

AUFTRAGSVERARBEITUNGSVERTRAG

(AVV) · für die Nutzung von **Truffalo.ai**

gemäß Artikel 28 Absatz 3 DSGVO

zwischen **[Vertragspartner / Kunde]**

[Anschrift, Firmenbuchnummer]

(Verantwortlicher, im Folgenden „ihr“)

und **truffalo GmbH**,

Güterslohgasse 3/3/1, 1220 Wien

FN 683027 b

(Auftragsverarbeiter, im Folgenden „wir“)

Präambel

Wir wissen, wie viel Vertrauen es braucht, Unternehmensdaten in fremde Hände zu geben. Dieses Vertrauen möchten wir schützen – deshalb zeigen wir euch direkt zu Beginn, welche **vier Grundsätze** uns beim Umgang mit euren Daten leiten:

01

Zero-Data-Retention

Jede KI-Anfrage wird nach Beantwortung verworfen, nicht gespeichert. Training nur mit eurer ausdrücklichen Zustimmung.

02

BYOK – euer eigener Schlüssel

Eigener API-Schlüssel, eigene Verschlüsselung: freie Wahl von Anbieter, Region und Vertrag – transparent, ohne Zwischenmarge.

03

Relevanzfilter

Nur Inhalte mit Kunden- oder Vertriebsbezug gehen in die KI-Verarbeitung. Privates bleibt außen vor – konfigurierbar.

04

Planbare Kosten

Dashboard, Alarmschwellen und intelligentes Modell-Routing halten eure KI-Kosten jederzeit im Blick.

Eure Geschäftskommunikation wird grundsätzlich nicht Teil fremder KI-Modelle. Unsere KI-Anfragen laufen über Verträge mit **Zero-Data-Retention**-Zusicherung – das bedeutet, dass jede Anfrage nach Beantwortung verworfen und nicht gespeichert wird. Eine Nutzung zu Trainingszwecken findet nicht ohne eure Zustimmung statt.

Ihr behaltet die Kontrolle über euren Schlüssel (**BYOK**, „bring your own key“): Mit eurem eigenen API-Schlüssel und euren eigenen Verschlüsselungsschlüsseln entscheidet ihr frei über Anbieter, Region und Vertrag – transparent, ohne Zwischenmarge und mit voller Kontrolle, falls ihr die Zusammenarbeit einmal beenden solltet. Das erleichtert euch auch die interne IT- und Datenschutzfreigabe.

Wir verarbeiten nur, was geschäftlich relevant ist. Ein **Relevanzfilter** lässt ausschließlich Inhalte mit Kunden- oder Vertriebsbezug in die KI-Verarbeitung – Privates und geschützte Mitarbeiterkommunikation bleiben außen vor. Ihr könnt auch selbst Ausschlusslisten konfigurieren. Das ist Datenminimierung als Architekturprinzip und schafft eine klare Grundlage für interne Freigaben, etwa durch euren Betriebsrat.

Eure **Kosten** bleiben jederzeit planbar. Über ein Dashboard, konfigurierbare Alarmschwellen und ein intelligentes Modell-Routing behaltet ihr eure KI-Kosten im Blick und im Griff – ohne unangenehme Überraschungen.

Diese Grundsätze prägen unsere Zusammenarbeit – die folgenden Regelungen setzen sie im Einzelnen um.

1. Worum geht es in diesem Vertrag?

Mit diesem Vertrag verpflichtet ihr uns, eure personenbezogenen Daten, also die personenbezogenen Daten, die ihr im Zusammenhang mit unserer cloudbasierten, KI-gestützten Plattform Truffalo.ai nutzt, nach euren Weisungen und gemäß der Datenschutz-Grundverordnung (DSGVO) zu verarbeiten. Dieser Vertrag ergänzt und konkretisiert unsere datenschutzrechtlichen Pflichten aus dem Hauptvertrag.

Der Vertrag beginnt mit Unterzeichnung und gilt für die Dauer eures Hauptvertrags zur Nutzung von Truffalo.ai. Was nach Vertragsende mit euren Daten passiert, regelt [Abschnitt 5](#).

Bitte beachtet, dass ihr selbst und allein darüber entscheidet, zu welchem Zweck und auf welche Weise die personenbezogenen Daten, die ihr selbst bereitstellt, verarbeitet werden. Es liegt in eurer Verantwortung sicherzustellen, dass die beauftragte Verarbeitung zulässig ist, dass eine passende Rechtsgrundlage nach Art. 6 DSGVO (und ggf. Art. 9 DSGVO) vorliegt und dass die Rechte der betroffenen Personen auch gegenüber Dritten gewahrt werden. Denn wir verarbeiten ganz automatisch nur die Daten, die ihr uns gebt – wir holen sie uns nicht von alleine.

2. Was machen wir mit euren Daten?

Wir verarbeiten eure personenbezogenen Daten, um euch folgende Leistungen zu ermöglichen:

- Automatisierung und Analyse von Vertriebsprozessen
- Auswertung von Kundenbeziehungen
- Identifikation von Verkaufschancen
- Früherkennung von Risiken (wie Kundenabwanderung)
- Zusammenführung und Auswertung eurer Unternehmensdaten aus verschiedenen Systemen
- KI-gestützte Entscheidungsunterstützung und Empfehlungen für eure Mitarbeiter
- Automatisierte Anlage und Aktualisierung von Aufgaben und CRM-Daten
- Workflow- und Prozessautomatisierung

Unsere Plattform unterstützt euch durch Analysen und Empfehlungen, trifft aber keine Entscheidungen mit rechtlicher Wirkung für Betroffene.

3. Wer ist von der Datenverarbeitung betroffen und welche Daten sind das?

Betroffene Personen:

- Eure Mitarbeitenden (z. B. im Vertrieb, Key Account Management, Management)
- Eure Kunden, Geschäftspartner und Ansprechpartner

Kategorien von Daten:

- Stammdaten (Name, Position, Firma, Kontaktdaten)
- Kommunikationsdaten (E-Mail, Chat, Telefon, Meetingprotokolle, Kalender)
- CRM/ERP-Daten (Angebote, Verträge, Support- und Kaufhistorie)
- Aufgaben, Notizen, Kommentare
- Benutzerkennungen, Rollen, Rechte
- Inhalte aus Dokumenten (PDF, Word, Excel, Präsentationen)
- Daten aus angebundenen Systemen (HR, Support, Analytics, Unternehmensdatenbanken)
- Öffentliche Firmeninformationen (Presse, Finanzdaten, Marktinformationen)

Eine detaillierte Übersicht über den Gegenstand und Zweck der Verarbeitung, die verarbeiteten Datenkategorien und die betroffenen Personengruppen findet ihr in [Anlage 1](#).

4. Wie läuft die technische Verarbeitung eurer Daten ab?

Wir empfangen Daten aus euren Unternehmenssystemen (z. B. CRM, ERP, Kommunikation) und externen Quellen. Diese Daten werden zentral in unserer KI-Plattform zusammengeführt, analysiert und ausgewertet. Die Ergebnisse und Empfehlungen werden euch beispielsweise per E-Mail oder Chat zur Verfügung gestellt.

KI-Modelle setzen wir nur im Rahmen eurer Vorgaben und Weisungen ein – ihr selbst entscheidet, welche Daten unser System verarbeitet, indem ihr sie hinzufügt. Die von uns eingesetzten externen KI-Anbieter sind als Unterauftragsverarbeiter nach Maßgabe von [Abschnitt 8](#) und [9](#) sowie [Anlage 3](#) vertraglich eingebunden; wir übermitteln personenbezogene Daten an sie nur im Rahmen dieser Regelungen und soweit datenschutzrechtlich zulässig. Unsere KI-Agenten handeln ausschließlich im Rahmen eurer festgelegten Rollen, Berechtigungen und Regeln („Guardrails“).

5. Was müssen wir als euer Auftragsverarbeiter tun?

- Wir verarbeiten eure personenbezogenen Daten so, dass sie sinnvoll für ein bestmögliches Ergebnis („truffle Card“ = Handlungsempfehlung) sind. Solange Weisungen von euch damit vereinbar sind, setzen wir sie um. Gesetzliche Pflichten bleiben davon unberührt; in solchen Fällen informieren wir euch vorab, sofern rechtlich zulässig. Sollten wir der Auffassung sein, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, weisen wir euch unverzüglich darauf hin.
- Alle unsere Mitarbeitenden und sonstigen Personen, die mit euren Daten arbeiten, sind schriftlich zur Vertraulichkeit verpflichtet und entsprechend geschult.
- Die Verarbeitung erfolgt je nach eingesetztem Unterauftragsverarbeiter innerhalb der EU/des EWR oder – unter den Voraussetzungen der Art. 44 ff. DSGVO – in Drittländern (siehe [Anlage 3](#)). Wir unterstützen euch bei der Wahrnehmung von Betroffenenrechten, bei Datenschutz-Folgenabschätzungen und gesetzlichen Meldepflichten.
- Wir führen ein Verzeichnis unserer Verarbeitungstätigkeiten und dokumentieren alle relevanten Prozesse.
- Wir informieren euch unverzüglich über Störungen, Verdachtsfälle auf Datenschutzverletzungen oder sicherheitsrelevante Vorfälle (unser Vorgehen dazu findet ihr in [Anlage 2](#), Incident-Response-Management).

Nach Vertragsende löschen oder geben wir euch sämtliche personenbezogenen Daten sowie alle Kopien und Datenträger nach eurer Wahl zurück, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Befinden sich personenbezogene Daten in Datensicherungen (Backups), löschen wir diese im Rahmen des regulären Backup-Rotationszyklus, spätestens jedoch innerhalb von [z. B. 60]

Tagen nach Vertragsende. Während dieser Zeit sind die Daten gesperrt und werden nicht mehr verarbeitet. Trefft ihr innerhalb von 14 Tagen nach Vertragsende keine ausdrückliche Wahl zwischen Rückgabe und Löschung, löschen wir die personenbezogenen Daten. Die Löschung bestätigen wir euch schriftlich.

Vertragsende Wahlrecht startet Ihr habt 14 Tage Zeit, euch zwischen Rückgabe und Löschung eurer Daten zu entscheiden.	+ 14 Tage Keine Wahl getroffen? Ohne ausdrückliche Wahl löschen wir die personenbezogenen Daten automatisch.	≤ [60] Tage Backups Daten in Sicherungen sind bis dahin gesperrt und werden im regulären Backup-Zyklus gelöscht (<i>Beispielwert – Frist im Vertrag festzulegen</i>).
---	--	---

6. (Wie) Könnt ihr uns neue Weisungen geben oder bestehende ändern?

Ihr könnt uns jederzeit neue Weisungen zur Datenverarbeitung geben oder bestehende ändern. Bitte teilt uns diese per E-Mail mit. Wir dokumentieren alle Weisungen und informieren euch, falls wir eine Weisung aus rechtlichen Gründen nicht umsetzen können. Wer bei euch berechtigt ist, uns Weisungen zu erteilen, und wer sie bei uns entgegennimmt, ist in [Anlage 1](#) benannt.

7. Wie schützen wir eure Daten technisch und organisatorisch?

Wir setzen alle erforderlichen technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 DSGVO um und halten sie auf dem aktuellen Stand. Dazu gehören insbesondere:

- Rollenbasierte Zugriffskonzepte und Guardrails
- Verschlüsselung von Daten bei Übertragung und Speicherung
- Protokollierung aller Zugriffe und Verarbeitungsvorgänge
- Trennung eurer Daten von anderen Kunden (Mandantentrennung)
- Integritäts- und Verfügbarkeitskontrollen
- Regelmäßige Überprüfung, Bewertung und Aktualisierung der Maßnahmen
- Schutz vor unbefugtem Zugriff (z. B. Firewalls, Zugangskontrollen)

Wir informieren euch unverzüglich über wesentliche Änderungen der TOMs. Eine aktuelle Übersicht unserer TOMs findet ihr in [Anlage 2](#).

8. Setzen wir Unterauftragsverarbeiter ein?

Wir setzen weitere Unterauftragsverarbeiter ein, zum Beispiel Hosting-Provider oder Anbieter von KI-Modellen. Ihr erteilt uns hierfür eine generelle Zustimmung.

Bevor wir einen neuen Unterauftragsverarbeiter einsetzen oder einen bestehenden austauschen, informieren wir euch aktiv und rechtzeitig per E-Mail. In dieser E-Mail nennen wir euch den Namen des Unterauftragsverarbeiters, die geplante Tätigkeit und das Datum des geplanten Einsatzes.

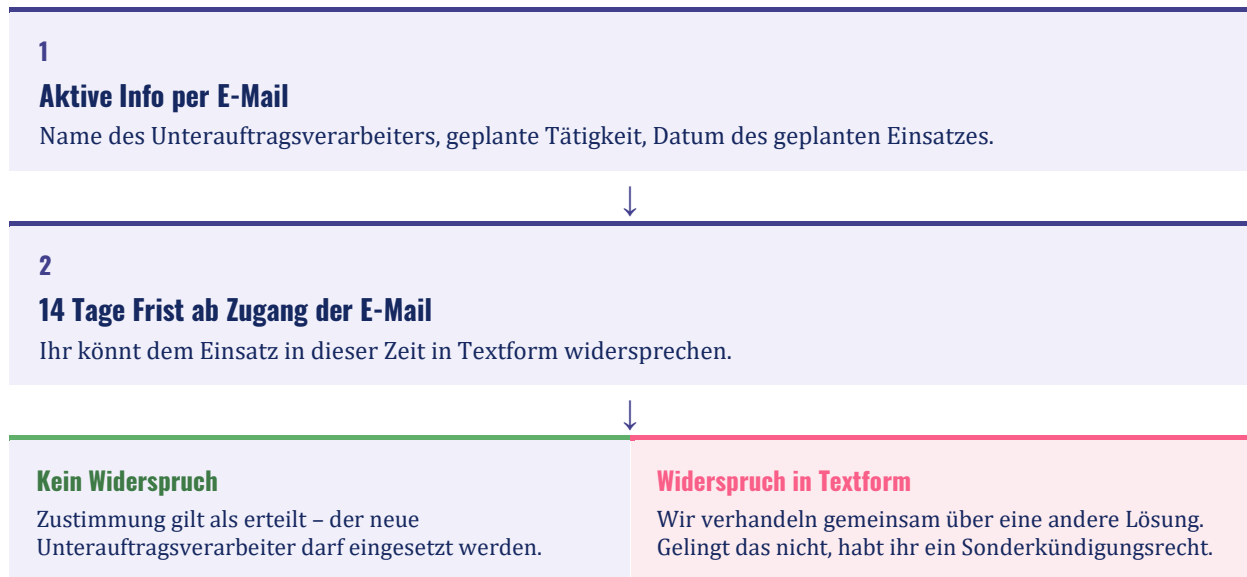
Ihr habt ab Zugang der E-Mail 14 Tage Zeit, dem Einsatz oder Wechsel des Unterauftragsverarbeiters in Textform, also z. B. per E-Mail, zu widersprechen. Widerspricht ihr innerhalb dieser Frist nicht, gilt

eure Zustimmung als erteilt und wir dürfen den genannten Unterauftragsverarbeiter einsetzen. Wir verpflichten alle Unterauftragsverarbeiter zur Einhaltung dieses Vertrags und der DSGVO.

Solltet ihr widersprechen, verpflichten wir uns beide, über eine andere Lösung zu verhandeln. Sollten wir keine andere Lösung finden, z. B. weil wir auf den neuen Unterauftragsverarbeiter angewiesen sind, so habt ihr ein Sonderkündigungsrecht.

Die aktuelle Liste der von uns eingesetzten Unterauftragsverarbeiter findet ihr in [Anlage 3](#) sowie unter: truffalo.ai/subprocessors.html

Der Ablauf im Überblick:



9. Werden Daten außerhalb der EU verarbeitet?

Gleicher Ablauf wie bei **Unterauftragsverarbeitern (§ 8)**:
E-Mail-Info → 14 Tage Widerspruchsfrist → bei Widerspruch Verhandlung, sonst Sonderkündigungsrecht.

Ja, in bestimmten Fällen verarbeiten wir eure personenbezogenen Daten auch in einem Drittland, also außerhalb der EU/des EWR – zum Beispiel beim Einsatz einzelner Unterauftragsverarbeiter (siehe [Anlage 3](#)) oder externer KI-Anbieter. Ihr erteilt uns hierfür eine generelle Zustimmung, sofern die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss oder Standardvertragsklauseln).

Bevor wir eine neue Verarbeitung in einem bislang nicht genutzten Drittland aufnehmen oder das eingesetzte Drittland wechseln, informieren wir euch aktiv und rechtzeitig per E-Mail. In dieser E-Mail nennen wir euch das betroffene Drittland, den Zweck der Verarbeitung sowie die eingesetzten Garantien (z. B. Standardvertragsklauseln).

Ihr habt ab Zugang der E-Mail 14 Tage Zeit, der Verarbeitung in diesem Drittland in Textform, also z. B. per E-Mail, zu widersprechen. Widersprecht ihr innerhalb dieser Frist nicht, gilt eure Zustimmung als erteilt.

Solltet ihr widersprechen, verpflichten wir uns beide, über eine andere Lösung zu verhandeln. Finden wir keine Lösung, z. B. weil wir auf die Verarbeitung in diesem Drittland angewiesen sind, habt ihr ein Sonderkündigungsrecht.

10. Wie unterstützen wir euch bei Betroffenenrechten und anderen Pflichten?

- Wir helfen euch, Anfragen von betroffenen Personen (z. B. Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit) fristgerecht zu erfüllen.
- Wir unterstützen euch bei Datenschutz-Folgenabschätzungen und behördlichen Vorabkontrollen.
- Wir melden jede Datenschutzverletzung unverzüglich und helfen euch bei der Erfüllung von Meldepflichten gegenüber Behörden und Betroffenen.

11. Wie könnt ihr kontrollieren, was wir mit euren Daten tun?

Ihr dürft jederzeit prüfen, ob wir die gesetzlichen und vertraglichen Datenschutzvorgaben einhalten – zum Beispiel durch Audits oder Inspektionen.

Kontrollen erfolgen mit angemessener Vorankündigung während der üblichen Geschäftszeiten und unter Wahrung der Vertraulichkeit und der Rechte anderer Kunden. Wir unterstützen euch dabei und stellen alle erforderlichen Informationen und Nachweise zur Verfügung.

12. Wie gehen wir mit KI-Modellen und Prompts um?

- Wir nutzen KI-Modelle und Agenten ausschließlich zur Vertragserfüllung für euch.
- Personenbezogene Daten, die für KI-Verarbeitung (z. B. Prompts, Dokumenteninhalte) genutzt werden, verwenden wir nicht für andere Zwecke, insbesondere nicht zum Training externer KI-Modelle – außer, ihr stimmt ausdrücklich zu.
- Auswahl und Konfiguration der eingesetzten KI-Modelle werden dokumentiert und auf euren Wunsch mit euch abgestimmt, es sei denn, es handelt sich dabei um Standardeinstellungen.

13. Was dokumentieren wir für euch?

- Wir dokumentieren alle wesentlichen Verarbeitungsschritte und stellen euch auf Anfrage Nachweise zur Verfügung.
- Alle Verarbeitungen werden nachvollziehbar protokolliert (z. B. Zugriffsprotokolle, Bearbeitungsverläufe).

14. Wer haftet, wenn etwas schiefgeht?

a) Ihr nutzt die Plattform auf eigene Verantwortung

Wenn ihr unsere Plattform und die von der Künstlichen Intelligenz (KI) erzeugten Ergebnisse, Analysen oder Empfehlungen verwendet, tut ihr das auf eigenes Risiko. Ihr entscheidet selbst, welche Informationen ihr der KI zuführt und wie ihr sie nutzt.

b) Wir übernehmen keine Garantie für die Ergebnisse

Wir können euch nicht zusichern, dass die von der KI gelieferten Ergebnisse – auch wenn wir sie euch als Möglichkeit präsentieren – immer richtig, vollständig, aktuell oder für euren speziellen Zweck geeignet oder umsetzbar sind. Die Vorschläge und Analysen der Plattform sind keine professionelle Beratung – sie sollen euch lediglich bei euren Entscheidungen unterstützen.

c) Ihr prüft die Ergebnisse selbst

Bitte prüft alle von der Plattform gelieferten Ergebnisse eigenständig, bevor ihr darauf aufbaut oder wichtige Entscheidungen trefft. Die Verantwortung für die Nutzung der KI-Ergebnisse liegt bei euch.

d) Wir haften nicht für Folgen aus den KI-Ergebnissen

Wir übernehmen keine Haftung für Schäden, die daraus entstehen, dass ihr auf Basis der KI-Ergebnisse handelt oder diese nutzt – dazu zählen auch entgangene Gewinne oder andere Folgeschäden. Das gilt auch dann, wenn Entscheidungen oder Maßnahmen auf Empfehlungen oder Analysen der Plattform beruhen.

e) Die Ergebnisse hängen von eurem Umgang mit der KI ab

Die Qualität der Ergebnisse hängt stark davon ab, welche Daten und Eingaben ihr macht und wie ihr die Plattform einsetzt. Wir haften nicht für Fehler oder Schäden, die entstehen, weil Eingaben falsch, unvollständig oder ungeeignet waren oder die Plattform nicht sachgemäß genutzt wurde.

f) Wann haften wir trotzdem?

Dieser Haftungsausschluss gilt nicht, wenn wir vorsätzlich oder grob fahrlässig gegen unsere Pflichten verstoßen oder wenn uns das Gesetz zwingend eine Haftung vorschreibt.

Wie regeln wir die Haftung untereinander bei Datenschutzverstößen?

Verstößt jemand von uns beiden gegen die DSGVO oder gegen diesen Vertrag und wird die jeweils andere Partei deshalb von einer betroffenen Person, einer Behörde oder einem Dritten in Anspruch genommen (z. B. auf Schadenersatz nach Art. 82 DSGVO oder durch ein Bußgeld nach Art. 83 DSGVO), stellt die verursachende Partei die andere Partei von sämtlichen Ansprüchen frei, soweit die Inanspruchnahme auf ihrem Verstoß beruht.

Haften wir beide gegenüber einer betroffenen Person als Gesamtschuldner (Art. 82 Abs. 4 DSGVO), richtet sich der Ausgleich im Innenverhältnis nach Art. 82 Abs. 5 DSGVO und danach, welcher Anteil am Schaden auf welche Partei entfällt.

Die Freistellungspflicht setzt voraus, dass die in Anspruch genommene Partei die andere Partei unverzüglich über die Inanspruchnahme informiert, ihr angemessen Gelegenheit zur Stellungnahme und Verteidigung gibt und ohne deren vorherige Abstimmung keine Anerkenntnisse oder Vergleiche abgibt.

Diese Regelung gilt zusätzlich zu und unabhängig von den restlichen Regelungen in [Abschnitt 14](#). Sie schränkt weder die gesetzliche Haftung nach Art. 82 DSGVO gegenüber betroffenen Personen noch behördliche Sanktionsbefugnisse nach Art. 83 DSGVO ein und lässt eine zwingende gesetzliche Haftung unberührt.

15. Wie gehen wir gemeinsam mit vertraulichen Informationen um?

Wir verpflichten uns beide, alle Informationen aus diesem Vertrag und dem Basis-Auftrag sowie alle im Rahmen unserer Zusammenarbeit gewonnenen Kenntnisse über interne Abläufe, Unternehmensdaten und Sicherheitsmaßnahmen der jeweils anderen Partei streng vertraulich zu behandeln. Wir beide dürfen sie nur weitergeben, wenn eine gesetzliche Pflicht zur Auskunft besteht.

16. Wer ist euer Ansprechpartner und wer ist unser Ansprechpartner?

Euer Ansprechpartner bei truffalo.ai:

[Name, Funktion, Kontakt]

Unser Ansprechpartner bei euch:

[Name, Funktion, Kontakt]

17. Was gilt bei Änderungen oder Unwirksamkeit einzelner Klauseln?

- Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform.
- Sollte eine Bestimmung dieses Vertrags ganz oder teilweise unwirksam, undurchführbar oder nichtig sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt. Die Parteien verpflichten sich, die unwirksame, undurchführbare oder nichtige Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck und dem Sinn der ursprünglichen Bestimmung möglichst nahekommt.
- Diese Vereinbarung unterliegt österreichischem Recht unter Ausschluss des UN-Kaufrechts. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist – soweit gesetzlich zulässig – das sachlich zuständige Gericht in Wien.

Ort, Datum

Verantwortlicher

Ort, Datum

Auftragsverarbeiter

Anlagen

- **Anlage 1:** Gegenstand des Auftrags
- **Anlage 2:** Technische und organisatorische Maßnahmen
- **Anlage 3:** Unterauftragsverarbeiter

Anlage 1 – Gegenstand des Auftrags

Gegenstand und Zweck	Datenkategorien	Personengruppen	Weisungsberechtigt bei euch	Weisungsempfänger bei uns
Bereitstellung der Software über das Internet (Hosting, Wartung, Betrieb)	Vorname, Nachname, Firma, Abteilung, Position, Kontaktdaten, Adressdaten, Bankdaten, Vertragsdaten, Auftrags- und Lieferdaten, Nutzungsdaten, Bilddaten, Positionsdaten, Nachrichteninhalte, Metadaten, Audio- und Sprachdaten	Beschäftigte des Auftragsverarbeiters; Kunden und Interessent:innen (Leads/Prospects) des Auftraggebers, insb. Ansprechpartner:innen bei dessen Geschäftskunden, deren Kontakt- und Kommunikationsdaten aus angebundenen Quellsystemen (z. B. CRM, E-Mail-Postfächer) verarbeitet werden; ggf. sonstige externe Kontaktpersonen (z. B. Geschäftspartner, Lieferanten des Auftraggebers), sofern deren Daten im Rahmen der angebundenen Systeme miterfasst werden	[von euch zu benennen]	Elemer Melik

Anlage 2 – Technische und organisatorische Maßnahmen

Maßnahme	Umsetzung
Zutrittskontrolle	Schutz der Räume vor unbefugtem Zutritt (z. B. durch Schließsysteme).
Zugangskontrolle	Login mit Benutzername und Passwort, Login mit biometrischen Daten, Software-Firewall, Verschlüsselung von stationären Datenträgern, automatische Desktopsperre, Passwort-Manager, Verwaltung von Benutzerberechtigungen, Erstellung von Benutzerprofilen, Richtlinie „Sicheres Passwort“, Anleitung „Manuelle Desktopsperre“.
Zugriffskontrolle	Physische Löschung von Datenträgern vor Wiederverwendung/Entsorgung, Protokollierung von Zugriffen auf Anwendungen (insbesondere bei Eingabe, Änderung und Löschung von Daten), Einsatz von Berechtigungskonzepten, minimale Anzahl an Administrator:innen, Verwaltung der Benutzerrechte durch Administrator:innen.
Trennungskontrolle	Trennung von Produktiv- und Testumgebung, physikalische Trennung (Systeme/Datenbanken/Datenträger), Mandantenfähigkeit relevanter Anwendungen, Steuerung über Berechtigungskonzept.
Pseudonymisierung	Es ist keine Pseudonymisierung von Daten vorgesehen.
Weitergabekontrolle	Bereitstellung über verschlüsselte Verbindungen (z. B. SFTP, HTTPS/TLS), Nutzung von Signaturverfahren, Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen, Übersicht über regelmäßige Abruf- und Übermittlungsvorgänge.
Eingabekontrolle	Manuelle oder automatisierte Kontrolle der Protokolle, Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können, Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen).
Verfügbarkeitskontrolle	Backup- und Recovery-Konzept, Kontrolle des Sicherungsvorgangs.
Datenschutzmanagement	Einsatz von Firewall und regelmäßige Aktualisierung, Einsatz von Spamfilter und regelmäßige Aktualisierung, Einbindung des/der Datenschutzbeauftragten bei Sicherheitsvorfällen und Datenpannen.
Incident-Response-Management	Definierte interne Verantwortlichkeiten (CTO, Boris Fedotov), Risikoklassifizierung, Sofortmaßnahmen zur Eindämmung (Isolierung betroffener Systeme, Sperrung von Zugängen), Meldung an euch binnen 48 Stunden nach Kenntnisnahme.
Datenschutzfreundliche Voreinstellungen	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind; ein formaler Prozess für die Einführung neuer Verarbeitungstätigkeiten berücksichtigt Datensparsamkeit bereits bei der Konzeption.
Auftragskontrolle (Outsourcing an Dritte)	Auswahl der Auftragnehmer:innen unter Sorgfaltsgesichtspunkten (insbesondere in Bezug auf Datenschutz und Datensicherheit).

Anlage 3 – Unterauftragsverarbeiter

Wir nehmen für die Verarbeitung eurer Daten die Leistungen folgender Unterauftragsverarbeiter in Anspruch:

Anbieter	Anschrift	Drittland	Leistung
Anthropic	Anthropic PBC, 548 Market Street, PMB 90375, San Francisco, CA 94104, USA	USA (mit EU Model Routes)	Erfasste Inhalte, die über das Vercel AI Gateway an große Sprachmodelle gesendet werden – Parsing, Cards, Deals, Chat, Anreicherung.
OpenAI	OpenAI Ireland Limited, 1st Floor, The Watermarque Building, South Lotts Road, Ringsend, Dublin 4, Irland	USA (mit EU Model Routes)	Erfasste Inhalte, die über das Vercel AI Gateway an große Sprachmodelle gesendet werden – Parsing, Cards, Deals, Chat, Anreicherung.
Google	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland	USA (mit EU Model Routes)	Erfasste Inhalte, die über das Vercel AI Gateway an große Sprachmodelle gesendet werden – Parsing, Cards, Deals, Chat, Anreicherung; Drive- und Chat-Inhalte.
Vercel	Vercel Inc., 650 California Street, San Francisco, CA 94108, USA	USA / EU-Region (Edge)	Hosting, Serverless-Funktionen und Edge – sämtliche Anwendungsdaten während der Übertragung; betreibt zudem das AI Gateway.
Neon (Postgres)	160 Spear Street, 13th Floor, San Francisco, CA 94105/94104, USA	USA	Sämtliche personenbezogenen Daten – Kunden, Kontakte, Nutzer, Quellen.
Cloudflare R2	Cloudflare Inc., 101 Townsend Street, San Francisco, CA 94107, USA	USA	Geparste Content-Blobs (Markdown), Logos, Avatare; betreibt zudem den EU-PDF-Render-Worker.
Upstash (Redis)	[Anschrift noch zu ergänzen – bekannt ist bislang nur der Sitz in San Jose, California, USA (Delaware Corp.)]	USA	Kurzfristiger Agent-Speicher.
Nylas	Nylas, Inc., 944 Market Street, San Francisco, CA 94102, USA	USA	E-Mail-Inhalte (lesend) und ausgehende E-Mails der Plattform.
Telegram	[noch zu klären – Telegram veröffentlicht keine öffentliche Geschäftsadresse; bekannt ist nur der Unternehmenssitz in Dubai, VAE]	Drittland (VAE) – kein AVV mit Telegram abschließbar	Eingehende Text- und Sprachnachrichten.

Glossar

Die wichtigsten Begriffe aus diesem Vertrag – kurz und verständlich erklärt.

Begriff	Erklärung
Verantwortlicher	Wer über Zweck und Mittel der Datenverarbeitung entscheidet – in diesem Vertrag seid das ihr.
Auftragsverarbeiter	Wer personenbezogene Daten im Auftrag und nach Weisung eines anderen verarbeitet – hier: wir.
Personenbezogene Daten	Alle Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen, z. B. Name, E-Mail-Adresse oder Kundennummer.
DSGVO	Die Datenschutz-Grundverordnung – das zentrale EU-Gesetz zum Schutz personenbezogener Daten.
Auftragsverarbeitungsvertrag (AVV)	Vertrag nach Art. 28 DSGVO, der die Datenverarbeitung durch einen Dienstleister rechtlich regelt – genau dieses Dokument.
Unterauftragsverarbeiter	Ein weiterer Dienstleister, den der Auftragsverarbeiter zur Erfüllung seiner Aufgabe hinzuzieht, z. B. ein Hosting- oder KI-Anbieter.
Drittland	Ein Land außerhalb der EU/des EWR, in dem ein mit der EU vergleichbares Datenschutzniveau nicht automatisch gewährleistet ist.
Standardvertragsklauseln (SCC)	Von der EU-Kommission vorformulierte Vertragsklauseln, die ein angemessenes Datenschutzniveau bei Übermittlungen in Drittländer sicherstellen.
Angemessenheitsbeschluss	Entscheidung der EU-Kommission, dass ein bestimmtes Land ein mit der EU vergleichbares Datenschutzniveau bietet.
TOM (Technische und organisatorische Maßnahmen)	Konkrete Schutzmaßnahmen wie Verschlüsselung oder Zugriffskontrollen, die Daten vor Missbrauch und Verlust schützen.
Betroffene Person	Die Person, um deren Daten es geht, z. B. ein Kunde, Mitarbeiter oder Geschäftspartner.
Datenschutz-Folgenabschätzung (DSFA)	Eine Risikoprüfung, die vor besonders sensiblen Datenverarbeitungen durchgeführt werden muss.
Gesamtschuldner	Wenn mehrere Parteien gemeinsam für denselben Schaden haften und jede von ihnen einzeln in voller Höhe in Anspruch genommen werden kann.
Zero-Data-Retention	Grundsatz, wonach KI-Anfragen nach ihrer Beantwortung nicht gespeichert, sondern verworfen werden.
BYOK (Bring Your Own Key)	Ihr nutzt euren eigenen Verschlüsselungs- bzw. API-Schlüssel, statt einen von uns bereitgestellten.