Auftragsverarbeitungsvereinbarung

Zwischen

_____

_____

_____

- nachstehend Auftraggeber genannt -

Und

SocialMe GmbH
Hausener Straße 9
89407 Dillingen an der Donau

- nachstehend Auftragnehmer genannt -

§ 1 Gegenstand des Auftrages

(1) Gegenstand des Auftrags ist die Erbringung von Dienstleistungen gemäß des zwischen den Parteien geschlossenen Leistungsvertrages.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers. Bei dem Vertragsgegenstand handelt es sich deshalb um eine Auftragsverarbeitung. Die Parteien sind sich darin einig, dass auf diesen Vertrag die Vorschriften der EU-Datenschutzgrundverordnung (DS-GVO), insbesondere die Vorschriften über die Datenverarbeitung im Auftrag, anzuwenden sind. Der Auftragnehmer erklärt, dass er in der Lage ist, die aufgetragenen Leistungen nach Maßgabe des Art. 28 DS-GVO ordnungsgemäß durchzuführen.

(3) Der Vertrag regelt die datenschutzrechtlichen Maßnahmen im Sinne von Art. 28 DS-GVO und die Rechte und Pflichten des Auftraggebers und des Auftragnehmers zur Erfüllung der datenschutzrechtlichen Anforderungen.

§ 2 Dauer, Laufzeit des Auftrages

(1) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet.

(2) Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt. Eine Kündigung des Vertrags kann nur schriftlich erfolgen.

§ 3 Kategorien von betroffenen Personen

Die Datenverarbeitung betrifft folgende Kategorien von natürlichen Personen:
Beschäftigte, Kunden, Lieferanten, Bewerber oder ggf. weitere Personen, die von den im Leistungsvertrag vereinbarten Dienstleistungen betroffen sein können.

§ 4 Arten der personenbezogenen Daten

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien:
Namen, Adresse, Kontaktinformationen, Bilder, Videos, Benutzerkennungen, weitere Daten, die im Rahmen der im Leistungsvertrag vereinbarten Dienstleistungen verarbeitet werden.

§ 5 Ort der Verarbeitung

Die Datenverarbeitung findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland oder innerhalb der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes statt. Eine Verarbeitung in anderen Staaten ist nur zulässig soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DS-GVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DS-GVO ein angemessenes Datenschutzniveau sichergestellt ist.

§ 6 Kontroll- und Auditrechte des Auftraggebers

(1) Der Nachweis angemessener technischer und organisatorischer Maßnahmen kann auch durch Vorlage von Testaten oder Zertifikaten oder durch eine Zertifizierung bzw. ein Datenschutzaudit einer unabhängigen Einrichtung bzw. eines autorisierten Sachverständigen geführt werden.

(2) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist eine Kontrolle im Sinne des Art. 28 Abs. 3 lit. h DS-GVO in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden könnten.

(3) Die Rechte des Auftraggebers bestehen während der Laufzeit dieser Vereinbarung und darüber hinaus bis zum Eintritt der Verjährung von Ansprüchen aus diesem Vertrag, mindestens jedoch solange der Auftraggeber personenbezogene Daten aus den beauftragten Verarbeitungen speichert.

§ 7 Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung der personenbezogenen Daten sowie für die Ausführung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der getroffenen Auftragsbeschreibung ein Weisungsrecht in Form von Einzelanweisungen über Art, Umfang und Verfahren der Datenverarbeitung sowie über Änderungen der Verarbeitung vor. Die Weisungen betreffen insbesondere aber nicht ausschließlich die datenschutzkonforme Auftragsabwicklung und sonstige Handlungen zur Sicherstellung einer gesetzmäßigen Auftragsabwicklung. Die Weisungen werden schriftlich, in Schriftform oder in einem anderen geeigneten elektronischen Format erteilt. Mündliche Weisungen werden unverzüglich in Schriftform, schriftlich oder in einem elektronischen Format bestätigt.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder gegen andere Datenschutzvorschriften verstößt. Der Auftragnehmer kann die Ausführung der Anweisung bis zu einer Bestätigung durch den Auftraggeber aussetzen. Der Auftraggeber haftet für rechtswidrige Weisungen und stellt den Auftragnehmer insoweit von Schadensersatzansprüchen und sonstigen Forderungen frei.

(4) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

§ 8 Pflichten des Auftragnehmers

(1) Verarbeitungspflichten

Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nicht oder nur nach Weisung des Auftraggebers erteilen. Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen erteilen.

Der Auftragnehmer verpflichtet sich, bei datenschutz- und datensicherheitsrelevanten Vorfällen alle erforderlichen Auskünfte zu erteilen und die Aufklärung derartiger Vorfälle nach Möglichkeit zu unterstützen.

(2) Informationspflichten

Der Auftragnehmer ist verpflichtet, wesentliche Änderungen in den technischen und organisatorischen Verhältnissen, die die Sicherheit und Ordnungsmäßigkeit der Durchführung der Auftragsleistungen herabsetzen, dem Auftraggeber zu melden.

Der Auftragnehmer unterrichtet den Auftraggeber über Kontrollen der Aufsichtsbehörde für den Datenschutz, insbesondere gem. Art. 58 DS-GVO, und über eventuelle Maßnahmen und Auflagen zum Schutz der personenbezogenen Daten.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Der Auftragnehmer teilt dem Auftraggeber Name und Kontaktdaten und Änderungen in der Person des betrieblichen Datenschutzbeauftragten oder, wenn keine Bestellpflicht besteht, den Namen und die Kontaktdaten der sonstigen zuständigen Stelle mit.

(3) Mitwirkungs- und Unterstützungspflichten

Der Auftragnehmer verpflichtet sich, im Rahmen des Art. 28 Abs. 3 lit. e und f DS-GVO, die für das Verzeichnis von Verarbeitungstätigkeiten sowie für die Risikoermittlung und eventuelle Datenschutzfolgenabschätzung erforderlichen Informationen zur Verfügung zu stellen und, soweit es seinen Verantwortungsbereich betrifft, im erforderlichen Umfang bei der Ermittlung der Risiken und einer eventuellen Datenschutzfolgenabschätzung mitzuwirken sowie den Auftraggeber bei der Erfüllung der Rechte der Betroffenen zu unterstützen.

§ 9 Wahrung der Vertraulichkeit und sonstiger Geheimnisse

(1) Personenbezogene und sonstige Daten oder Informationen, die dem Auftragnehmer im Rahmen der Erfüllung dieses Vertrags bekannt werden, darf der Auftragnehmer nur für Zwecke der beauftragten Leistung verwenden. Der Auftragnehmer verpflichtet sich, die Vertraulichkeit und Integrität der personenbezogenen Daten zu wahren und alle ihm im Zusammenhang mit der Übernahme und Abwicklung des Auftrages bekannt werdenden personenbezogenen Daten und sonstige unternehmensinterne Umstände, Daten und Informationen (Betriebsgeheimnisse) vertraulich zu behandeln sowie die im Rahmen dieses Vertrages tätig werdenden Mitarbeiter auch über die Beendigung des Beschäftigungsverhältnisses hinaus auf die Wahrung der Vertraulichkeit schriftlich zu verpflichten und über die Datenschutzpflichten aus diesem Vertrag, die Weisungsgebundenheit der Verarbeitung der Daten und deren Zweckbindung zu belehren. Diese Geheimhaltungspflicht gilt auch über die Beendigung des Vertragsverhältnisses hinaus.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die mit der Auftragsdurchführung beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht.

(3) Der Auftragnehmer verpflichtet sich zur Beachtung aller sonstigen Geheimnisse, soweit diese für die Verarbeitung einschlägig sind, wie des Sozialgeheimnisses, des Fernmeldegeheimnisses und sonstiger Berufsgeheimnisse gem. § 203 StGB sowie zur Verpflichtung und Belehrung der Beschäftigten zur Sicherstellung der Wahrung dieser Geheimnisse.

(4) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über administrative Zugangsdaten und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen. Von den ihm eingeräumten Zugriffsrechten darf der Auftragnehmer nur in dem Umfang Gebrauch machen, der für die Durchführung der Datenverarbeitung erforderlich ist. Die Verpflichtung zur Wahrung der Vertraulichkeit und der sonstigen Geheimnisse gilt auch über die Beendigung dieses Vertrages hinaus.

§ 10 Unterauftragsverhältnisse

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung von Subunternehmern erbracht.

(2) Informationen zu den eingesetzten Subunternehmen können auf der Webseite des Auftragnehmers unter **https://socialme.eu/avv/** eingesehen werden. Der Auftraggeber genehmigt die Beauftragung von Subunternehmern, soweit diese zur Erfüllung der vom Auftragnehmer im Leistungsvertrag vereinbarten Tätigkeiten erforderlich ist. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Änderung bestehender oder Begründung weiterer Unterauftragsverhältnisse mit Subunternehmern befugt. Der Auftragnehmer informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Subunternehmern oder Änderungen bei Unterauftragsverhältnissen. Der Auftraggeber kann in Textform und unter Darlegung eines wichtigen Grundes der Beauftragung des Subunternehmers oder der Änderung innerhalb von 14 Tagen nach Kenntnisnahme widersprechen. Im Fall des begründeten Widerspruchs räumt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Ersetzung des von dem Widerspruch betroffenen Subunternehmers durch einen anderen Subunternehmer ein. Ist dies dem Auftragnehmer nicht möglich oder nicht zumutbar oder dem Auftraggeber nicht zumutbar, ist der jeweilige Vertragspartner berechtigt, den Leistungsvertrag aus wichtigem Grund zu kündigen.

(3) Der Auftragnehmer hat die eingesetzten Unterauftragnehmer sorgfältig auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieses Vertrages zu verpflichten. Die Verpflichtung des Unterauftragnehmers muss den Anforderungen von Art. 28 Abs. 4 DSGVO entsprechen.

(4) Unterauftragsverhältnisse mit Subunternehmern im Sinne dieser Vereinbarung liegen nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt.

§ 11 Mitteilungspflichten bei Störungen und Datenschutzverletzungen

(1) Bei einer Störung der Verarbeitung oder Datenschutzverletzung leitet der Auftragnehmer umgehend alle geeigneten und erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung eines eventuellen Schadens für die Betroffenen und den Auftraggeber ein.

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich über Verstöße gegen Vorschriften zum Schutz der personenbezogenen Daten oder gegen die in dieser Vereinbarung getroffenen Festlegungen zu unterrichten. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder andere Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers, die Auswirkungen auf die betroffenen Personen oder den Auftraggeber nach sich ziehen oder Schaden verursachen können.

§ 12 Rechte der Betroffenen

(1) Für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und zuständig. Der Auftragnehmer darf Rechte der Betroffenen nur nach Weisung des Auftraggebers umsetzen. Der Auftragnehmer unterstützt jedoch den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen.

(2) Anfragen von Betroffenen zu ihren Rechten oder von einem Betroffenen verlangte Auskünfte, Berichtigungen, Löschungen von Daten werden vom Auftragnehmer unverzüglich an den Auftraggeber zur Erledigung weitergeleitet. Auskünfte an Dritte dürfen nur nach Weisung des Auftraggebers erteilt werden oder sind an den Auftraggeber zur Erledigung weiterzuleiten. Ebenso dürfen Auskünfte an Beschäftigte des Auftraggebers nicht unmittelbar an diese, sondern nur über vereinbarten Kontaktpersonen erteilt werden.

§ 13 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer sichert die Einhaltung der in der **Anlage 1** genannten Maßnahmen und Regelungen zu. Diese Maßnahmen gelten als vereinbart und die Beschreibung der Maßnahmen wird Bestandteil dieses Vertrages.

(2) 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.

§ 14 Verfahren nach Beendigung des Auftrages

(1) Nach Abschluss der Verarbeitung, spätestens nach Beendigung dieses Vertrages, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse oder zur Leistungserfüllung hergestellten oder kopierten personenbezogenen oder sonstige vertrauliche Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder in Abstimmung mit dem Auftraggeber datenschutzgerecht zu vernichten oder sicher zu löschen. Test- und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen. Diese Verpflichtung gilt in gleichem Maße auch für eventuell beauftragte Unterauftragnehmer. Unberührt bleiben Daten, deren Löschung aus technischen Gründen nicht möglich ist oder einen unverhältnismäßig hohen Aufwand verursachen würde, sowie Kopien, die zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung oder zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind.

§ 15 Haftung

Für die Haftung gelten die Regelungen des Art. 82 DS-GVO.

§ 17 Anwendbares Recht

(1) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

(2) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort / Datum	Ort / Datum
_____	_____
Unterschrift / Stempel Auftraggeber	Unterschrift/Stempel Auftragnehmer
_____	_____

Anlage 1: Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DS-GVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, werden geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

I. Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden (Gelände, Gebäude, Räumlichkeiten), zu verwehren.

Technische Maßnahmen
☒ Manuelles Schließsystem
☒ Türen mit Knauf Außenseite
☒ Videoüberwachung der Eingänge

Organisatorische Maßnahmen
☒ Schlüsselregelung / Liste
☒ Besucher in Begleitung der Mitarbeiter
☒ Sorgfältige Auswahl von Reinigungspersonal

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer, Papierakten) von Unbefugten genutzt oder eingesehen werden können.

Technische Maßnahmen
☒ Login mit Benutzername + Passwort
☒ Zwei-Faktor-Authentifizierung
☒ Einsatz von Anti-Viren-Software
☒ Einsatz einer Software-Firewall
☒ Automatische Desktopsperre bei Inaktivität

Organisatorische Maßnahmen
☒ Verwalten von Benutzerberechtigungen
☒ Clean Desk-Policy
☒ Zentrale Passwortverwaltung
☒ Richtlinie für Passwörter
☒ Dienstanweisung für Umgang mit mobilen Datenträgern

3. Zugriffskontrolle

Maßnahmen, die geeignet sind, ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems zu verhindern und sicherzustellen, dass Nutzer nur auf die ihrer Berechtigung unterliegenden Daten zugreifen können.

Technische Maßnahmen
☒ Shredder (mind. P3 Cross Cut)
☒ Ordnungsgemäße Vernichtung von Datenträgern

Organisatorische Maßnahmen
☒ Einsatz von Berechtigungskonzepten
☒ Minimale Anzahl an Administratoren
☒ Verwaltung Benutzerrechte durch Administratoren

II. Integrität

1. Weitergabekontrolle

Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass dies überprüft und festgestellt werden kann.

Technische Maßnahmen
☒ Einsatz eines Passwort Managers
☒ Datenaustausch über Cloud
☒ Bereitstellung über verschlüsselte Verbindungen wie https

2. Eingabekontrolle

Maßnahmen, die geeignet sind, nachträglich zu überprüfen und festzustellen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten

III. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und möglichst schnell wieder hergestellt werden können.

Technische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen
☒ RAID System / Festplattenspiegelung

Organisatorische Maßnahmen
☒ Backup & Recovery-Konzept
☒ Einsatz von Cloud-Diensten
☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

IV. Regelmäßige Überprüfung, Bewertung & Evaluierung der Wirksamkeit

1. Datenschutz-Maßnahmen

Maßnahmen, die dem kontinuierlichen Schutz von personenbezogenen Daten dienen.

Organisatorische Maßnahmen
☒ externer Datenschutzbeauftragter
☒ Regelmäßige Schulung der Mitarbeiter zum Datenschutz
☒ Mitarbeiter auf Vertraulichkeit verpflichtet
☒ Richtlinie zur EDV-Nutzung
☒ DSFA wird bei Bedarf durchgeführt

2. Incident-Response Management

Organisatorischer und technischer Prozess als Reaktion auf erkannte oder vermutete Sicherheitsvorfälle.

Technische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung

3. Auftragskontrolle

Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Organisatorische Maßnahmen
☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
☒ Abschluss der notwendigen Verträge zur Auftragsverarbeitung
☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer