Vertrag über die Auftragsverarbeitung

gemäß Art. 28 DSGVO · für die Nutzung der Software Leadcosmos

Leadcosmos

Zwischen den Vertragsparteien

Auftraggeber (Kunde, Verantwortlicher)

Firma

Ansprechpartner/in

E-Mail-Adresse

Straße und Hausnummer

PLZ, Ort, Land

Leadcosmos-Konto / Kundennummer (optional)

– nachfolgend „Auftraggeber“ –

Auftragnehmer (Anbieter der Software, Auftragsverarbeiter)

Leadcosmos.io GmbH, vertreten durch den Geschäftsführer Daniel Huchler, Karlsruher Str. 2, 76646 Bruchsal, Deutschland

– nachfolgend „Auftragnehmer“; Auftraggeber und Auftragnehmer gemeinsam „Parteien“ –

wird folgender Vertrag geschlossen:

Präambel und Transparenzhinweis

Leadcosmos ist eine White-Label-Version der Software **HighLevel** (auch „GoHighLevel“) der HighLevel, Inc. und ihres verbundenen Unternehmens LeadConnector LLC, beide mit Sitz in Dallas, Texas (USA). Der Auftragnehmer stellt dem Auftraggeber die Software unter der Marke Leadcosmos bereit. Betrieb, Hosting und die Kommunikationsdienste der Software (z. B. E-Mail, SMS, Telefonie, WhatsApp) sowie die KI-Funktionen werden technisch über HighLevel als Unterauftragnehmer erbracht. Personenbezogene Daten werden dadurch in die USA übermittelt. Diese Übermittlung ist abgesichert durch die Zertifizierung von HighLevel unter dem EU-US Data Privacy Framework sowie durch die EU-Standardvertragsklauseln, die Bestandteil des Auftragsverarbeitungsvertrags von HighLevel sind (www.gohighlevel.com/data-processing-agreement). Einzelheiten regeln Ziffer 10 sowie Anlage 3.

1. Gegenstand und Geltungsbereich

1.1 Der Auftragnehmer stellt dem Auftraggeber die Software Leadcosmos als Online-Dienst (Software-as-a-Service) auf Grundlage eines gesonderten Vertrags über die Nutzung der Software (Abonnement, nachfolgend „Hauptvertrag“) bereit. Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien nach Art. 28 DSGVO.

1.2 Dieser Vertrag gilt ausschließlich für die Bereitstellung und Nutzung der Software Leadcosmos. Sonstige Leistungen des Auftragnehmers oder mit ihm verbundener Unternehmen, etwa Beratungs-, Einrichtungs- oder Agenturleistungen, sind nicht Gegenstand dieses Vertrags.

1.3 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO, der Auftragnehmer Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO. Der Auftraggeber ist allein verantwortlich für die Beurteilung der Zulässigkeit der Verarbeitung nach Art. 6 DSGVO und für die Wahrung der Rechte der betroffenen Personen.

1.4 Gegenstand, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

1.5 Der Auftraggeber versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Auftragnehmer durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen (Anlage 2) in der Lage ist, seine Pflichten aus diesem Vertrag zu erfüllen.

1.6 Der Auftragnehmer selbst verarbeitet die Daten in der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Da die Software über HighLevel betrieben wird, verarbeiten Unterauftragnehmer die Daten auch in den USA und gegebenenfalls in weiteren Drittländern. Dies erfolgt ausschließlich nach Maßgabe von Ziffer 10 und unter Einhaltung von Kapitel V DSGVO (Art. 44 ff.). Mit Abschluss dieses Vertrags stimmt der Auftraggeber den in Anlage 3 beschriebenen Übermittlungen zu.

1.7 Die Vergütung richtet sich nach dem Hauptvertrag; sie wird außerhalb dieses Vertrags vereinbart.

2. Laufzeit

Dieser Vertrag beginnt mit seiner Annahme (Ziffer 15.1) und läuft für die Dauer des Hauptvertrags. Er endet automatisch mit dem Ende des Hauptvertrags, ohne dass es einer gesonderten Kündigung bedarf. Bestimmungen, die ihrer Natur nach über das Vertragsende hinaus fortgelten, insbesondere zu Löschung, Rückgabe und Vertraulichkeit (Ziffern 12 und 13), bleiben unberührt. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung gegenüber dem Auftragnehmer zu. Er kann insbesondere die unverzügliche Löschung, Berichtigung, Einschränkung der Verarbeitung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Die Weisungen sind zunächst durch diesen Vertrag und den Hauptvertrag festgelegt; im laufenden Betrieb erteilt der Auftraggeber Weisungen insbesondere durch die Konfiguration und Nutzung der Funktionen der Software (z. B. Anlegen, Bearbeiten, Exportieren und Löschen von Daten). Der Auftragnehmer ist verpflichtet, den Weisungen des Auftraggebers Folge zu leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

3.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt. Zweifelt der Auftragnehmer die Rechtmäßigkeit einer Weisung begründet an, ist er berechtigt, deren Ausführung auszusetzen, bis der Auftraggeber sie ausdrücklich bestätigt oder ändert.

3.3 Weisungen sind grundsätzlich schriftlich oder in Textform (z. B. per E-Mail) zu erteilen. Mündliche Weisungen hat der Auftraggeber auf Verlangen des Auftragnehmers in Textform zu bestätigen. Der Auftragnehmer hält Person, Datum und Uhrzeit mündlicher Weisungen in geeigneter Form fest.

3.4 Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch zur Verschwiegenheit verpflichtete Dritte kontrollieren zu lassen. Der Auftragnehmer duldet diese Kontrollen, unterstützt sie im erforderlichen Maß und erteilt die hierfür relevanten Auskünfte vollständig und wahrheitsgemäß.

4.2 Der Auftragnehmer kann die Einhaltung seiner Pflichten auch durch geeignete Nachweise belegen, insbesondere durch aktuelle Testate, Prüfberichte oder Zertifizierungen, auch solche seiner Unterauftragnehmer (z. B. den SOC-2-Bericht von HighLevel). Kontrollen bei Unterauftragnehmern richten sich nach deren Vertragsbedingungen.

4.3 Der Auftraggeber stellt sicher, dass Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigen. Kontrollen vor Ort finden grundsätzlich während der üblichen Geschäftszeiten und nach vorheriger Terminvereinbarung mit angemessener Frist statt, es sei denn, der Kontrollzweck steht einer vorherigen Ankündigung entgegen.

4.4 Die Ergebnisse von Kontrollen und erteilte Weisungen werden von beiden Parteien in geeigneter Weise dokumentiert.

5. Allgemeine Pflichten des Auftragnehmers

5.1 Der Auftragnehmer verarbeitet die vertragsgegenständlichen Daten ausschließlich auf Grundlage dieses Vertrags und des Hauptvertrags in Verbindung mit den Weisungen des Auftraggebers. Eine abweichende Verarbeitung ist nur aufgrund zwingender Rechtsvorschriften der Union oder der Mitgliedstaaten zulässig (z. B. bei Ermittlungen von Strafverfolgungsbehörden). In diesem Fall informiert der Auftragnehmer den Auftraggeber vor der Verarbeitung, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2 Der Auftragnehmer beachtet bei der Durchführung des Auftrags alle gesetzlichen Vorschriften. Insbesondere trifft er die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen und führt, soweit gesetzlich vorgeschrieben, ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

5.3 Soweit der Auftragnehmer gesetzlich zur Benennung eines Datenschutzbeauftragten verpflichtet ist, benennt er einen solchen und teilt dem Auftraggeber dessen Kontaktdaten mit; Änderungen teilt er unverzüglich mit. Ansprechpartner für Datenschutzfragen beim Auftragnehmer ist: **[Datenschutz-Kontakt: E-Mail-Adresse noch festzulegen]**.

5.4 Die Datenverarbeitung durch Beschäftigte des Auftragnehmers darf auch außerhalb seiner Betriebsstätten erfolgen, insbesondere im Homeoffice oder per Fernzugriff, sofern die technischen und organisatorischen Maßnahmen nach Anlage 2 eingehalten werden. Der Auftraggeber stimmt dem hiermit zu.

5.5 Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor dieser Verpflichtung erhalten sie keinen Zugang zu den Daten des Auftraggebers.

5.6 Der Auftraggeber kann betroffenen Personen auf Anfrage eine Kopie dieses Vertrags zur Verfügung stellen. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen erforderlich ist, insbesondere hinsichtlich der Maßnahmen nach Anlage 2, darf er Teile vorher unkenntlich machen; er stellt dann eine aussagekräftige Zusammenfassung zur Verfügung, wenn die betroffene Person den Inhalt andernfalls nicht verstehen oder ihre Rechte nicht ausüben könnte. Die Pflichten des Auftraggebers nach Art. 13 und 14 DSGVO bleiben unberührt.

5.7 Der Auftragnehmer kontrolliert die Erfüllung seiner Pflichten regelmäßig selbst und dokumentiert dies in geeigneter Weise.

6. Pflichten des Auftraggebers; besondere Kategorien personenbezogener Daten

6.1 Der Auftraggeber ist dafür verantwortlich, dass für die von ihm veranlasste Verarbeitung eine Rechtsgrundlage besteht, insbesondere erforderliche Einwilligungen eingeholt werden (z. B. für Newsletter, SMS, WhatsApp-Nachrichten oder die Aufzeichnung von Telefongesprächen), und dass er seine Informationspflichten gegenüber den betroffenen Personen erfüllt. Stellt der Auftraggeber Fehler oder Unregelmäßigkeiten bei der Verarbeitung fest, informiert er den Auftragnehmer unverzüglich.

6.2 Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO (z. B. Gesundheitsdaten, Angaben zur ethnischen Herkunft, zu religiösen oder politischen Überzeugungen, genetische oder biometrische Daten) sowie von Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO ist nicht vorgesehen. Der Auftraggeber wird solche Daten nicht in die Software einpflegen, es sei denn, er stellt sicher, dass hierfür eine eigene Rechtsgrundlage besteht; in diesem Fall ist er für erforderliche zusätzliche Schutzmaßnahmen selbst verantwortlich.

7. Technische und organisatorische Maßnahmen; Verletzungen des Schutzes personenbezogener Daten

7.1 Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu diesen Daten führt (nachfolgend „Verletzung des Schutzes personenbezogener Daten“). Dabei tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den Risiken für die betroffenen Personen gebührend Rechnung. Der Auftragnehmer setzt mindestens die in Anlage 2 aufgeführten Maßnahmen um und überprüft regelmäßig, ob sie weiterhin ein angemessenes Schutzniveau bieten. Er darf die Maßnahmen weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird.

7.2 Der Auftragnehmer gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist.

7.3 Im Fall einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung nach diesem Vertrag ergreift der Auftragnehmer geeignete Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer nachteiligen Auswirkungen. Er meldet die Verletzung dem Auftraggeber unverzüglich, nachdem sie ihm bekannt wurde. Die Meldung enthält die Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der Art der Verletzung (soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze), die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen. Können nicht alle Informationen gleichzeitig bereitgestellt werden, enthält die erste Meldung die verfügbaren Informationen; weitere Informationen werden ohne unangemessene Verzögerung nachgereicht.

7.4 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei dessen Pflichten nach der DSGVO, insbesondere bei der Benachrichtigung der zuständigen Aufsichtsbehörde und der betroffenen Personen.

8. Unterstützungspflichten des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber nach Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Rechte der betroffenen Personen nach Kapitel III DSGVO (Art. 12 bis 22), insbesondere bei der Erteilung von Auskünften und bei der Löschung, Berichtigung oder Einschränkung der Verarbeitung personenbezogener Daten. Viele dieser Maßnahmen kann der Auftraggeber über die Funktionen der Software selbst umsetzen. Die Reichweite der Unterstützung bestimmt sich im Einzelfall nach der Art der Verarbeitung.

8.2 Der Auftragnehmer unterstützt den Auftraggeber nach Art. 28 Abs. 3 lit. f DSGVO ferner bei dessen Pflichten nach Art. 32 bis 36 DSGVO (insbesondere Meldepflichten und Datenschutz-Folgenabschätzung). Die Reichweite bestimmt sich nach der Art der Verarbeitung und den dem Auftragnehmer zur Verfügung stehenden Informationen.

9. Unterauftragnehmer

9.1 Der Auftragnehmer nimmt in Übereinstimmung mit Art. 28 Abs. 2 Satz 1 DSGVO keine weiteren Auftragsverarbeiter (Unterauftragnehmer) ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Die Bestimmungen zu Unterauftragsverhältnissen gelten entsprechend für alle weiteren Unterauftragnehmer in der Kette.

9.2 Der Auftraggeber genehmigt hiermit die Beauftragung der in Anlage 3 aufgeführten Unterauftragnehmer.

9.3 Die Kern-Unterauftragnehmerin HighLevel setzt ihrerseits weitere Unterauftragnehmer ein, u. a. für Datenspeicherung und Hosting, Kommunikationsdienste (z. B. E-Mail-Versand, SMS und Telefonie) sowie KI-Funktionen. Diese sind in der jeweils aktuellen Liste unter www.gohighlevel.com/sub-processors aufgeführt. Der Auftraggeber genehmigt deren Einsatz.

9.4 Darüber hinaus genehmigt der Auftraggeber in allgemeiner Weise die Inanspruchnahme weiterer Unterauftragnehmer. Der Auftragnehmer informiert den Auftraggeber in Textform (z. B. per E-Mail) über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragnehmern. Der Auftraggeber kann innerhalb von 14 Tagen nach Zugang der Information in Textform Einspruch erheben; der Einspruch ist nur aus wichtigem datenschutzrechtlichem Grund zulässig, der dem Auftragnehmer nachzuweisen ist. Erhebt der Auftraggeber innerhalb dieser Frist keinen Einspruch, gilt die Änderung als genehmigt. Können sich die Parteien im Fall eines Einspruchs nicht einigen, ist der Auftraggeber berechtigt, den Hauptvertrag

außerordentlich zu kündigen.

9.5 Der Auftragnehmer verpflichtet jeden Unterauftragnehmer vertraglich auf Datenschutzpflichten, die ein gleichwertiges Schutzniveau wie dieser Vertrag gewährleisten (Art. 28 Abs. 4 DSGVO). Die Beauftragung von Unterauftragnehmern in Drittländern erfolgt nur nach Maßgabe von Ziffer 10.

9.6 Der Auftragnehmer stellt dem Auftraggeber auf Verlangen eine Kopie der Vereinbarung mit einem Unterauftragnehmer oder die maßgeblichen Vertragsbedingungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen notwendig ist, kann er den Wortlaut vorher unkenntlich machen.

9.7 Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Unterauftragnehmers. Der Auftragnehmer benachrichtigt den Auftraggeber, wenn ein Unterauftragnehmer seinen Pflichten nicht nachkommt.

10. Übermittlung in Drittländer

10.1 Eine Übermittlung personenbezogener Daten in ein Land außerhalb der EU und des EWR (Drittland) erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

10.2 Die Übermittlung an HighLevel, Inc. und LeadConnector LLC in die USA stützt sich auf die Zertifizierung von HighLevel unter dem EU-US Data Privacy Framework (Angemessenheitsbeschluss der EU-Kommission vom 10. Juli 2023, Art. 45 DSGVO) sowie ergänzend auf die EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914), die Bestandteil des Auftragsverarbeitungsvertrags von HighLevel sind.

10.3 Für die übrigen Unterauftragnehmer ist die jeweilige Übermittlungsgrundlage in Anlage 3 angegeben.

10.4 Entfällt eine Übermittlungsgrundlage, etwa weil ein Angemessenheitsbeschluss aufgehoben wird, stellt der Auftragnehmer die Übermittlung unverzüglich auf eine andere geeignete Garantie nach Art. 46 DSGVO um oder informiert den Auftraggeber, falls dies nicht möglich ist.

11. Mitteilungspflichten des Auftragnehmers

11.1 Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen teilt der Auftragnehmer dem Auftraggeber unverzüglich mit; dasselbe gilt bei einem begründeten Verdacht. Dies gilt unabhängig davon, ob der Verstoß vom Auftragnehmer, seinen Beschäftigten, einem Unterauftragnehmer oder einer sonstigen von ihm eingesetzten Person begangen wurde.

11.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten nach Art. 33 und 34 DSGVO. Eigenständige Meldungen an Behörden oder betroffene Personen nach Art. 33 und 34 DSGVO nimmt der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers vor.

11.3 Wendet sich eine betroffene Person, eine Behörde oder ein sonstiger Dritter mit einem Ersuchen um Auskunft, Berichtigung, Einschränkung oder Löschung an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter. Ohne Zustimmung des Auftraggebers kommt er dem Ersuchen nicht selbst nach.

11.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich über bevorstehende Kontrollhandlungen oder sonstige Maßnahmen einer Behörde, die die Verarbeitung der Daten des Auftraggebers betreffen können, sowie über alle Ereignisse oder Maßnahmen Dritter, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

12. Vertragsende, Rückgabe und Löschung der Daten

12.1 Bis zum Ende des Hauptvertrags kann der Auftraggeber seine Daten jederzeit über die Exportfunktionen der Software (z. B. Export von Kontakten im CSV-Format) selbst exportieren. Er ist dafür verantwortlich, benötigte Daten vor Vertragsende zu sichern.

12.2 Innerhalb von 30 Tagen nach Vertragsende löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers bzw. veranlasst deren Löschung bei den Unterauftragnehmern, soweit keine gesetzliche Pflicht zur Aufbewahrung besteht. Datensicherungen werden im Rahmen der regulären Löschzyklen gelöscht.

12.3 Auf Verlangen bestätigt der Auftragnehmer dem Auftraggeber die Löschung in Textform.

13. Vertraulichkeit

13.1 Der Auftragnehmer ist zeitlich unbefristet und über das Ende dieses Vertrags hinaus verpflichtet, die im Rahmen dieses Vertragsverhältnisses erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln zu beachten, denen der Auftraggeber unterliegt (z. B. § 203 StGB). Der Auftraggeber weist den Auftragnehmer bei Vertragsschluss auf solche besonderen Geheimnisschutzregeln hin.

13.2 Der Auftragnehmer macht seine Beschäftigten mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut und verpflichtet sie zur Verschwiegenheit, bevor sie ihre Tätigkeit aufnehmen.

13.3 Der Auftragnehmer dokumentiert die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise und legt die Dokumentation dem Auftraggeber auf Verlangen vor.

14. Haftung

14.1 Jede Partei haftet gegenüber der anderen Partei für Schäden, die sie dieser durch einen Verstoß gegen diesen Vertrag verursacht, nach den gesetzlichen Vorschriften.

14.2 Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO.

14.3 Wurde eine Partei nach Art. 82 Abs. 4 DSGVO in Anspruch genommen, ist sie berechtigt, von der anderen Partei den Teil des Schadenersatzes zurückzufordern, der deren Anteil an der Verantwortung für den Schaden entspricht (Art. 82 Abs. 5 DSGVO).

14.4 Der Auftragnehmer kann sich nicht auf das Verhalten eines Unterauftragnehmers berufen, um sich seiner eigenen Haftung zu entziehen.

15. Vertragsschluss und Schlussbestimmungen

15.1 Dieser Vertrag wird unter leadcosmos.io/avv zur Ansicht und zum Download bereitgestellt. Er kommt zustande durch die Bestätigung des Auftraggebers im Kauf- oder Onboarding-Prozess der Software oder durch Unterzeichnung dieses Dokuments. Die elektronische Form genügt (Art. 28 Abs. 9 DSGVO).

15.2 Änderungen und Ergänzungen dieses Vertrags sowie Nebenabreden bedürfen der Schriftform oder der elektronischen Form und müssen ausdrücklich erkennen lassen, dass und welche Bestimmung geändert oder ergänzt wird.

15.3 Ändern sich die DSGVO oder sonstige in Bezug genommene gesetzliche Regelungen während der Vertragslaufzeit, gelten die Verweise für die jeweiligen Nachfolgeregelungen.

15.4 Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen hinsichtlich des Schutzes personenbezogener Daten die Regelungen dieses Vertrags vor.

15.5 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

15.6 Die Anlagen 1 (Auftragsdetails), 2 (Technische und organisatorische Maßnahmen) und 3 (Unterauftragnehmer) sind Bestandteil dieses Vertrags.

Unterschriften

Nicht erforderlich, wenn der Vertrag im Kauf- oder Onboarding-Prozess elektronisch bestätigt wurde (Ziffer 15.1).

Für den Auftraggeber

Ort _____ **Datum** _____

Name, Funktion (in Druckbuchstaben)

_____

Unterschrift / Firmenstempel

_____

Für den Auftragnehmer

Ort _____ **Datum** _____

Name, Funktion

Daniel Huchler, Geschäftsführer
Leadcosmos.io GmbH

Unterschrift

_____

Anlage 1 – Auftragsdetails

Gegenstand und Art der Verarbeitung

Bereitstellung der Software Leadcosmos (White-Label-Version von HighLevel) als Online-Dienst. Die Verarbeitung umfasst insbesondere das Erheben, Erfassen, Speichern, Organisieren, Anpassen, Abfragen, Verwenden, Übermitteln (z. B. Versand von Nachrichten), Exportieren und Löschen personenbezogener Daten, soweit der Auftraggeber dies über die Software veranlasst. Folgende Funktionen der Software können dabei genutzt werden:

- CRM: Verwaltung von Kontakten, Leads und Kunden inkl. Notizen, Aufgaben und Tags
- Pipeline- und Verkaufschancen-Management
- Website-, Funnel- und Formular-Builder (Landingpages, Formulare, Umfragen)
- Kalender und Online-Terminbuchung
- E-Mail- und SMS-Marketing inkl. Newsletter-Versand
- WhatsApp-Kommunikation über die Software
- Telefonie inkl. optionaler Gesprächsaufzeichnung und Transkription
- Zentraler Posteingang (E-Mail, SMS, WhatsApp, Web-Chat, soziale Netzwerke)
- Workflow-Automatisierungen
- KI-Funktionen (z. B. Chat- und Sprachassistenten, Texterstellung, Zusammenfassungen)
- Social-Media-Planer
- Mitgliederbereiche, Community und Online-Kurse
- Rechnungs-, Zahlungs- und Verkaufsfunktionen (z. B. Checkout, Angebote, Rechnungen)
- Tracking, Reporting und Analyse
- Medienverwaltung (Media Manager)
- Support und technische Betreuung der Software durch den Auftragnehmer

Zweck der Verarbeitung

Bereitstellung und Betrieb der Software gemäß Hauptvertrag, damit der Auftraggeber seine Kunden- und Interessentenbeziehungen verwalten, mit ihnen kommunizieren, Termine und Verkäufe abwickeln sowie Marketing- und Vertriebsmaßnahmen durchführen kann; ferner Support und Fehlerbehebung.

Arten personenbezogener Daten

- Stammdaten: Name, Firma, Position, Anrede
- Kontaktdaten: E-Mail-Adresse, Telefonnummer, Anschrift, Social-Media-Profile
- Weitere vom Auftraggeber erfasste Angaben, z. B. Geburtsdatum
- Kommunikationsinhalte: E-Mails, SMS, WhatsApp- und Chat-Nachrichten
- Gesprächsaufzeichnungen und Transkripte aus der Telefonie, sofern aktiviert
- Formular- und Umfragedaten, Notizen, Aufgaben, Tags
- Termin- und Buchungsdaten
- Vertrags-, Bestell- und Rechnungsdaten, ggf. Zahlungsstatus
- Einwilligungs- und Abmeldestatus (z. B. Newsletter-Bestätigung)
- Nutzungs- und technische Daten: IP-Adresse, Geräte- und Browserdaten, Zeitstempel, Öffnungs- und Klickdaten, Protokolldaten
- Zugangsdaten und Nutzungsdaten der Nutzer des Auftraggebers

Besondere Kategorien personenbezogener Daten

Keine vorgesehen. Der Auftraggeber pflegt keine Daten im Sinne der Art. 9 und 10 DSGVO in die Software ein, es sei denn, er stellt eine eigene Rechtsgrundlage und erforderliche zusätzliche Schutzmaßnahmen sicher (Ziffer 6.2).

Kategorien betroffener Personen

- Kunden und Interessenten (Leads) des Auftraggebers
- Website-Besucher, Formular- und Terminbucher, Newsletter-Empfänger
- Mitglieder und Teilnehmer von Mitgliederbereichen, Communities und Kursen
- Geschäftspartner und Dienstleister des Auftraggebers
- Beschäftigte und sonstige Nutzer des Auftraggebers mit Zugang zur Software

Häufigkeit und Dauer der Verarbeitung

Fortlaufend, je nach Nutzung der Software durch den Auftraggeber, für die Dauer des Hauptvertrags. Nach Vertragsende werden die Daten innerhalb von 30 Tagen gelöscht (Ziffer 12), vorbehaltlich gesetzlicher Aufbewahrungspflichten.

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

Der Auftragnehmer setzt die folgenden Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Maßnahmen, die Server, Rechenzentren und den Betrieb der Software betreffen, werden durch die Kern-Unterauftragnehmerin HighLevel und deren Hosting-Dienstleister umgesetzt (Abschnitt V).

I. Zweckbindung und Trennbarkeit

Trennungskontrolle

Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet.

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Berechtigungskonzept
- Versehen der Datensätze mit Zweckattributen, Datenfeldern oder Signaturen
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und Aufbewahrung auf einem getrennten, abgesicherten IT-System

II. Vertraulichkeit und Integrität

1. Verschlüsselung

- Verschlüsselung gespeicherter Daten mit AES-256 (Advanced Encryption Standard)
- Transportverschlüsselung mit TLS 1.2 und TLS 1.3 (Transport Layer Security)

2. Pseudonymisierung

Personenbezogene Daten werden pseudonymisiert, soweit dies für den jeweiligen Zweck möglich ist. Die Kernfunktionen der Software (Kontaktverwaltung und Kommunikation) erfordern systembedingt die Verarbeitung identifizierbarer Kontaktdaten.

3. Zutrittskontrolle

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen verwehrt (Büroräume des Auftragnehmers bzw. Rechenzentren der Unterauftragnehmer).

- Alarmanlage
- Automatisches Zugangskontrollsystem
- Schließsystem mit Codesperre
- Biometrische Zugangssperren
- Lichtschranken und Bewegungsmelder
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl von Wachpersonal
- Zutrittskonzept und Besucherregelung
- Absicherung von Gebäudeschächten
- Chipkarten- oder Transponder-Schließsystem
- Manuelles Schließsystem
- Videoüberwachung der Zugänge
- Sicherheitsschlösser
- Personenkontrolle beim Pförtner oder Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Tragepflicht von Berechtigungsausweisen

4. Zugangskontrolle

Die Nutzung der Datenverarbeitungssysteme durch Unbefugte wird verhindert.

- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifikation mit biometrischen Verfahren
- Zwei-Faktor-Authentifizierung
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie bei der Übertragung von Daten
- Verschlüsselung der Datensicherungssysteme
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Erstellen von Benutzerprofilen
- Passwort-Richtlinien (Mindestlänge, Komplexität, Wechsel bei Bedarf)
- Authentifikation mit Benutzername und Passwort
- Einsatz eines Passwortmanagers
- Gehäuseverriegelungen
- Verschlüsselung mobiler IT-Systeme und Datenträger
- Sperren externer Schnittstellen (USB etc.)
- Zentrale Smartphone-Administration (z. B. Fernlöschung)
- Verschlüsselung von Datenträgern in Laptops und Notebooks
- Einsatz einer Software-Firewall

5. Zugriffskontrolle

Berechtigte greifen ausschließlich auf die ihrer Berechtigung unterliegenden Daten zu; Daten können nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Berechtigungskonzept
- Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insbesondere beim Ausscheiden von Beschäftigten)
- Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel
- Physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Verschlüsselung von Datenträgern
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das Notwendigste reduziert
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Protokollierung der Vernichtung

6. Eingabekontrolle

Es kann nachträglich festgestellt werden, ob und von wem Daten eingegeben, verändert oder entfernt wurden.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung auf Basis eines Berechtigungskonzepts
- Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
- Aufbewahrung von Formularen, aus denen Daten in automatisierte Verarbeitungen übernommen wurden

7. Auftragskontrolle

Daten werden nur entsprechend den Weisungen des Auftraggebers verarbeitet; Unterauftragnehmer werden sorgfältig ausgewählt und kontrolliert.

- Auswahl von Unterauftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere Datensicherheit)
- Schriftliche Weisungen bzw. Auftragsverarbeitungsverträge mit Unterauftragnehmern
- Benennung eines Datenschutzbeauftragten, soweit gesetzlich erforderlich
- Wirksame Kontrollrechte gegenüber Unterauftragnehmern
- Vertragsstrafen bei Verstößen
- Vorherige Prüfung und Dokumentation der Sicherheitsmaßnahmen der Unterauftragnehmer
- Verpflichtung der Beschäftigten auf Vertraulichkeit
- Sicherstellung der Löschung von Daten nach Beendigung des Auftrags
- Laufende Überprüfung der Unterauftragnehmer und ihrer Tätigkeiten

8. Weitergabekontrolle

Daten können bei der Weitergabe nicht von Unbefugten erlangt oder zur Kenntnis genommen werden.

- Einsatz von VPN-Tunneln
- Verschlüsselung der Kommunikationswege (z. B. E-Mail-Verkehr)
- Verschlüsselung physischer Datenträger beim Transport

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Die Systeme funktionieren zuverlässig; Daten sind gegen zufällige Zerstörung oder Verlust geschützt (Serverräume: über die Rechenzentren der Unterauftragnehmer).

- Unterbrechungsfreie Stromversorgung (USV)
- Klimatisierung der Serverräume
- Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen
- Backup- und Recovery-Konzept
- Regelmäßiges Testen der Datenwiederherstellung
- Notfallplan
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- In Hochwassergebieten: Serverräume über der Wassergrenze
- Belastbares Datensicherungs- und Wiederherstellungskonzept

IV. Überprüfung, Bewertung und Anpassung

Der Auftragnehmer überprüft, bewertet und aktualisiert die in dieser Anlage beschriebenen Maßnahmen regelmäßig, mindestens jährlich, sowie anlassbezogen und passt sie bei Bedarf an.

V. Maßnahmen der Kern-Unterauftragnehmerin HighLevel

Nach eigenen Angaben von HighLevel (www.gohighlevel.com/privacy-and-security, abgerufen am 19.11.2026) gelten für den Betrieb der Plattform insbesondere:

- Prüfung nach SOC 2 Type II (Kriterien Sicherheit, Verfügbarkeit, Vertraulichkeit); HighLevel gibt an, sich jährlich prüfen zu lassen
- Zertifizierung unter dem EU-US Data Privacy Framework
- Hosting auf der Google Cloud Platform; Verschlüsselung mit TLS 1.2+ bei der Übertragung und AES-256 bei der Speicherung
- Schutz vor DDoS-Angriffen und Web Application Firewall
- Zwei-Faktor-Authentifizierung, granulare Benutzerrechte, Audit-Logs und Single Sign-on
- Regelmäßige Penetrationstests durch Dritte, automatisierte Schwachstellenscans und ein Responsible-Disclosure-Programm

Anlage 3 – Unterauftragnehmer

Zum Zeitpunkt des Vertragsschlusses setzt der Auftragnehmer die folgenden Unterauftragnehmer ein. Die weiteren Unterauftragnehmer von HighLevel ergeben sich aus www.gohighlevel.com/sub-processors (Ziffer 9.3).

Unternehmen und Anschrift	Leistung / Zweck	Ort der Verarbeitung	Übermittlungsgrundlage
HighLevel, Inc. 1801 N. Lamar St., Suite 600, Dallas, TX 75202, USA	Kernplattform der Software Leadcosmos: Betrieb, Hosting, CRM- und Automatisierungsfunktionen, KI-Funktionen	USA	EU-US Data Privacy Framework (Art. 45 DSGVO) und EU-Standardvertragsklauseln (Art. 46 DSGVO)

Unternehmen und Anschrift	Leistung / Zweck	Ort der Verarbeitung	Übermittlungsgrundlage
LeadConnector LLC 400 N. Saint Paul St., Suite 920, Dallas, TX 75201, USA (verbundenes Unternehmen von HighLevel)	Kommunikationsdienste der Software (E-Mail, SMS, Telefonie, WhatsApp) und Support	USA	EU-US Data Privacy Framework (Art. 45 DSGVO) und EU-Standardvertragsklauseln (Art. 46 DSGVO) gemäß HighLevel-AVV
Google Ireland Limited Gordon House, Barrow Street, Dublin 4, Irland	Google Workspace: E-Mail, Dokumente, Datenablage, Kalender des Auftragnehmers	Irland/EU; Übermittlung in die USA möglich	EU-US Data Privacy Framework (Art. 45 DSGVO) und EU-Standardvertragsklauseln (Art. 46 DSGVO)
Zoom Communications, Inc. 55 Almaden Blvd., Suite 600, San Jose, CA 95113, USA	Videokonferenzen (z. B. Onboarding und Support)	USA	EU-US Data Privacy Framework (Art. 45 DSGVO) und EU-Standardvertragsklauseln (Art. 46 DSGVO)
Loom, Inc. (Atlassian-Gruppe) 140 2nd Street, Floor 3, San Francisco, CA 94105, USA	Bildschirm- und Erklärvideos (z. B. Support, Anleitungen)	USA	EU-US Data Privacy Framework (Art. 45 DSGVO) und EU-Standardvertragsklauseln (Art. 46 DSGVO)
Stripe Payments Europe, Limited One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Irland	Zahlungsabwicklung	Irland/EU; Übermittlung an Stripe, Inc. (USA)	EU-US Data Privacy Framework (Art. 45 DSGVO) und EU-Standardvertragsklauseln (Art. 46 DSGVO)
FunnelPay (Patrick Mentler, Einzelunternehmen) Siemenstr. 42, 59199 Bönen, Deutschland	Checkout, Zahlungen und Rechnungsstellung	Deutschland/EU	Keine Drittlandübermittlung durch den Anbieter selbst; AVV nach Art. 28 DSGVO
OpenAI Ireland Ltd 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	KI-Assistenz (ChatGPT, Business-Nutzung): Texterstellung, Auswertung, Support	Irland/EU; Übermittlung an OpenAI OpCo, LLC (USA)	EU-Standardvertragsklauseln (Art. 46 DSGVO) gemäß OpenAI-AVV
Anthropic Ireland, Limited 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Irland	KI-Assistenz (Claude, Business-Nutzung): Texterstellung, Auswertung, Support	Irland/EU; Übermittlung an Anthropic, PBC (USA)	EU-Standardvertragsklauseln (Art. 46 DSGVO) gemäß Anthropic-AVV
Anysphere, Inc. (Cursor) 2261 Market Street, STE 86466, San Francisco, CA 94114, USA	KI-Assistent „Grok Bot“: Unterstützung bei Support, Einrichtung und Auswertungen	USA	EU-Standardvertragsklauseln (Art. 46 DSGVO, Modul 2) gemäß Cursor-AVV