsamen Aufenthalten im Rahmen von CoronaSchVO.	Mitarbeiter des Auftraggebers

E-Mail-Adresse	Aufzeichnung zwecks Authentifizierung der Administratoren.	Nutzer der Administrationsoberfläche
Name	Aufzeichnung zwecks Identifizierung der Administratoren.	Nutzer der Administrationsoberfläche
IP-Adresse	Aufzeichnung zwecks Nachvollziehbarkeit der Zugriffe	Nutzer der Web-Anwendung

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
2. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen

und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.
4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen:

Ansprechpartner: Philipp Uhl
Telefon: +4915732512036
Email: philipp@tisch.im

7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der

Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.
3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber bei Bedarf die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

1. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
2. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift des Subunternehmens	Beschreibung der Teilleistungen
Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg	Hosting der Datenhaltung und Datenverarbeitung, Hosting der Webpräsenz der Plattform. Die Speicherung und Verarbeitung der personenbezogenen Daten geschieht ausschließlich auf Servern in Deutschland.

3. Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.
4. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
4. Es gilt deutsches Recht.

§9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Aachen, DATUM _____
Ort, Datum

Unterschrift Betreiber

Ort, Datum

Unterschrift Kunde

Anlage 2 – Technische und organisatorische Maßnahmen – zum Vertrag vom DATUM

Zwischen der KUNDE

– Auftraggeber –

und der Philipp Uhl Capital UG (haftungsbeschränkt)

– Auftragnehmer –

Die im Folgenden geschilderten Maßnahmen unterliegen dem technischen Fortschritt und werden stetig weiterentwickelt. Der Auftragnehmer darf solche Maßnahmen alternativ ergreifen, wenn die weiterentwickelten Maßnahmen das vereinbarte Schutzniveau mindestens erreichen und der Auftraggeber rechtzeitig über die Änderungen informiert wird, sowie die Möglichkeit einer Prüfung der Maßnahmen hat.

1. Büroräume des Auftragnehmers:

Es gibt keine Server in den Büroräumen des Auftragnehmers. Alle Server stehen in einem Rechenzentrum in Frankfurt am Main (Deutschland) das von Amazon Web Services betrieben wird.

Zutrittskontrolle

- Das Firmengebäude ist mit Sicherheitsschlössern ausgestattet.
- Jedem Mitarbeiter des Auftragnehmers wird ein Schlüssel für das Firmengebäude sowie ggf. ein Schlüssel zu seinem jeweiligen Büro ausgehändigt.
- Die Vergabe von Schlüsseln wird dokumentiert und regelmäßig überprüft.
- Besucher werden immer durch mindesten einen Mitarbeiter des Auftragnehmers begleitet.

Zugangskontrolle

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

- Alle Systeme sind passwortgeschützt.
- Die Vergabe und Verwaltung von Benutzerrechten für einzelne Systeme erfolgt ausschließlich durch Systemadministratoren.
- Alle Arbeitsgeräte (Notebook, PC, ...), auf denen Kundendaten verarbeitet werden, sind für den jeweiligen Mitarbeiter personalisiert (User), mit Passwort geschützt, haben eine

verschlüsselte Festplatte und verwenden das aktuelle Betriebssystem (Linux) mit jeweils der aktualisierten Version und Firewall.

- Jedes Arbeitsgerät hat einen passwortgesicherten Bildschirmschoner.
- Organisatorische Maßnahmen bei Beendigung eines Dienstverhältnisses mit einem Mitarbeiter:
 - Löschung aller seiner Zugänge.
 - Änderung von Zugangsdaten, auf die der Mitarbeiter Zugriff hatte.

Zugriffskontrolle

Kontrollierter Zugriff auf personenbezogene Daten durch:

- Autorisierte Mitarbeiter des Auftragnehmers
 - Zugangsdaten zur Datenbank werden vom autorisierten Systemadministrator verwaltet und nach dem Prinzip der minimalen Berechtigung vergeben.

Weitergabekontrolle

Die Datenübertragung erfolgt über verschlüsselte Netzwerkverbindungen, die dem aktuellen Stand der Technik entsprechen.

Eingabekontrolle

Protokollierung des Zugriffs (Lesen, Ändern, Löschen) auf personenbezogene Daten.

Auftragskontrolle

(Nicht zutreffend)

Verfügbarkeitskontrolle

(Nicht zutreffend)

Datentrennung

(Nicht zutreffend)

2. Web-Anwendung Tisch.im:

Die über Tisch.im erhobenen Daten werden auf der IT-Infrastruktur der Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg (nachfolgend „AWS“ genannt), in der AWS Verfügbarkeitszone „Frankfurt / Deutschland“ gespeichert. AWS garantiert, die Daten nicht außerhalb der Verfügbarkeitszone zu transferieren. Weitere Informationen unter:

- <https://aws.amazon.com/de/compliance/data-privacy-faq/>
- <https://aws.amazon.com/de/compliance/germany-data-protection/>

Zutrittskontrolle & Zugangskontrolle

Das genutzte Rechenzentrum von AWS erfüllt EU adäquate Standard- und Datenschutz Bedingungen, unter anderem die DIN ISO/IEC 27001 und 27018 Zertifizierung, und ermöglicht Zutritt nur für autorisiertes Fachpersonal des Rechenzentrums. Der Zugang zur Datenverarbeitungsanlage ist durch das Rechenzentrum von AWS geregelt. Weitere Informationen zu den Sicherheitsprozessen des AWS Rechenzentrums finden Sie hier:

- <https://aws.amazon.com/compliance/data-center/data-centers/>
- <https://aws.amazon.com/compliance/data-center/controls/>

Zugriffskontrolle

Kontrollierter Zugriff auf personenbezogene Daten durch:

- Vom Auftraggeber definierte Benutzergruppen
 - Der Zugriff auf die personenbezogenen Daten ist durch ein Login-Verfahren geschützt, bei dem der Nutzer eine E-Mail-Adresse angeben muss. Ist diese E-Mail-Adresse dem System bekannt und autorisiert, so erhält der Nutzer über jene E-Mail-Adresse einen Link, um sich auf der Plattform zu authentifizieren.
 - Vom Auftraggeber definierte Benutzergruppen haben die Möglichkeit, weitere Nutzer zu autorisieren und deren Zugriffsrechte zu verwalten.

Die Datenhaltung befindet sich auf einer zugriffsschlüsselgesicherten Datenbank mit AES-256 Verschlüsselung der Daten.

Weitergabekontrolle

Die Datenübertragung erfolgt über verschlüsselte Netzwerkverbindungen, die dem aktuellen Stand der Technik entsprechen.

Eingabekontrolle

Änderungen/Eingaben von personenbezogenen Daten über die Tisch.im-Plattform werden aufgezeichnet. Zugriffe (erfolgreiche, sowie versuchte) auf die Tisch.im-Plattform werden mit Zeitstempel und IP-Adresse aufgezeichnet.

Auftragskontrolle

- Allgemeine Geschäftsbedingungen und Vereinbarungen zur Auftragsverarbeitung des Unteraufnehmers (AWS).

Die Daten werden physisch in Deutschland gespeichert und nicht in Drittländer übertragen. AWS hat sich dem Auftragsverarbeiter gegenüber innerhalb einer Datenverarbeitungs-Vereinbarung zur Wahrung von Datenschutzstandards nach EU Recht verpflichtet. Die Rechte an den gehaltenen Daten liegen beim Auftragsverarbeiter und nicht bei AWS.

Verfügbarkeitskontrolle

- AWS garantiert eine hochverfügbare Cloud-Infrastruktur.
- Verwendung von Backups (täglich, für die letzten sieben Tage), redundanten Systemen.
- Automatisch skalierende Hosting-Infrastruktur, um erhöhtem Nutzungsaufkommen Stand zu halten.

Datentrennung

- Trennung von Produktiv-, Entwicklungs- und Testsystemen.
- Mandantenfähigkeit des Produktivsystems.

Aachen, DATUM

Ort, Datum

Unterschrift Betreiber

Ort, Datum

Unterschrift Kunde