Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung (AV-Vertrag)

Zwischen

Dem Kunden als Auftraggeber

und

sagittarius GmbH
Steinlachstr. 98/1
72116 Mössingen

– als Auftragnehmer–

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

Präambel

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

§ 1. Gegenstand und Dauer und Spezifizierung der Auftragsverarbeitung

a. Aus der Beauftragung zur Bereitstellung der Hinweisgeberplattform ergeben sich Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung.
b. Die Dauer richtet sich nach der Laufzeit der Beauftragung.

§ 2. Spezifizierung der Auftragsverarbeitung

a. Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.
b. Es werden folgende Daten verarbeitet:
    i. Anrede, Kommunikationsdaten, Vor-und Zuname, Email Adresse, Adresse, Kontaktdaten,
    ii. inhaltliche Meldungen zu betrieblichen Vorkommnissen inklusive möglicher vertraulicher Informationen und/oder Geschäftsgeheimnissen,
    iii. Daten über beteiligte Personen (Anrede, Kommunikationsdaten, Vor- und Zuname, Adressen)
c. Von der Verarbeitung betroffen sind:
    i. Beschäftigte des Auftraggebers,
    ii. Kunden und Lieferanten des Auftraggebers,
    iii. Interessenten und/oder Bewerber des Auftraggebers,
    iv. natürliche Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit

    Informationen über Verstöße im Zusammenhang mit dem Auftraggeber erlangt haben.

§ 3. Anwendungsbereich und Verantwortlichkeit

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

§ 4. Pflichten des Auftragnehmers

a. Der Auftragnehmer darf personenbezogene Daten, die Gegenstand des Auftrags sind, nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor und dessen Voraussetzungen werden gewahrt.
b. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
c. Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat insbesondere technische und organisatorische Maßnahmen zu treffen, gemessen am Risiko für die Rechte und Freiheiten der betroffenen Personen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der

Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer gewährleisten. Der Auftragnehmer hat die erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung zu dokumentieren.

d. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Diese sind vom Auftragnehmer entsprechend zu dokumentieren.
e. Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.
f. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Unterstützungsleistungen, die nicht in der Beauftragung enthalten sind oder die über die gesetzlichen Pflichten des Auftragnehmers hinausgehen oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, werden zu einem üblichen Stundensatz vergütet.
g. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die mit der Verarbeitung der personenbezogenen Daten zuständigen Personen zur Vertraulichkeit verpflichtet haben und diese Vertraulichkeitsverpflichtung auch nach Beendigung des Auftrags fortbesteht.
h. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
i. Eine Meldung von Datenschutzverletzungen muss mindestens enthalten:
    i. eine Beschreibung des Vorfalls, soweit möglich mit Angabe der Art der Verletzung des Schutzes personenbezogener Daten, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
    ii. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
    iii. eine Beschreibung der wahrscheinlichen Folgen des gemeldeten Vorfalls, eine Beschreibung der ergriffenen Maßnahmen zur Behebung und ggf. Maß- nahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
    iv. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
j. Der Auftragnehmer gewährleistet, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen (Art. 32 Abs. 1 lit. d DS-GVO).

§ 5. Pflichten des Auftraggebers

a. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten feststellt.
b. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DS-GVO, gilt §4 Abs. e)-f) entsprechend.

§ 6. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Anträgen gemäß Art. 15 bis 21 DS-GVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung dieser Anträge der betroffenen Personen im erforderlichen Umfang.

§ 7. Nachweismöglichkeiten

a. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Ver- trag niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die dokumentierten Kontrollen und erforderlichen Auskünfte zur Verfügung zu stellen. Insbesondere ist die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art 32 DS-GVO nachzuweisen.
b. Der Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten kann erfolgen durch
    i. aktuelle Testate, Berichte oder Berichtsauszüge
    ii. Selbstaudits
    iii. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701)
    iv. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
    v. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO

§ 8. Kontrollrechte

a. Der Auftragnehmer verpflichtet sich, den Auftraggeber bei seinen Prüfungen gemäß Art. 28 Abs. 3 Satz 2 lit. h DS-GVO zur Einhaltung der Vorschriften zum Datenschutz sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu unterstützen.
b. Die Prüfungen werden durch den Auftraggeber selbst oder einen von ihm beauftragten Dritten durchgeführt. Sollte der durch den Auftraggeber beauftragte Dritter in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Beauftragte Dritte müssen durch den Auftraggeber zur Verschwiegenheit verpflichtet werden. Dem Auftragnehmer steht das Recht zu, die Abgabe einer separaten Verschwiegenheitserklärung des beauftragten Dritten zu verlangen. Dies gilt insbesondere für die Abgabe von Erklärungen zur berufsrechtlichen oder gesetzlichen Verschwiegenheit.

§ 9. Unterauftragsverhältnisse (Subunternehmer)

a. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit im Vertrag vereinbarten Verarbeitung personenbezogener Daten beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.
b. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
c. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb einer Frist von 14 Kalendertagen – aus wichtigem datenschutzrechtlichem Grund – gegenüber dem Auftragnehmer widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.
d. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 10. Übermittlung in Drittstaaten

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

Bestimmungen dieses Vertrags erfolgen.

b. Eine Übermittlung von Daten in Drittstatten findet nicht statt. Sollte eine Übermittlung notwendig werden, wird dies in einer separat zu erstellenden Anlage zu dieser Vereinbarung festgehalten.
c. Der Auftragnehmer stellt einen Kontakt zur Verfügung, den der Auftraggeber Betroffenen als Stelle mitteilen kann, bei dem die Garantien verfügbar sind bzw. eine Kopie der Garantie angefordert werden kann.

§ 11. Sonderkündigungsrecht und Haftung

a. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
b. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
c. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.
d. Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.
e. Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

§ 12. Informationspflichten, Schriftformklausel, Rechtswahl

a. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz- Grundverordnung liegen.
b. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – ein- schließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
c. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
d. Es gilt deutsches Recht.

§ 13. Gültigkeit und Inkrafttreten

a. Diese Vereinbarung ist Teil der Bestellung des Kunden und der Bereitstellung der Hinweisgeberplattform durch die sagittarius GmbH.
b. Diese Vereinbarung wird auf elektronischem Wege geschlossen und ist ohne Unterschrift gültig.