Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO
[Stand: März 2023]

Vereinbarung

zwischen

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

Thomas Bauer, Speedule

Ernst – Udet – Str.1

85764 Oberschleißheim

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Vertreter gemäß Art. 27 DS-GVO:

Thomas Bauer, Ernst - Udet – Str.1,85764 Oberschleißheim

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/AGB vom April 2021, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom April 2021

Die Erbringung der vertraglich vereinbarten Datenverarbeitung 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. DS-GVO erfüllt sind.

(2)Art der Daten

Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: §10.2 c

(3)Kategorien betroffener Personen

Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Nutzung der Dienste und die Übermittlung von Daten.

3. Technisch-organisatorische Maßnahmen

(1)Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(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 [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1)Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Thomas Bauer, Ernst -Udet- Str.1,85764 Oberschleißheim, info@speedule.org benannt.

(2)Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3)Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

(4)Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5)Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(6)Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(7)Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die

Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(8)Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Strato AG	Pascalstraße 10 10587 Berlin Deutschland	Datenspeicherung Bereitstellung Server

b) der Wechsel des bestehenden Unterauftragnehmers
sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer
bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);
sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

a)die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

b)die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

c)aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

d)eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit

personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) 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.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlage – Technisch-organisatorische Maßnahmen

Speedule hat mit seinem Unterauftragsnehmer (Strato AG - Bereitstellung Server) einen Auftragsverarbeitungsvertrag geschlossen in dem sich dieser zu nachfolgenden Maßnahmen verpflichtet:

1. **Gegenstand und Dauer der Verarbeitung**

   Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Leistungsbeschreibung und AGB (nachfolgend Hauptvertrag), soweit eine Verarbeitung von personenbezogenen Daten durch STRATO AG (nachfolgend Auftragnehmer) als Auftragsverarbeiter für den Kunden als Verantwortlicher (nachfolgend Auftraggeber) gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.Die Dauer der Verarbeitung entspricht der im Vertrag vereinbarten Laufzeit.

2. **Art und Zweck der Verarbeitung**

   2.1. Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags.

   2.2. Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung (siehe hierzu auch Anhang 1 Leistungsbeschreibung) insbesondere im Bereich Cloud-Dienstleistungen, Hosting, Softwareas a Service (SaaS) und IT-Support erforderlichen Zwecke.

3. **Art der personenbezogenen Daten und Kategorien von Betroffenen**

   3.1. Die Art der verarbeiteten Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration,die Nutzung der Dienste und die Übermittlung von Daten. Siehe hierzu auch die Leistungsbeschreibung in Anhang 1.

   3.2. Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration,die Nutzung der Dienste und die Übermittlung von Daten. Siehe hierzu auch die Leistungsbeschreibung in Anhang 1.

4. **Verantwortlichkeit und Verarbeitung auf dokumentierte Weisungen**

   4.1. 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. 4Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung.

   4.2. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem

elektronischen Format (Textform) durch einzelne Weisungen geändert werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden. Eine Unzumutbarkeit liegt insbesondere vor, wenn die Leistungen in einer Infrastruktur erbracht werden, die von mehreren Auftraggebern / Kunden des Auftragnehmers genutzt wird (Shared Services), und eine Änderung der Verarbeitung für einzelne Auftraggeber nicht möglich oder nicht zumutbar ist.

4.3. Die vertraglich vereinbarte Datenverarbeitung findet in der Regel überwiegend in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern nicht zur Erbringung der Leistung der Datentransfer in Drittstaaten erforderlich wird. Für den Fall, dass eine Übermittlung in einen Drittstaat erfolgt, stellt der Auftragnehmer sicher, dass die Voraussetzungen nach Art. 44 ff. DSGVO erfüllt sind.

5. Rechte des Auftraggebers, Pflichten des Auftragnehmers

5.1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor (Verpflichtung nach dem Recht der Europäischen Union oder eines Mitgliedstaates). Dies bezieht sich auch auf Übermittlungen von personenbezogenen Daten an Drittländer oder internationale Organisationen.Besteht eine Verarbeitungspflicht entgegen einer Weisung, so informiert der Auftragnehmer vor der Verarbeitung den Auftraggeber über die entsprechende rechtliche Anforderung.Es sei denn, das betreffende Recht verbietet eine solche Information wegen eines wichtigen öffentlichen Interesses. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, das seine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange auszusetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Die Weisungen sind durch den Auftraggeber zu dokumentieren und mindestens für die Dauer des Auftragsverhältnisses aufzubewahren.

5.2. Der Auftragnehmer unterstützt angesichts der Art der Verarbeitung nach Möglichkeit den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Ansprüche der betroffenen Personen nach Kapitel III der DSGVO. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen, soweit die Unterstützung nicht aufgrund eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

5.3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen

bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen, soweit die Unterstützung nicht aufgrund eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

5.4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und anderen 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. Gleiches gilt für das Sozialgeheimnis, das Fernmeldegeheimnis nach § 3 TTDSG und – in Kenntnis der Strafbarkeit – für die Wahrung von Geheimnissen der Berufsgeheimnisträger nach § 203 StGB. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5.5. 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 für die betroffenen Personen.

5.6. Der Auftragnehmer gewährleistet die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Eine Kontaktmöglichkeit wird auf der Webseite des Auftragnehmers veröffentlicht.

5.7. Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Auftraggeber zurück, sofern nicht nach dem Unionsrecht oder nach dem anwendbaren Recht eines Mitgliedstaates eine Verpflichtung zurSpeicherung der personenbezogenen Daten besteht oder sich aus jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart. Wählt der Auftraggeber die Rückgabe, kann der Auftragnehmer eine angemessene Vergütung verlangen. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

5.8. Machen betroffene Person Schadensersatzansprüche nach Art. 82 DSGVO geltend, unterstützt der Auftragnehmer den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten. Der Auftragnehmer kann hierfür eine angemessene Vergütung verlangen.

6. Pflichten des Auftraggebers

6.1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Durchführung des Auftrags Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

6.2. Im Falle der Beendigung verpflichtet sich der Auftraggeber, diejenigen personenbezogenen Daten vor Vertragsbeendigung zu löschen, die er in den Diensten gespeichert hat.

6.3. Auf Anforderung des Auftragnehmers benennt der Auftraggeber einen Ansprechpartner in Datenschutzangelegenheiten.

7. Anfragen betroffener Personen

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. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8. Maßnahmen zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO

8.1. Der Auftragnehmer ergreift in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und den Schutz für die Rechte und Freiheiten der betroffenen Person gewährleistet. Der Auftraggeber ergreift in seinem Verantwortungsbereich gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

8.2. Die aktuellen technischen und organisatorischen Maßnahmen des Auftragnehmers sind unter folgendem Link einsehbar: https://www.strato.de/agb/tom/. Der Auftragnehmer stellt klar, dass es sich bei den unter dem Link aufgeführten technischen und organisatorischen Maßnahmen lediglich um Beschreibungen technischer Art handelt, welche nicht als Bestandteil dieser Vereinbarung anzusehen sind.

8.3. Der Auftragnehmer betreibt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d) DSGVO.

8.4. Der Auftragnehmer passt die getroffenen Maßnahmen im Laufe der Zeit an die Entwicklungen beim Stand der Technik und die Risikolage an. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das Schutzniveau nach Art 32 DSGVO nicht unterschritten wird.

9. Nachweis und Überprüfung

9.1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht im Einzelfall

Überprüfungen - einschließlich Inspektionen -, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden. Der Auftragnehmer ist berechtigt, eine Verschwiegenheitserklärung vom Auftraggeber und von dessen beauftragten Prüfer zu verlangen, welche dem Auftraggeber aber nicht daran hindern soll, selbst Nachweis gegenüber der für ihn zuständigen Aufsichtsbehörde zu erbringen. Unmittelbare Wettbewerber des Auftraggebers oder Personen, die für unmittelbare Wettbewerber des Auftraggebers tätig sind, kann der Auftragnehmer als Prüfer ablehnen.

9.2. Als Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten reicht dem Auftraggeber inder Regel die vorliegende Zertifizierung nach ISO 27001 aus. Das jeweils aktuelle Zertifikat stellt der Auftragnehmer auf seiner Webseite zur Verfügung.

9.3. Sofern der Auftraggeber auf Basis tatsächlicher Anhaltspunkte berechtigte Zweifel daran geltend macht,dass die vorbezeichneten Zertifizierungen zureichend oder zutreffend sind, oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DSGVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung für den Auftraggeber dies rechtfertigen, kann er Vor-Ort-Kontrollen durchführen. Diese können zu den üblichen Geschäftszeiten ohne übermäßige Störung des Betriebsablaufs in der Regel nach Anmeldung (wenn nichteine Kontrolle ohne Anmeldung erforderlich erscheint, weil andernfalls der Kontrollzweck gefährdet wäre)durchgeführt werden. Das Inspektionsrecht des Auftraggebers hat das Ziel, die Einhaltung der einem Auftragsverarbeiter obliegenden Pflichten gemäß der DSGVO und dieses Vertrages zu überprüfen. Der Auftragnehmer wird aktiv an der Durchführung der Kontrolle mitwirken.

9.4. Für Informationen und Unterstützungshandlungen kann der Auftragnehmer eine angemessene Vergütung verlangen, soweit die Kontrolle nicht wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

10. Subunternehmer (weitere Auftragsverarbeiter)

10.1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.

10.2. Die aktuell eingesetzten weiteren Auftragsverarbeiter sind in Anhang 2 aufgeführt. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.

10.3. Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben.

10.4. Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem sachlichen Grund innerhalb von14 Tagen nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer erhoben werden.Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die

beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist (mindestens 14 Tage) nach Zugang des Einspruchs einstellen.

10.5. Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer,seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen. Der Auftragnehmer stellt insbesondere durch regelmäßige Überprüfungen sicher, dass die weiteren Auftragsverarbeiter die technischen und organisatorischen Maßnahmen einhalten.

11. Haftung und Schadensersatz

11.1. Im Fall der Geltendmachung eines Schadensersatzanspruches durch eine betroffene Person nach Art. 82DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.

11.2. Die zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung zur Auftragsverarbeitung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter nach Art 82 DSGVO, außer soweit ausdrücklich etwas anderes vereinbart ist.

12. Vertragslaufzeit, Sonstiges

12.1. Die Vereinbarung beginnt mit dem Abschluss durch den Auftraggeber. Sie endet mit Ende des letzten Vertrages unter der jeweiligen Kundennummer. Sollte eine Auftragsverarbeitung noch nach Beendigung dieses Vertrages stattfinden, gelten die Regelungen dieser Vereinbarungen bis zum tatsächlichen Ende der Verarbeitung.

12.2. Der Auftragnehmer kann die Vereinbarung nach billigem Ermessen mit angemessener Ankündigungsfrist ändern. Insbesondere behält er sich ausdrücklich vor, die vorliegende Vereinbarung einseitig zu ändern, sofern sich wesentliche rechtliche Änderungen im Bezug auf diese Vereinbarung ergeben. Der Auftragnehmer wird den Auftraggeber über die Bedeutung der geplanten Änderung gesondert hinweisen und darüber hinaus dem Auftraggeber eine angemessene Frist zur Erklärung eines Widerspruchseinräumen. Der Auftragnehmer weist den Auftraggeber in der Änderungs-Ankündigung darauf hin, dass die Änderung wirksam wird, wenn er nicht binnen der gesetzten Frist widerspricht. Im Falle eines Widerspruchs durch den Auftraggeber, steht dem Auftragnehmer ein außerordentliches Kündigungsrecht zu.

12.3. Der Auftraggeber erkennt diese Vereinbarung als Teil der AGB https://www.strato.de/agb/ über die/das von ihm gebuchte/n Produkt/e an. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten

einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht.

12.4. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragnehmers. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes. Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Deutschland.

12.5. 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 DSGVO liegen.

Anhang 1 Leistungsbeschreibung

Domain

Leistungsbeschreibung: Wenn Sie bei uns nur eine Domain bestellen, kümmern wir uns um die Konnektierung und die Registrierung Ihrer Domain bei der zuständigen Registry. Zudem ist die Aufrechterhaltung der Registrierung Vertragsbestandteil.Art der personenbezogenen Daten: Domain, Stammdaten (Name, Adresse, E-Mail, Telefonnummer)Kategorien betroffener Personen: Mitarbeiter, Besucher Ihrer Webseite

Mail

Leistungsbeschreibung: Wenn Sie bei uns ein Mailprodukt bestellen, erhalten Sie eine E-Mail-Adresse mit persönlicher Domain. Wir legen für Sie ein Postfach an, auf das Sie mittels Web zugreifen oder inverschiedene Web Clients einbinden können. Des Weiteren können Sie Termine und Aufgaben erstellen undKontakte verwalten. Zudem gehört auch ein konfigurierbarer Spamfilter zum Produkt. Zusätzlich haben Sie die Möglichkeit, das Produkt Mailarchivierung zu erwerben und somit Ihre Mails revisionssicher zuspeichern. Wenn Sie das Produkt Webmailer erworben haben, können Sie zudem Termine und Aufgabenerstellen und Kontakte verwalten.Art der personenbezogenen Daten: Mails, Kontakte, Termine, Domain Kategorien betroffener Personen: Mitarbeiter, Besucher der Webseite

HiDrive Cloud Speicher

Leistungsbeschreibung: Unser Cloud-Speicher ermöglicht die Speicherung Ihrer Daten in unserem Rechenzentrum, sodass Sie von überall und jederzeit auf die Daten zugreifen können. Sie können dabei, je nach bestelltem Paket, z.B. mehrere Nutzer anlegen oder andere Konfigurationen vornehmen. Sie können zudem Freigaben auf bestimmte Ordner erteilen und diese verwalten.Art der personenbezogene Daten: Daten, die Sie in der Cloud speichern Kategorien betroffener Personen: Mitarbeiter

Hosting

Leistungsbeschreibung: Wenn Sie bei uns ein Hosting Paket bestellen, gehören zu unserer Leistung die Registrierung und Konnektierung der Domain sowie die Zurverfügungstellung des Webspaces und der Datenbanken. Inbegriffene Leistungen sind SSL-Zertifikate, SiteLock Scan und Mail. Mittels SSL-Zertifikat werden die Daten zwischen Ihrer Webseite und dem Webserver verschlüsselt übertragen. SiteLock Scan hilft Ihnen dabei, Ihren Webspace frei von Schadsoftware zu halten, indem Ihre Webseite gescannt wird und Sie im Falle eines Fundes informiert werden.Art der personenbezogenen Daten: Inhaltsdaten der Webseite, Domain, Daten E-Mail (siehe unter Mailprodukt), Daten Ihrer Webseitbesucher Kategorien betroffener Personen: Mitarbeiter, Besucher der Webseite

Server

Leistungsbeschreibung: Sie können virtuelle und dedizierte Server bei uns bestellen. Je nach gewähltem Produkt, stellen wir Ihnen eigene Hardware oder einen nur geteilten Speicherplatz zur Verfügung. Wir bieten Ihnen von Root Servern (bei welchem Sie die volle Administrationsfreiheit haben) bis hin zu gemanagten Servern (bei welchen wir die Administration übernehmen) unterschiedliche Serverprodukte an. Die konkrete Datenverarbeitung hängt zudem davon ab, welches Betriebssystem Sie wählen und wie die Virtualisierung umgesetzt wird.Art der verarbeiteten Daten: Daten, die Sie auf dem Server speichern Kategorien betroffener Personen: Mitarbeiter, Besucher der Webseite

Webshop

Leistungsbeschreibung: Wenn Sie einen Webshop bestellt haben, verarbeiten wir in der Regel auch Daten Ihrer Kunden. Das Produkt ermöglicht es Ihnen, Waren etc. online zu verkaufen. Vertragsbestandteil sind demnach auch viele Funktionen und Plug-Ins, die für Sie hilfreich sind, um Ihre Waren erfolgreich zu verkaufen. Dazu gehört z.B. die Möglichkeit Newsletter zu versenden oder sich Statistiken anzeigen zulassen sowie die Implementierung unterschiedlicher Zahlungsanbieter oder Anbindung von Social Media.Art der verarbeiteten Daten: Daten Ihrer Kunden (Zahlungsdaten, Adressdaten, etc.), Daten zu Ihrem Shop Kategorien betroffener Personen: Mitarbeiter, Kunden, Besucher der Webseite

weitere SaaS Produkte

Wir bieten zudem noch weitere Software-as-a-Service Produkte an. Hierzu gehören z.B. - aber nicht abschließend - Online Marketing Tools, die Möglichkeit, sich eine Webseite mittels Homepage-Baukastens zu erstellen oder erstellen zu lassen oder auch der Vertrieb von Office Anwendungen.Art der verarbeiteten Daten: Daten, die Sie in den Diensten speichern Kategorien betroffener Personen: Mitarbeiter, Kunden, Besucher der Webseite

Anhang 1 zur Vereinbarung zur Auftragsverarbeitung - Genehmigte Subunternehmer /weitere Auftragsverarbeiter

Stand: 05.09.2022

Subunternehmer	Land	Adresse	Kurzbeschreibung der Leistung
we22 Solutions GmbH	Deutschland	Otto-Ostrowski-Straße 7, 10249 BerlinStrato	Homepage-Design-Service; Entwicklung, Wartung und Pflege des Homepagebaukastens
e Pages GmbH	Deutschland	Pilatuspool 2, 20355Hamburg	Entwicklung, Wartung und Pflege der Webshopsoftware
Ionos SE	Deutschland	Elgendorfer Straße 7, 56410 Montabaur	Bereitstellung, Betrieb und Wartung von Produkten;insbesondere:Betrieb,Wartung und Pflege des AutoUpdaters für Apps (Installatron) Bereitstellung der Umgebung für den Betrieb der Strato Mail-Archivierung Betrieb der Plattform zur Bereitstellung von dedizierten und virtuellen Servern.
Dropsuite Ltd.	Singapur	PTE, Ltd. 01-12 Block 71, Ayer Rajah Crescent, Singapore 139951	Entwicklung, Wartung, Pflege und Betrieb der Strato Mail-Archivierungsoftware
Virtuozzo International GmbH	Schweiz	Vordergasse 59, 8200Schaffhausen, Schweiz	Software für V-Server und Support
rankingcoach GmbH Im	Deutschland	Im Mediapark 6B, 50670Köln	Anwendungen zur Verbesserung der Sichtbarkeit einer Website in Suchmaschinen
Hewlett-Packard GmbH	Deutschland	Herrenberger Strasse 140, 710 Böblingen	Betrieb und Support von V-Server
Acronis Germany GmbH	Deutschland	Landsbergerstrasse 105, 80339 München	Support Backup Produkt

SiteLock, LLC	USA	8701 East Hartford Drive Suite 200, Scottsdale AZ 85255 US	Erkennung und Beseitigung von Malware
Cyren GmbH	Deutschland	Heidestraße 10, 10557Berlin	Spamfilter für E-Mail
Plesk International GmbH	Schweiz	Vordergasse 59, 8200Schaffhausen, Schweiz	Bereitstellung und Nutzung der Server Administrations Software
ServerGuard24 GmbH	Deutschland	Melbweg 8, 53127 Bonn	Monitoring Software Server
Open-Xchange GmbH	Deutschland	Olper Hütte 5f, 57462Olpe	Nutzung von OX App Suite und OX Premium Postfächern

Speedule selbst hat zudem folgende Maßnahmen beim Zugriff auf oben genannte Systeme ergriffen:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

• Zugangskontrolle

• Keine unbefugte Systembenutzung, Speedule verwendet sichere Kennwörter (monatlicher Kennwortwechsel) und automatische Sperrmechanismen.

• Speedule begrenzt den Zugriff auf die Systeme auf Personen, die mit der Wartung der Systeme vertraut sind (Vertraulichkeitsvereinbarung)

• Alle Geräte die Speedule zum Zugriff verwendet, sind mit Sicherheitssoftware geschützt und nur mit sicheren Passwörtern zugänglich.

2. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs.1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

• Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

• Auftragskontrolle

•Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers

• Auswahl weiterer Auftragnehmer nach geeigneten Garantien

•Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern

• Abschluss einer Vereinbarung zur Auftragsverarbeitung mit Speedule