Vertrag über die Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) · MeinLeadFlow

zwischen

Auftraggeber (Verantwortlicher)	**Auftragnehmer** (Auftragsverarbeiter)
Firma: _____	Oleksiy Ostapenko – Webdesign & IT-Lösungen (Einzelunternehmer), Anbieter von MeinLeadFlow
Anschrift: _____	Edisonstr. 44 65199 Wiesbaden, Deutschland
_____	E-Mail: hallo@meinleadflow.de Telefon: +49 611 16855244
vertreten durch: _____	

– nachfolgend gemeinsam „die Parteien“ –

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer stellt dem Auftraggeber die Software-as-a-Service-Lösung „MeinLeadFlow“ bereit: ein KI-gestütztes Anfrageformular („Widget“), das der Auftraggeber auf seiner Website einbindet, sowie die Anwendung unter app.meinleadflow.de zur Verwaltung der eingehenden Anfragen („Leads“). Grundlage ist der zwischen den Parteien geschlossene Nutzungsvertrag bzw. die Teilnahme an der Pilotphase („Hauptvertrag“).

(2) Im Rahmen dieser Leistung verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien. Er gilt für alle Tätigkeiten, bei denen der Auftragnehmer oder von ihm beauftragte Unterauftragsverarbeiter personenbezogene Daten des Auftraggebers verarbeiten.

(3) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Pflichten, die ihrer Natur nach über das Vertragsende hinaus wirken (insbesondere § 4 und § 9), bleiben bestehen.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

(2) Die Verarbeitung erfolgt ausschließlich in einem Mitgliedstaat der Europäischen Union oder des EWR, soweit nicht in Anlage 3 für einzelne Unterauftragsverarbeiter ausdrücklich etwas anderes geregelt ist. Jede Übermittlung in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(3) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Information der Besucher seiner Website (Art. 13 DSGVO) und für die Inhalte, die er im Widget hinterlegt (Leistungen, Fragen, Hinweise). Er wird über das Widget keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) abfragen.

§ 3 Weisungen des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet (Art. 28 Abs. 3 lit. a DSGVO). In einem solchen Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

(2) Die Weisungen werden durch den Hauptvertrag, diesen Vertrag und die Einstellungen festgelegt, die der Auftraggeber in der Anwendung vornimmt (z. B. Leistungen, Fragen, Benachrichtigungsadresse, Löschfrist). Weitere Weisungen erteilt der Auftraggeber in Textform (z. B. per E-Mail).

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung der Weisung aussetzen, bis sie vom

Auftraggeber bestätigt oder geändert wird.

§ 4 Vertraulichkeit

(1) Der Auftragnehmer gewährleistet, dass sich alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(2) Der Auftragnehmer verarbeitet die Daten nicht für eigene Zwecke. Insbesondere werden Anfragedaten weder an Dritte verkauft noch für Werbung genutzt; der eingesetzte KI-Anbieter verwendet über die Programmierschnittstelle (API) übermittelte Daten nach seinen Vertragsbedingungen nicht zum Training seiner Modelle.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die zum Vertragsschluss geltenden Maßnahmen sind in **Anlage 2** beschrieben.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie durch gleichwertige oder bessere Maßnahmen ersetzen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, die in **Anlage 3** aufgeführten Unterauftragsverarbeiter einzusetzen (Art. 28 Abs. 2 DSGVO).

(2) Über beabsichtigte Hinzuziehungen oder Ersetzungen weiterer Unterauftragsverarbeiter informiert der Auftragnehmer den Auftraggeber mindestens 30 Tage im Voraus in Textform. Der Auftraggeber kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Können sich die Parteien nicht einigen, ist der Auftraggeber berechtigt, den Hauptvertrag zum Zeitpunkt der Änderung zu kündigen.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die den in diesem Vertrag festgelegten im Wesentlichen entsprechen (Art. 28 Abs. 4 DSGVO).

(4) Nicht als Unterauftragsverarbeitung gelten Nebenleistungen wie Telekommunikationsdienste oder die Nutzung öffentlicher Netze, sofern dabei kein Zugriff auf personenbezogene Daten des Auftraggebers erfolgt.

§ 7 Rechte betroffener Personen

Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anfragen betroffener Personen nach Kapitel III DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch). Der Auftraggeber kann Anfragen in der Anwendung einsehen und löschen. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst, soweit nicht anders vereinbart.

§ 8 Unterstützungs- und Meldepflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(2) Wird dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten des Auftraggebers bekannt, meldet er diese dem Auftraggeber unverzüglich, möglichst innerhalb von 24 Stunden, mit den ihm vorliegenden Informationen nach Art. 33 Abs. 3 DSGVO. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung betroffener Personen obliegen dem Auftraggeber.

§ 9 Löschung und Rückgabe

(1) Anfragedaten werden in der Anwendung automatisch nach Ablauf der vom Auftraggeber gewählten Speicherfrist gelöscht (wählbar: 3, 6 oder 12 Monate ab Eingang; Voreinstellung 6 Monate). Der Auftraggeber kann einzelne Anfragen jederzeit vorher löschen. Für die weitere Aufbewahrung der Anfragen, die ihm per E-Mail zugehen, ist der Auftraggeber selbst verantwortlich.

(2) Nach Beendigung des Hauptvertrags oder mit Löschung des Kontos durch den Auftraggeber löscht der Auftragnehmer sämtliche personenbezogenen Daten des Auftraggebers, sofern nicht nach Unionsrecht oder mitgliedstaatlichem Recht eine Speicherpflicht besteht. Die Löschung aus Datensicherungen erfolgt im Rahmen der regulären Rotationszyklen der Sicherungen. Auf Wunsch stellt der Auftragnehmer dem Auftraggeber die Anfragedaten vor der Löschung in einem gängigen Format bereit, sofern der Wunsch vor Vertragsende in Textform mitgeteilt wird.

§ 10 Nachweise und Kontrollen

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer (Art. 28 Abs. 3 lit. h DSGVO). Kontrollen vor Ort sind mit angemessener Frist, in der Regel mindestens 14 Tage, anzukündigen und während der üblichen Geschäftszeiten durchzuführen. Der Nachweis kann vorrangig durch Selbstauskünfte, aktuelle Dokumentation der Maßnahmen nach Anlage 2 sowie Zertifikate und Berichte der Unterauftragsverarbeiter erbracht werden.

§ 11 Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags.

(2) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags in Bezug auf den Datenschutz vor.

(3) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, Wiesbaden.

_____	Wiesbaden, _____
Ort, Datum	Ort, Datum
_____	_____
Auftraggeber (Name, Unterschrift)	Oleksiy Ostapenko, Auftragnehmer

Anlage 1 – Gegenstand der Verarbeitung

Art der Verarbeitung	Erheben, Erfassen, Strukturieren, Speichern, Auslesen, Übermitteln an den Auftraggeber (E-Mail und Anwendung), automatisierte Zusammenfassung, Löschen.
Zweck	Entgegennahme und Vorqualifizierung von Anfragen, die Besucher über das auf der Website des Auftraggebers eingebundene Widget stellen; KI-gestützte Auswahl passender Rückfragen; Zustellung der strukturierten Anfrage samt Einschätzung an den Auftraggeber; optionale Eingangsbestätigung an den Anfragenden, sofern vom Auftraggeber aktiviert.
Kategorien betroffener Personen	Besucherinnen und Besucher der Website des Auftraggebers, die über das Widget eine Anfrage stellen (Interessenten, Kunden, Ansprechpartner von Unternehmen).
Arten personenbezogener Daten	**Kontaktdaten:** Anrede, Name, E-Mail-Adresse, Telefonnummer, ggf. Firmenname. **Anfragedaten:** gewünschte Leistung, Antworten auf Fragen, Freitexte, Kundentyp (privat/gewerblich), Dringlichkeit. **Ortsdaten:** Postleitzahl, Ort, ggf. Straße und Hausnummer des Leistungsorts. **Nachweis- und Metadaten:** Einwilligung mit Zeitpunkt, Sprache, Eingangszeitpunkt, Quellseite und Kampagnenparameter (UTM). **Technische Daten:** IP-Adresse (kurzzeitig zur Missbrauchsabwehr und in Server-Logs des Hosting-Anbieters).
Besondere Kategorien (Art. 9 DSGVO)	Werden nicht bestimmungsgemäß verarbeitet. Der Auftraggeber stellt sicher, dass keine solchen Daten abgefragt werden.
Speicherdauer	Automatische Löschung nach der vom Auftraggeber gewählten Frist (3, 6 oder 12 Monate ab Eingang; Voreinstellung 6 Monate), spätestens mit Löschung des Kontos.

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

Vertraulichkeit – Zutritt	Der Auftragnehmer betreibt keine eigenen Server. Die Daten liegen in Rechenzentren der Unterauftragsverarbeiter (Anlage 3), deren physische Sicherheit durch Zertifizierungen (z. B. ISO 27001, SOC 2) nachgewiesen ist. Arbeitsgeräte des Auftragnehmers sind mit Festplattenverschlüsselung und Bildschirmsperre geschützt.
Vertraulichkeit – Zugang und Zugriff	Anmeldung an der Anwendung nur mit E-Mail-Adresse und Passwort; Passwörter werden ausschließlich als bcrypt-Hash gespeichert. Jeder Auftraggeber sieht ausschließlich die Anfragen seines eigenen Kontos (mandantengetrennte Datenhaltung). Zugänge zu Infrastruktur- und Datenbankkonten sind auf den Auftragnehmer beschränkt und, soweit verfügbar, mit Zwei-Faktor-Authentifizierung gesichert. Zugangsdaten werden nicht im Quellcode gespeichert.
Datenminimierung und Trennung	Es werden nur die für die Anfrage erforderlichen Daten erhoben. Kontaktdaten werden vor der Übermittlung an den KI-Anbieter entfernt bzw. pseudonymisiert; an diesen gehen nur die inhaltlichen Angaben, die für die Fragenauswahl erforderlich sind. Keine personenbezogenen Daten in Anwendungs-Logs oder URL-Parametern. Das Widget setzt keine Cookies und speichert keine Daten im Browser. Entwicklung und Tests erfolgen mit einer lokalen Datenbank und Testdaten, getrennt vom Produktivsystem.
Integrität – Weitergabe	Alle Verbindungen (Website, Widget, Anwendung, Datenbank, E-Mail-Versand) sind TLS-verschlüsselt. Das Widget kann an die Domain des Auftraggebers gebunden werden. Bestätigungs- und Zurücksetzungs-Links verwenden einmalige, zeitlich begrenzte Token, die nur als Hash gespeichert werden.
Integrität – Eingabekontrolle	Eingaben werden serverseitig validiert. Die Einwilligung des Anfragenden wird serverseitig geprüft und mit Zeitpunkt gespeichert. Missbrauch wird durch Ratenbegrenzung, Duplikaterkennung und Spam-Schutz (Honeypot) abgewehrt.
Verfügbarkeit und Belastbarkeit	Datenbank-Hosting mit täglicher Sicherung durch den Anbieter; vor Änderungen an der Datenbankstruktur zusätzliche manuelle Sicherung. Der Versand von Benachrichtigungen erfolgt nach dem Speichern der Anfrage, sodass ein Ausfall des E-Mail-Dienstes nicht zum Verlust der Anfrage führt.
Löschung	Automatische, tägliche Löschung von Anfragen nach Ablauf der gewählten Speicherfrist; vollständige Löschung aller Daten bei Kontolöschung.
Verfahren zur Überprüfung	Änderungen an der Anwendung werden versioniert, vor Veröffentlichung geprüft und automatisiert getestet. Unterauftragsverarbeiter werden vor Einsatz und anlassbezogen auf ihre Datenschutzgarantien geprüft. Diese Maßnahmen werden mindestens jährlich überprüft.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung	Garantie für Drittland
Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, USA	Hosting und Betrieb der Anwendung und des Widgets	EU (Region Frankfurt am Main)	EU-U.S. Data Privacy Framework; EU-Standard vertragsklauseln
Supabase Inc., USA	Datenbank-Hosting (PostgreSQL)	EU (AWS-Region eu-central-1, Frankfurt am Main)	EU-Standardvertragsklauseln
Anthropic PBC, 500 Howard Street, San Francisco, CA 94105, USA	KI-gestützte Auswahl von Rückfragen und Zusammenfassung der Anfrage (serverseitig, ohne Kontaktdaten)	USA	EU-Standardvertragsklauseln; keine Nutzung zum Modelltraining
Sendinblue SAS (Brevo), 106 boulevard Haussmann, 75008 Paris, Frankreich	Versand transaktionaler E-Mails (Anfrage-Benachrichtigung, Eingangsbestätigung)	EU	nicht erforderlich

Bei Unterauftragsverarbeitern mit Sitz in den USA kann trotz Verarbeitung in der EU ein Zugriff aus einem Drittland nicht vollständig ausgeschlossen werden; die Übermittlung ist durch die genannten Garantien nach Art. 44 ff. DSGVO abgesichert. Die aktuelle Liste stellt der Auftragnehmer auf Anfrage bereit; Änderungen erfolgen nach § 6 Abs. 2.