Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

ViralSpoon UG (haftungsbeschränkt)
Baseler Platz 6
60329 Frankfurt am Main

Der vorliegende Auftragsverarbeitungsvertrag („**AVV**“) gilt für die Verarbeitungsmaßnahmen personenbezogener Daten durch die ViralSpoon UG (haftungsbeschränkt) (auch als „**wir**" oder „**Auftragnehmer**" bezeichnet), die gegenüber Kunden (nachfolgend „**Auftraggeber**“ oder „**Sie**“) in Erfüllung des Hauptvertrages erbracht werden.

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen gemäß dem zwischen ihnen geschlossenen Lizenzvertrag über die Nutzung von ViralSpoon (im Folgenden: "**Hauptvertrag"**). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung ("**DSGVO**"). Zur Erfüllung der Anforderungen der DSGVO an derartige Konstellationen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (auch „**Vertrag**“), der mit Unterzeichnung bzw. Wirksamwerden des Hauptvertrages zustande kommt.

1. Gegenstand/Umfang der Beauftragung

(1) Im Rahmen der Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages hat der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend "**Auftraggeberdaten**"). Diese Auftraggeberdaten verarbeitet der Auftragnehmer im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO.

(2) Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt in der in den Anlagen beschriebenen Art sowie in dem dort spezifizierten Umfang und Zweck. Der Kreis der von der Datenverarbeitung betroffenen Personen wird dargestellt. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

(3) Ob die Leistungen des Auftragnehmers für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO geeignet sind, bedarf einer Risikobewertung durch den Auftraggeber.

(4) Dem Auftragnehmer ist eine von den in den Anlagen genannten Verarbeitungen abweichende Verarbeitung von Auftraggeberdaten untersagt.

(5) Die Verarbeitung der Auftraggeberdaten findet grds. im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Sollte es eine Verlagerung der Auftragsverarbeitung in ein Drittland geben, bedarf dies der vorherigen Zustimmung des Auftraggebers und erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Der Auftraggeber stimmt bereits mit Abschluss dieses Auftragsverarbeitungsvertrages der Verarbeitung personenbezogener Daten durch die in den Anlagen genannten Subunternehmen zu.

(6) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen. Gleiches gilt für alle Tätigkeiten, bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit Auftraggeberdaten in Berührung kommen.

2. Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten im Rahmen der Beauftragung und im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber hat das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "Weisungsrecht"). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Weisungen werden vom Auftraggeber grundsätzlich schriftlich oder in elektronischer Form (E-Mail ausreichend) erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer in elektronischer Form zu bestätigen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

3. Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden "Mitarbeiter" genannt), zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO). Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

(3) Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DSGVO, insbesondere die in Anlage 2 zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten.

(4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(5) Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der technischen und organisatorischen Maßnahmen nachweisen.

(6) Der Auftragnehmer und die bei oder für ihn Beschäftigten ist berechtigt, die gem. des Hauptvertrags zu erbringenden Leistungen und damit auch die Verarbeitung personenbezogenen Daten aus seiner Hauptverwaltung, seinen Betriebsstätten, Niederlassungen oder aus dem Home- und Mobile-Office heraus erbringen zu lassen, sofern sichergestellt ist, dass die Schutzmaßnahmen, die in diesem AVV definiert werden, hierbei eingehalten werden.

4. Informations- und Unterstützungspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte, wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens aber innerhalb von 48 Stunden in Schriftform oder elektronischer Form informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Diese Meldungen sollten jeweils zumindest die in Art. 33 Absatz 3 DSGVO genannten Angaben enthalten.

(2) Der Auftragnehmer wird den Auftraggeber im o.g. Falle bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen Anforderung innerhalb angemessener Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind.

5. Sonstige Verpflichtungen des Auftragnehmers

(1) Der Auftragnehmer ist, sofern die Voraussetzungen des Art. 30 DSGVO auf ihn zutreffen, verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gem. Art. 30 Absatz 2 DSGVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen.

(3) Der Auftragnehmer bestätigt, dass er – soweit eine gesetzliche Verpflichtung hierzu besteht – einen Datenschutzbeauftragten bestellt hat.

(4) Sollten die Auftraggeberdaten 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, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DSGVO liegt.

6. Subunternehmerverhältnisse

(1) Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachfolgend „Unterauftragnehmer") erbringen lassen. Der Auftragnehmer informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen sachlicher Gründe der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

(3) Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden TOM ein gleichwertiges Schutzniveau aufweisen.

(4) Der Auftragnehmer hat mit den in Anlage 1 genannten Unternehmen Subunternehmerverhältnisse begründet, denen der Auftraggeber mit Abschluss dieses Auftragsverarbeitungsvertrages zustimmt. Die in der Anlage 1 genannten Unternehmen können durch den Auftragnehmer ergänzt oder verringert werden. Sollte der Auftragnehmer einen weiteren Subunternehmer hinzufügen, so fügt er diese in die Anlage 1 ein. Sollte der Auftraggeber nicht mit der Hinzufügung des weiteren Subunternehmen einverstanden sein, so hat er die Möglichkeit, innerhalb von 3 Wochen nach Zufügung gegenüber dem Auftragnehmer zu widersprechen. Widerspricht der Auftraggeber der Hinzufügung des weiteren Subunternehmen, so hat der Auftragnehmer das Recht den Hauptvertrag inkl. sämtlicher Anlagen innerhalb von 1 Woche zu kündigen, sollte keine alternative Lösung zur weiteren Zusammenarbeit gefunden werden und sollte die Hinzufügung des weiteren Subunternehmen für das Unternehmen des Auftragnehmers von besonderer Wichtigkeit sein.

(5) Mit den Unterauftragnehmern hat der Auftragnehmer den Anforderungen aus § 6 Abs. 3 entsprechende Auftragsverarbeitungsverträge geschlossen. Mit Wirksamwerden dieses AVV genehmigt der Auftraggeber die vorgenannten Unterauftragnehmer.

(6) Bestandteil der Auftragsverarbeitungsverträge mit den Unterauftragnehmern ist insbesondere auch, dass die Unterauftragnehmer sicherstellen, ihrerseits angemessene und geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO wegen der von ihnen im Auftrag durchgeführten Verarbeitungen personenbezogener Daten getroffen zu haben.

7. Kontrollrechte

(1) Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages zu überzeugen. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers zu den üblichen Geschäftszeiten selbst persönlich bzw. durch

einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(2) Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

8. Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO. Er wird dem Auftraggeber unverzüglich, spätestens aber innerhalb von 14 Werktagen, die gewünschte Auskunft über Auftraggeberdaten geben, sofern der Auftraggeber nicht selbst über die entsprechenden Informationen verfügt.

(2) Macht der Betroffene seine Rechte gemäß Art. 16 bis 18 DSGVO geltend, ist der Auftragnehmer dazu verpflichtet, die Auftraggeberdaten auf Weisung des Auftraggebers unverzüglich, spätestens binnen einer Frist von 7 Werktagen zu berichtigen, löschen oder einzuschränken. Der Auftragnehmer wird dem Auftraggeber die Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen schriftlich nachweisen.

(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

9. Laufzeit und Kündigung

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Er endet damit automatisch mit Beendigung des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung für diesen Vertrag entsprechend. Sollte der Auftragnehmer vor Ablauf des Hauptvertrages keine Auftraggeberdaten mehr verarbeiten, endet dieser Vertrag ebenfalls automatisch.

10. Löschung und Rückgabe nach Vertragsende

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragsnehmer für eine Dauer von 6 Monaten aufzubewahren und auf Verlangen an den Auftragsgeber herauszugeben.

(2) Der Auftragnehmer wird dem Auftraggeber die Löschung elektronisch bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

11. Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. Dies gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

12. Vertraulichkeit & Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen.

(2) Es besteht eine Verschwiegenheitspflicht für die Mitarbeiter des Auftragnehmers und durch ihn beauftragte Dritte. Der Auftragnehmer hat die bei der Verarbeitung von Auftraggeberdaten beschäftigten Personen gemäß Art. 28 Abs. 3 lit. b DSGVO schriftlich auf die Vertraulichkeit zu verpflichten. Dies ist nicht erforderlich, wenn die beschäftigten Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer wird die in dieser Ziffer niedergelegte Verpflichtung schriftlich dokumentieren und sie auf Verlangen des Auftraggebers diesem vorlegen.

(3) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und er diese auf die Einhaltung der geltenden Datenschutzvorschriften zu verpflichten. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Diese in dieser Ziffer geregelten Verschwiegenheitspflichten besteht auch nach der Beendigung des Vertragsverhältnisses fort.

(5) Darüber hinaus ist der Auftragnehmer neben den jeweils geltenden gesetzlichen Bestimmungen (insbesondere § 3 TTDSG, § 203 StGB, §§ 4, 23 GeschGehG sowie ggf. besondere berufsständische Verschwiegenheitspflichten) auch verpflichtet, alle Informationen und Daten, die ihm im Rahmen der vertraglich vereinbarten Leistungen zur Kenntnis gelangen, geheim zu halten und nicht an Dritte weiterzugeben (vertrauliche Informationen). Vertrauliche Informationen sind insbesondere Geschäfts- und Betriebsgeheimnisse, Vertragsschlüsse, technische oder kaufmännische Informationen jedweder Art bzw. anderweitige Angaben, die als vertraulich bezeichnet oder ihrer Natur nach als vertraulich anzusehen sind. Dies gilt insbesondere auch für:

   Namen, Anschriften sowie die persönlichen, rechtlichen und wirtschaftlichen Verhältnisse aller Kunden vom Auftraggeber und die persönlichen, rechtlichen und wirtschaftlichen Verhältnisse vom Auftraggeber und aller anderen für Auftraggeber tätigen Personen.

   Eine Information ist nicht als vertraulich anzusehen, wenn sie zu der Zeit, zu der der Auftragnehmer von der Information Kenntnis erlangt hat, bereits öffentlich bekannt gewesen ist. Ebenso als nicht vertraulich sind solche Informationen anzusehen, die zeitlich später mit Zustimmung des Auftraggebers öffentlich bekannt geworden sind bzw. bekannt gemacht wurden.

(6) Der Auftragnehmer verpflichtet sich, sämtliche Mitarbeiter, die im Rahmen der Tätigkeit für Auftraggeber Kenntnis von vorgenannten vertraulichen Informationen von Auftraggeber erlangen, ebenso wie sich selbst zu verpflichten.

(7) Beauftragt der Auftragnehmer Dritte, hat er dafür Sorge zu tragen, dass die Forderungen der Absätze 1 bis 6 entsprechend umgesetzt werden.

13. Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer iSd § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der elektronischen Form.

(3) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers.

Anlagen

Anlage 1 Festlegungen zum Vertrag

Anlage 2 Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DSGVO)

Anlage 1 – Festlegungen zum Vertrag

Gegenstand und Dauer des Auftrages Übersicht der Anforderungen und Festlegungen	
(1) Hauptvertrag	Lizenzvertrag
(2) Gegenstand des Auftrages	Vollumfassende, plattformübergreifende und KI-gestützte Software zur Erledigung des Social Media Managements – von der Planung bis zum Post der Beiträge.
(3) Zweck der Datenerhebung, Datenverarbeitung oder Datennutzung	Zur Erfüllung der Pflichten des Auftragnehmers aus dem Hauptvertrag werden personenbezogene Daten aus dem Herrschaftsbereich des Auftraggebers durch den Auftragnehmer vollumfänglich i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet, insbesondere soweit jeweils erforderlich erhoben, gespeichert, verändert, ausgelesen, abgefragt, verwendet, offengelegt, abgeglichen, verknüpft und gelöscht. Der Zweck der Verarbeitung hängt damit von dem jeweils im Hauptvertrag beschriebenen Auftrag ab.
(4) Art der Daten	Die von der Verarbeitung betroffenen Kategorien personenbezogener Daten hängen von der Nutzung der Leistungen des Auftragnehmers durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind möglich • Stammdaten (z.B. Namen, Anschriften, Geburtsdaten), • Kontaktdaten (z.B. E-Mail-Adressen, Telefonnummern), • Inhaltsdaten (z.B. Fotografien, Videos, Inhalte von Dokumenten), • Vertragsdaten (z.B. Vertragsgegenstand, Laufzeiten, Kunden), • Zahlungsdaten (z.B. Bankverbindungen, Zahlungsdienstleister), • Nutzungsdaten (z.B. Verlauf Web-Dienste, Zugriffszeiten), • Verbindungsdaten (z.B. Geräte-ID, IP-Adressen, URL-Referrer), und • Standortdaten (z.B. GPS-Daten, IP-Geolokalisierung).
(5) Kreis der Betroffenen	Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der Nutzung der Leistungen des Auftragnehmers durch den Auftraggeber ab. Als Kategorien betroffener Personen kommen dabei in Betracht: • Beschäftigte • Auszubildende und Praktikanten • Bewerber • ehemalige Arbeitnehmer • freie Mitarbeiter • Gesellschafter, Organe der Gesellschaft • Angehörige von Beschäftigten • Kunden / Interessenten • Lieferanten und Dienstleister • Mieter • Geschäftspartner • externe Berater • Besucher • Pressevertreter

Unterauftragnehmer

Nr.	Name des Unterauftragnehmers Anschrift / Land	Gegenstand der Leistung	Verarbeitete personenbezogene Daten
1	STRATO AG Otto-Ostrowski-Straße 7, 10249 Berlin	Hosting	Siehe oben „Art der Daten“
2	OpenAI, L.L.C., 3180 18th Street, San Francisco, California 94110, United States	KI Dienste	Siehe oben „Art der Daten“
3	Microsoft Corporation, One Microsoft Way Redmond, WA 98052-6399 USA	Cloudbasiertes Hosting	Siehe oben „Art der Daten“
4	Twenty Four Twelve Systems Pte. Ltd., #05-16 People's Park Centre,101 Upper Cross Street,Singapore 058357	API Services	Siehe oben „Art der Daten“
5	Google Gemini, Google Ireland Limited Gordon House, Barrow Street Dublin 4 Irland	KI Dienste	Siehe oben „Art der Daten“
6	Canva Pty Ltd Level 1, 110 Kippax St Surry Hills NSW 2010 Australien	IT Services	Siehe oben „Art der Daten“
7	Microsoft Corporation, One Microsoft Way Redmond, WA 98052-6399 USA	KI Dienste	Siehe oben „Art der Daten“
	Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 United States	KI Dienste	Siehe oben „Art der Daten“

Anlage 2 - Technische und organisatorische Maßnahmen

Verantwortliche für die Datenverarbeitung sind gem. Art. 32 DSGVO verpflichtet, technische und organisatorische Maßnahmen zu treffen, durch die die Sicherheit der Verarbeitung personenbezogener Daten gewährleistet wird. Maßnahmen müssen dabei so gewählt sein, dass durch sie in der Summe ein angemessenes Schutzniveau sichergestellt wird. Diese Übersicht erläutert vor diesem Hintergrund, welche konkreten Maßnahmen durch den Auftragnehmer im Hinblick auf die Verarbeitung personenbezogener Daten im konkreten Fall getroffen sind.

Weisungen zu technischen und organisatorischen Maßnahmen

1. Organisation der Informationssicherheit

Es sind Richtlinien, Prozesse und Verantwortlichkeiten festzulegen, mit denen die Informationssicherheit implementiert und kontrolliert werden kann.

Maßnahmen:

x Festlegung der Rollen und Verantwortlichkeiten für Betrieb von Anwendungen und System, Datenschutz und Informationssicherheit.

x Verpflichtung der Mitarbeiter auf Geheimhaltung und Wahrung des Datengeheimnisses

2. Privacy by Design

Privacy by Design beinhaltet den Gedanken, dass Systeme so konzipiert und konstruiert sein sollten, dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird. Wesentliche Elemente der Datensparsamkeit sind die Trennung personenbezogener Identifizierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und die Anonymisierung. Außerdem muss das Löschen von personenbezogenen Daten gemäß einer konfigurierbaren Aufbewahrungsfrist realisiert sein.

Maßnahmen:

x Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

x Die Verarbeitungen und Systeme sind so konzipiert, dass Sie ein DSGVO konformes Löschen der verarbeiteten personenbezogenen Daten ermöglichen und sicherstellen.

3. Privacy by Default

Privacy by Default bezieht sich auf die datenschutzfreundlichen Voreinstellungen / Standardeinstellungen. Inwieweit wurden diese von Ihnen vorgenommen? Beispiel: Bei einem Besuch einer Webseite kann der Besucher erwarten, dass alle Programme zunächst deaktiviert sind, die personenbezogene Daten erheben.

Maßnahmen:

x Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen.

x Trackingfunktionen, die den Betroffenen überwachen, sind standardmäßig deaktiviert.

x Sämtliche Vorbelegungen von Auswahlmöglichkeiten erfüllen die Anforderungen der DSGVO in Bezug auf datenschutzfreundliche Voreinstellungen (z.B. keine Vorbelegungen von Opt-ins).

4. Zugriffskontrolle und Zugangskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten bzw. schutzbedürftigen Informationen und Daten zugreifen können (Beschreibung von systemimmanenten Sicherungsmechanismen, Verschlüsslungsverfahren entsprechend dem Stand der Technik. Bei Online-Zugriffen ist klarzustellen, welche Seite für die Ausgabe und Verwaltung von Zugriffssicherungscodes verantwortlich ist.). Der Auftragnehmer gewährleistet, dass die zur Benutzung von IT-Infrastruktur berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind, und dass personenbezogene Daten bei der Verarbeitung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

Maßnahmen:

x Vermeidung von Gruppenusern.

x Zugriff auf Daten ist eingeschränkt und nur für Berechtigte möglich.

x Anzahl der Administratoren auf das „Notwendigste“ reduziert.

x Passwortrichtlinie, Implementierung komplexer Passwörter.

Weisungen zu technischen und organisatorischen Maßnahmen

5. Kryptographie und / oder Pseudonymisierung

Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes der Vertraulichkeit, Authentizität oder Integrität von personenbezogenen Daten bzw. schutzbedürftigen Informationen.

Maßnahmen, die geeignet sind, eine Identifikation des Betroffenen zu erschweren.

Maßnahmen:

- x Verschlüsselung von Datenträgern (z.B. mobile Festplatten, USB-Sticks etc.).
- x Verschlüsselte Ablage von personenbezogenen Daten.
- x Verschlüsselung von Zugängen zum Netzwerkzugängen und -verbindungen.
- x Einsatz Verfahren zur Anonymisierung von Daten.

6. Schutz von Gebäuden

Verhinderung des unautorisierten physischen Zugriffs auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung. Der Auftragnehmer trifft Maßnahmen, um zu verhindern, dass unbefugte Personen Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten mit denen personenbezogene Daten verarbeitet werden.

Maßnahmen:

- □ Zonenkonzept und Festlegung von Sicherheitsbereichen.
- □ Gebäudesicherung durch Zäune.
- □ Sicherheitsschlösser und Schlüsselverwaltung / Protokollierung der Schlüsselausgabe
- □ Einsatz von Schliess- und Zutrittssystemen (Chipkarten- / Transponder-Schließsystem, Codesicherung etc.).
- □ Alarmanlage.
- □ Videoüberwachung.
- □ Lichtschranken / Bewegungsmelder.
- □ Einsatz von Wachpersonal.
- □ Mitarbeiter- /Besucherausweise.
- □ Regelung für den Umgang mit Besuchern.
- □ Anmeldung für Besucher (Empfang).
- □ Kontrolle von Besuchern (Pförtner/Empfang).
- □ Protokollierung von Besuchern (Besucherbuch).

Weitere umgesetzte Maßnahmen / Erläuterungen: wir haben kein Gebäude :)

7. Schutz von Betriebsmitteln / Informationswerten

Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit der Organisation.

Weisungen zu technischen und organisatorischen Maßnahmen

Maßnahmen:

x Sichere Platzierung der Systeme, so dass Schutz vor Diebstahl gewährleistet ist.

□ Schutz der Betriebsmittel vor Feuer, Wasser oder Überspannung.

□ Ablage von Akten und Dokumente in verschlossenen Büros, Aktenschränken.

x Unterbringung der Server- und Netzkomponenten in gesicherten Räumen, Schränken etc.

□ Regelmäßige Wartung der Betriebsmittel.

□ Sichere Löschung, Vernichtung und Entsorgung von Betriebsmitteln.

Weitere umgesetzte Maßnahmen / Erläuterungen: Also das läuft alles auf nicht eigenen Servern, daher sollte das auch „sicher“ sein

8. Betriebsverfahren und Zuständigkeiten

Sicherstellung des ordnungsgemäßen und sicheren Betriebes von Systemen sowie Verfahren zur Verarbeitung von Informationen.

Maßnahmen:

x Klare Zuordnung von Verantwortlichkeiten für die System- und Anwendungsbetreuung.

x Trennung der Verarbeitung von Daten der einzelnen Mandanten.

x Trennung von Entwicklungs-, Test- und Produktivsystemen.

x Wartungsverträge mit geeigneter Reaktionszeit

9. Datensicherungen

Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:

x Datensicherungskonzept mit regelmäßigen Backups.

□ Auslagerung der Backup in andere Brandzonen.

□ Auslagerung der Backups in andere Gebäude.

□ Regelmäßige Tests der Datensicherung und Wiederherstellung von Daten, Anwendungen und Systemen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Backup läuft auf MS Azure, Wiederherstellung liegt heir quasi bei MS

10. Schutz vor Malware und Patchmanagement

Verhinderung einer Ausnutzung technischer Schwachstellen durch den Einsatz von aktueller Virenschutzsoftware und die Implementierung eines Patchmanagements.

Maßnahmen:

x Regelmäßige Überwachung des Status von Sicherheitsupdates und Systemschwachstellen.

x Regelmäßige Einspielen von Sicherheitspatches und Updates.

Weisungen zu technischen und organisatorischen Maßnahmen

11. Protokollierung und Überwachung

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind. (Sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens 3 Jahre lang durch den Auftragnehmer aufbewahrt.)

Maßnahmen:

x Protokollierung von Zugängen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Für die Zugänge nutzen wir eine Userliste

12. Netzwerksicherheitsmanagement

Es muss ein angemessener Schutz für das Netzwerk implementiert werden, so dass die Informationen und die Infrastrukturkomponenten geschützt werden.

Maßnahmen:

□ Einsatz von Netzwerkmanagementsoftware.

x Einsatz von Firewallsystemen.

□ Einsatz von Intrusion Detection / Intrusion Prevention Systemen.

□ Benutzerauthentifizierung und Verschlüsselung von externen Zugriffen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Cloud Firewall

13. Informationsübertragung

Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft sowie festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten bzw. schutzbedürftiger Informationen sowie Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
(Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)

Maßnahmen:

x Weitergabe von Daten an Dritte nur nach Prüfung der Rechtsgrundlage.

x Sichere Datenübertragung zwischen Client und Server.

x Angemessener Schutz von Emails, die sensible Informationen / Daten beeinhalten.

x Sicherer Transport und Versand von Datenträgern, Daten und Dokumenten.

14. Anschaffung, Entwicklung und Instandhaltung von Systemen

Maßnahmen, die sicherstellen, dass Informationssicherheit ein fester Bestandteil über den Lebenszyklus von Informationssystemen ist.

Maßnahmen:

x Festlegung von sicherheitsspezifischen Regelungen und Anforderungen für den Einsatz neuer Informationssysteme und für die Erweiterung bestehender Informationssysteme.

Weisungen zu technischen und organisatorischen Maßnahmen

15. Lieferantenbeziehungen

Maßnahmen betreffend die Informationssicherheit zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf die Werte des Unternehmens, sollten mit Sublieferanten / Subunternehmern vereinbart und dokumentiert werden.

Maßnahmen:

- □ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit).
- □ Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. DSGVO der Auftragnehmer hat Datenschutzbeauftragten bestellt.
- □ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart.
- □ Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen.
- □ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis.
- □ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.
- □ Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten.
- □ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.

Weitere umgesetzte Maßnahmen / Erläuterungen: Zählen MS/Open AI etc. als Lieferanten?

16. Management von Informationssicherheitsvorfällen

Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall etc.) zu implementieren.

Maßnahmen:

- x Sofortige Information des Auftraggebers bei Datenschutzvorfällen.

17. Informationssicherheitsaspekte des Business Continuity Management / Notfallmanagements

Die Aufrechterhaltung der Systemverfügbarkeit in schwierigen Situationen, wie Krisen- oder Schadensfälle. Ein Notfallmanagement muss dieses sicherstellen. Die Anforderungen bezüglich der Informationssicherheit sollten bei den Planungen zur Betriebskontinuität und Notfallwiederherstellung festgelegt werden.

Maßnahmen:

- □ Einsatz redundanter Systeme.
- □ Einsatz redundanter Systeme an räumlich getrennten Standorten (z.B. Notfall-Rechenzentrum).
- □ Dokumentierte Notfallpläne.
- □ Regelmäßige Tests bzgl. der Wirksamkeit der Notfallmaßnahmen.
- □ Frühzeitige Information des Auftraggebers bei Notfällen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Zukünftig redundante Systeme geplant, derzeit aus kostengründen noch nicht eingerichtet

18. Einhaltung gesetzlicher und vertraglicher Anforderungen

Implementierung von Maßnahmen zur Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen sowie gegen jegliche Sicherheitsanforderungen.

Weisungen zu technischen und organisatorischen Maßnahmen

Maßnahmen:

- □ Sicherstellung der Einhaltung der gesetzlichen Verpflichtungen im Rahmen der Zusammenarbeit.
- □ Rückgabe sämtlicher Daten, Betriebsmittel und Informationswerte an den Auftraggeber bei Vertragsende.
- □ Einrichtung eines Lizenzmanagements.
- □ Geheimhaltungsverpflichtungen mit Mitarbeitern sowie Sublieferanten und Dienstleistern.

Weitere umgesetzte Maßnahmen / Erläuterungen: Lizenzmanagement über SaaS Veertrag?

19. Datenschutzanforderungen und Datenschutzmanagement

Die Privatsphäre sowie der Schutz von personenbezogenen Daten sollte entsprechend den Anforderungen der einschlägigen gesetzlichen Regelungen, anderen Vorschriften sowie Vertragsbestimmungen sichergestellt werden.

Maßnahmen:

- □ Einrichtung einer Datenschutzorganisation.
- □ Bestellung eines Datenschutzbeauftragten.
- □ Verzeichnis der Verarbeitungstätigkeiten.
- □ Datenschutzfolgeabschätzung für Verfahren, die sensible Informationen / Daten verarbeiten.
- □ Durchführung von Datenschutzschulungen.
- □ Aufbau eines Datenschutz-Managementsystems.
- □ Dokumentiertes Datenschutz-Konzept.
- □ Umgesetzte Richtlinien zum Datenschutz.

Weitere umgesetzte Maßnahmen / Erläuterungen: DSVGO nach besteme Wissen und Gewissen umgesetzt

20. Informationssicherheitsüberprüfungen

Es muss regelmäßig überprüft werden, ob die Informationsverarbeitung entsprechend der definierten Sicherheitsmaßnahmen durchgeführt wird. Hierfür wird der Auftragnehmer regelmäßige Prüfungen durchführen. Der Auftragnehmer räumt dem Auftraggeber das Recht ein, regelmäßige Audits / Überprüfungen bei ihm durchzuführen.

Maßnahmen:

- □ Regelmäßige Durchführung von internen Audits zu den Themen Datenschutz- und Informationssicherheit.
- □ Durchführung von Penetrationstests.

Weitere umgesetzte Maßnahmen / Erläuterungen: