HEDDY
CRM

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Version	**2.0**
Stand	**24. September 2026**
Dienst	**Heddy CRM**
Dokument-ID	**AVV-HEDDY-CRM-002**

zwischen

dem Kunden, der Heddy CRM im Rahmen des Hauptvertrags nutzt (nachfolgend „Auftraggeber“ oder „Verantwortlicher“),

und

Beyond Matrix Solutions LLC
1621 Central Ave
Cheyenne, WY 82001, USA
support@heddycrm.de
(nachfolgend „Auftragnehmer“ oder „Auftragsverarbeiter“).

Dieser Vertrag konkretisiert die Pflichten der Parteien für die Verarbeitung personenbezogener Daten im Auftrag. Er ist Bestandteil des Hauptvertrags über Heddy CRM.

§ 1 Gegenstand, Dauer und Geltungsbereich

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Auftrag des Auftraggebers, soweit dies für die Bereitstellung und den Betrieb der SaaS-Plattform „Heddy CRM“ erforderlich ist. Die Einzelheiten der Verarbeitung ergeben sich aus Anlage 1.

(2) Die Verarbeitung beginnt mit der Nutzung des Dienstes durch den Auftraggeber und endet mit Beendigung des Hauptvertrags. Verpflichtungen zur Rückgabe, Löschung, Vertraulichkeit und zum Nachweis der Verarbeitung gelten über das Vertragsende hinaus, soweit dies nach diesem Vertrag oder zwingendem Recht erforderlich ist.

(3) Der Auftraggeber bleibt Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Der Auftragnehmer verarbeitet die Daten nicht für eigene Zwecke und bestimmt weder Zwecke noch wesentliche Mittel der Verarbeitung, soweit nicht zwingendes Recht etwas verlangt.

§ 2 Weisungen und Verarbeitung auf Weisung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, auch bei einer Übermittlung in ein Drittland oder an eine internationale Organisation. Die Weisungen ergeben sich zunächst aus diesem Vertrag, dem Hauptvertrag und der jeweiligen Nutzung des Dienstes. Ergänzende Weisungen bedürfen mindestens der Textform.

(2) Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich. Er darf die Umsetzung aussetzen, bis der Auftraggeber die Weisung bestätigt oder anpasst, sofern kein zwingendes Recht entgegensteht.

(3) Ist der Auftragnehmer durch Unionsrecht oder das Recht eines Mitgliedstaats, dem er unterliegt, zu einer Verarbeitung verpflichtet, informiert er den Auftraggeber vor der Verarbeitung, soweit dieses Recht eine Information nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

§ 3 Vertraulichkeit und zugriffsberechtigte Personen

Der Auftragnehmer stellt sicher, dass die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Zugriffe auf Kundendaten werden auf den für Betrieb, Support und Sicherheit erforderlichen Umfang beschränkt.

§ 4 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Stand dieses Vertrags geltenden Maßnahmen sind in Anlage 2 beschrieben.

(2) Der Auftragnehmer darf die Maßnahmen an den technischen Fortschritt und die Weiterentwicklung des Dienstes anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert und dem Auftraggeber auf Anfrage erläutert.

§ 5 Unterstützung des Auftraggebers

(1) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, bei der Erfüllung von Anträgen betroffener Personen nach Kapitel III DSGVO.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO. Hierzu gehören insbesondere angemessene Informationen zu Sicherheitsmaßnahmen, Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und einer vorherigen Konsultation.

§ 6 Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, grundsätzlich spätestens innerhalb von 48 Stunden nach Kenntnisnahme, über Verletzungen des Schutzes personenbezogener Daten, soweit diese Daten des Auftraggebers betreffen. Eine spätere Ergänzung bereits mitgeteilter Informationen bleibt zulässig, soweit Angaben noch nicht vorliegen.

(2) Die Mitteilung enthält, soweit verfügbar, mindestens Art der Verletzung, Kategorien und ungefähre Zahl betroffener Personen und Datensätze, wahrscheinliche Folgen sowie bereits ergriffene oder vorgeschlagene Abhilfemaßnahmen und eine Anlaufstelle für Rückfragen.

§ 7 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, die in Anlage 3 bezeichneten Unterauftragsverarbeiter einzusetzen. Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich zu mindestens denselben Datenschutzpflichten, die ihn nach diesem Vertrag treffen.

(2) Über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters informiert der Auftragnehmer den Auftraggeber mindestens 30 Tage vor Wirksamwerden in Textform. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist widersprechen. Finden die Parteien keine angemessene Lösung, steht dem Auftraggeber ein außerordentliches Kündigungsrecht hinsichtlich der betroffenen Leistung zu.

(3) Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Erfüllung der Datenschutzpflichten seiner Unterauftragsverarbeiter verantwortlich.

§ 8 Übermittlungen in Drittländer

(1) Die Kerninfrastruktur für Anwendung, Datenbank, Dateien und Datensicherungen wird bei Hetzner in Deutschland betrieben. Soweit Daten bei der Nutzung aktivierter Funktionen dennoch in einem Drittland verarbeitet werden oder ein Drittlandzugriff besteht, erfolgt dies nur unter Beachtung der Voraussetzungen der Art. 44 ff. DSGVO.

(2) Für den Einsatz von Unterauftragsverarbeitern in Drittländern verwendet der Auftragnehmer jeweils einen geeigneten Übermittlungsmechanismus, insbesondere einen Angemessenheitsbeschluss nach Art. 45 DSGVO oder geeignete Garantien nach Art. 46 DSGVO einschließlich der einschlägigen Standardvertragsklauseln und erforderlicher ergänzender Maßnahmen.

(3) Beyond Matrix Solutions LLC hat ihren Sitz in den Vereinigten Staaten von Amerika. Soweit ein Auftraggeber im EWR personenbezogene Daten an den Auftragnehmer übermittelt oder dem Auftragnehmer einen Zugriff aus einem Drittland ermöglicht, prüfen die Parteien den jeweils erforderlichen Übermittlungsmechanismus. Soweit erforderlich, schließen sie die einschlägigen Standardvertragsklauseln der Europäischen Kommission mit den hierfür notwendigen Anhängen gesondert oder ergänzend ab. Die aktuelle Transferbewertung für die OpenAI-API ist kein Ersatz für diese Prüfung zwischen Auftraggeber und Auftragnehmer.

§ 9 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten nachzuweisen. Geeignete Nachweise können insbesondere Dokumentationen, aktuelle Prüfberichte, Zertifizierungen oder Auskünfte zu den TOMs sein.

(2) Der Auftraggeber darf Kontrollen selbst oder durch einen zur Vertraulichkeit verpflichteten Prüfer durchführen. Vor-Ort-Inspektionen sind mindestens 14 Tage vorher anzukündigen, während der üblichen Geschäftszeiten durchzuführen und so zu planen, dass Betrieb, Sicherheitsinteressen und Rechte anderer Kunden angemessen

berücksichtigt werden.

§ 10 Rückgabe und Löschung

(1) Nach Beendigung der Verarbeitungsleistungen gibt der Auftragnehmer die im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Auftraggebers zurück oder löscht sie und löscht vorhandene Kopien, soweit keine unions- oder mitgliedstaatliche Aufbewahrungspflicht entgegensteht.

(2) Auf Wunsch des Auftraggebers stellt der Auftragnehmer die Daten vor der Löschung in einem gängigen, maschinenlesbaren Format bereit, soweit dies im Rahmen der vertraglich vereinbarten Funktionen möglich ist. Die Löschung erfolgt grundsätzlich innerhalb von 30 Tagen nach Vertragsende; gesetzlich erforderliche oder technisch unvermeidbare Sicherungskopien werden im regulären Sicherungszyklus gelöscht und bis dahin nicht aktiv verarbeitet.

(3) Der Auftragnehmer bestätigt die Löschung auf Anfrage in Textform.

§ 11 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Übermittlung personenbezogener Daten, der Weisungen und der Verarbeitung in seinem Verantwortungsbereich verantwortlich. Er wahrt insbesondere die Rechte der betroffenen Personen und stellt sicher, dass die Nutzung von Heddy CRM auf einer geeigneten Rechtsgrundlage erfolgt.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich über Fehler oder Unregelmäßigkeiten, die er bei der Verarbeitung feststellt, und benennt einen Ansprechpartner für Datenschutzfragen im Rahmen dieses Vertrags.

§ 12 Haftung, Laufzeit und Schlussbestimmungen

(1) Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften, insbesondere Art. 82 DSGVO, sowie nach den Regelungen des Hauptvertrags, soweit diese zwingendem Datenschutzrecht nicht entgegenstehen.

(2) Dieser Vertrag tritt mit Abschluss des Hauptvertrags in Kraft und endet mit dessen Beendigung, vorbehaltlich der in diesem Vertrag geregelten Nachwirkungen. Änderungen und Ergänzungen bedürfen der Textform.

(3) Es gilt deutsches Recht, soweit dem keine zwingenden Regelungen entgegenstehen. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.

Anlage 1 – Gegenstand und Einzelheiten der Verarbeitung

Diese Anlage konkretisiert § 1 und § 2 des AVV.

Merkmal	Festlegung
Gegenstand	Bereitstellung, Betrieb, Support und Sicherheit der SaaS-Plattform Heddy CRM.
Dauer	Für die Laufzeit des Hauptvertrags einschließlich der in § 10 geregelten Nachwirkungen.
Art der Verarbeitung	Erheben, Speichern, Ordnen, Abrufen, Übermitteln, Analysieren, Ändern, Löschen sowie Bereitstellen von Funktionen nach Weisung des Auftraggebers.
Zwecke	Kontaktverwaltung, Kommunikationshistorie, Kampagnen- und E-Mail-Funktionen, Lead- und Vertriebsunterstützung, automatisierte Workflows, Reporting und – nur bei aktiver Nutzung – KI-gestützte Entwürfe oder Zusammenfassungen.
Datenarten	Stammdaten und Kontaktdaten; Kommunikations- und Inhaltsdaten; Nutzungs-, Protokoll- und Gerätedaten; vom Auftraggeber eingegebene Notizen, Tags und benutzerdefinierte Felder; gegebenenfalls technische Abrechnungsreferenzen wie eine Stripe-Kunden-ID. Vollständige Zahlungskartendaten werden nicht in Heddy CRM verarbeitet.
Betroffene Personen	Kontakte, Interessenten, Kunden und Geschäftspartner des Auftraggebers sowie dessen Beschäftigte, Nutzer und sonstige autorisierte Personen.
Besondere Kategorien	Nicht als regulärer Verarbeitungszweck vorgesehen. Der Auftraggeber übermittelt sie nur, wenn er dies rechtmäßig angeordnet und die erforderlichen Schutzmaßnahmen getroffen hat.

Hinweis zu KI-Funktionen

Bei einer aktiv verwendeten KI-Funktion können die eingegebene Information und der für die Aufgabe erforderliche Kontext an den eingesetzten KI-Dienst übermittelt werden. Der Auftraggeber beschränkt die Eingaben auf für die Aufgabe erforderliche und rechtmäßig nutzbare Daten. Besondere Kategorien personenbezogener Daten sollen nicht eingegeben werden, sofern die betreffende Verarbeitung nicht ausdrücklich vorgesehen und rechtlich abgesichert ist.

Anlage 2 – Technische und organisatorische Maßnahmen

Stand: 24. September 2026 · Diese Anlage beschreibt die Maßnahmen von Beyond Matrix Solutions LLC für Heddy CRM.

1. Verantwortlichkeiten und Berechtigungen

Zugänge sind auf Personen oder kontrollierte Dienstkonten beschränkt. Berechtigungen richten sich nach der jeweiligen Aufgabe und werden bei Rollenwechseln oder dem Ende einer Zusammenarbeit überprüft und angepasst. Zugriffe auf Kundendaten werden auf den für Betrieb, Support und Sicherheit erforderlichen Umfang begrenzt.

2. Mandanten- und Zwecktrennung

Daten verschiedener Kunden werden logisch getrennt. Zugriffe werden anhand der zugeordneten Organisation und Berechtigung geprüft. Produktiv- und Testverarbeitung werden getrennt; personenbezogene Produktivdaten werden nicht ohne geeignete Grundlage in Testumgebungen übernommen.

3. Übertragung und Speicherung

Datenübertragungen erfolgen über verschlüsselte Verbindungen. Datenbanken, Dateien und Speicherzugänge sind auf erforderliche Systeme und berechtigte Personen beschränkt. Die Kerninfrastruktur für Anwendung, Datenbank, Dateien und Datensicherungen wird bei Hetzner in Deutschland betrieben.

4. Protokollierung und Kontrolle

Sicherheitsrelevante Vorgänge werden im erforderlichen Umfang nachvollziehbar protokolliert. Protokolle unterliegen Zugriffsschutz und zweckbezogenen Löschfristen. Inhaltsdaten und Geheimnisse werden in Protokollen auf das notwendige Maß begrenzt.

5. Verfügbarkeit und Wiederherstellung

Sicherungen dienen der Wiederherstellung bei Datenverlust und technischen Störungen. Sicherungsumfang, Aufbewahrung, Zugriffsschutz und Wiederherstellungsverfahren werden dokumentiert und überprüft. Bereits ausgeführte Löschungen werden bei Wiederherstellungen berücksichtigt.

6. Sicherheitsvorfälle

Für Sicherheitsvorfälle bestehen Zuständigkeiten und ein Ablauf zur Eingrenzung, Bewertung, Dokumentation und rechtzeitigen Information betroffener Auftraggeber. Sicherheitsrelevante Aktualisierungen und erkannte Schwachstellen werden risikogerecht bearbeitet.

7. Auftragskontrolle und Dienstleister

Dienstleister werden vor ihrem Einsatz auf Zweck, Datenbedarf und geeignete Schutzmaßnahmen geprüft. Soweit erforderlich, werden vertragliche Regelungen zur Auftragsverarbeitung geschlossen. Die mit diesem Vertrag genehmigten Unterauftragsverarbeiter ergeben sich aus Anlage 3.

8. Datenschutzorganisation

Personen mit Zugriff auf personenbezogene Daten werden angemessen zur Vertraulichkeit verpflichtet und unterwiesen. Neue Verarbeitungen und Dienstleister werden auf Zweck, Datenbedarf, Betroffenenrechte, Schutzmaßnahmen und mögliche internationale Übermittlungen geprüft. Die Wirksamkeit der Maßnahmen wird regelmäßig und anlassbezogen bewertet.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Stand: 24. September 2026. Diese Liste gilt für die in ihr beschriebene Verarbeitung. Änderungen richten sich nach § 7 dieses Vertrags.

Dienstleister	Leistung / Daten	Ort / Transfer
Hetzner Online GmbH	Betrieb der Kerninfrastruktur für Anwendung, Datenbank, Dateien und Datensicherungen.	Deutschland · Auftragsverarbeitungsvertrag.
OpenAI, L.L.C.	Nur bei aktiv verwendeten KI-Funktionen: Verarbeitung der Eingabe und des für die Aufgabe erforderlichen Kontexts.	Drittlandverarbeitung möglich · geeignete Garantien nach Art. 44 ff. DSGVO und aktuelle Transferbewertung.
Plus Five Five, Inc. (Resend)	Versand von System-, Support- und – soweit eingerichtet – Newsletter-E-Mails.	Drittlandverarbeitung möglich · geeignete Garantien nach Art. 44 ff. DSGVO.

Nicht als Unterauftragsverarbeiter für CRM-Inhalte

Stripe verarbeitet Zahlungsdaten, die Kundinnen und Kunden unmittelbar dort eingeben, für die Zahlungsabwicklung nach den eigenen Bedingungen. Stripe ist deshalb nicht als Unterauftragsverarbeiter für CRM-Inhalte in dieser Anlage geführt.

Drittlanddokumentation

Die Parteien dokumentieren für jeden einschlägigen Drittlandtransfer den gewählten Übermittlungsmechanismus und die erforderlichen ergänzenden Maßnahmen. Für die aktive Nutzung der OpenAI-API ist die aktuelle Transferbewertung zu beachten. Der Auftragnehmer teilt dem Auftraggeber auf Anfrage die für die jeweilige Verarbeitung verfügbaren Informationen mit.

Unterschriften

Dieser Vertrag kann in Textform geschlossen werden. Für eine individuelle Unterzeichnung verwenden die Parteien die folgenden Felder.

Auftraggeber	Auftragnehmer
Ort, Datum: _____ Name, Funktion: _____ Unterschrift: _____	Beyond Matrix Solutions LLC Ort, Datum: _____ Name, Funktion: Seamus Schulze Unterschrift: _____

Dokumentstand

Dieser AVV ersetzt die Fassung AVV-HEDDY-CRM-001 vom 5. August 2026. Er aktualisiert insbesondere die Firma und Anschrift des Auftragnehmers, die Produktbezeichnung Heddy CRM, die Hetzner-basierte Kerninfrastruktur, die Unterauftragsverarbeiterliste und die Verweise auf die aktuellen Rechtstexte.

Online-Fassung: https://heddycrm.de/avv · TOMs: https://heddycrm.de/toms · Unterauftragsverarbeiter: https://heddycrm.de/subprocessors