

AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

Zwischen

Dem Kunden gemäß Bezeichnung im Hauptvertrag
(nachfolgend „**Verantwortlicher**“)

und

TNT Ventures GmbH

Venloer Str. 240
50823 Köln, Deutschland

Eingetragen beim Amtsgericht Köln, HRB 125080
Vertreten durch die Geschäftsführer: Felix Schürholz, Lukas Schaefer

(nachfolgend „**Auftragsverarbeiter**“)

(gemeinsam die „**Parteien**“).

1. Präambel

Dieser Auftragsverarbeitungsvertrag („AVV“) ist Bestandteil der Nutzungsbedingungen („Hauptvertrag“) zwischen den Parteien über die Nutzung des Produkts „**drall.ai**“. Er gilt, soweit der Auftragsverarbeiter im Rahmen der Erbringung der im Hauptvertrag definierten Leistungen (die „Leistungen“) personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

2. Umfang und Verantwortlichkeit

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Auftrag des Verantwortlichen und gemäß dessen dokumentierten Weisungen (Art. 28 DSGVO). Der Hauptvertrag und dieser AVV stellen die dokumentierten Weisungen dar.
- (2) Der Verantwortliche ist allein für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (z. B. für die Einholung erforderlicher Einwilligungen von Nutzern, die zur Nutzung und Zusammenarbeit innerhalb des Tools eingeladen werden).

3. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter gewährleistet, dass er:

- (a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeitet, einschließlich in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland, sofern er nicht durch geltendes Recht hierzu verpflichtet ist.
- (b) sicherstellt, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben.
- (c) alle gemäß Artikel 32 DSGVO erforderlichen Maßnahmen (Sicherheit der Verarbeitung) ergreift.
- (d) den Verantwortlichen bei der Einhaltung der Pflichten gemäß den Artikeln 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, DSFA) unterstützt. Gemäß DSGVO (Art. 33) gewährleistet der Auftragsverarbeiter im unwahrscheinlichen Fall eines bestätigten Sicherheitsvorfalls, der personenbezogene Kundendaten betrifft, eine schriftliche Benachrichtigung des Verantwortlichen unverzüglich und spätestens innerhalb von 72 Stunden nach

Bekanntwerden der Verletzung.

(e) nach Beendigung der Erbringung der mit der Verarbeitung verbundenen Leistungen nach Wahl des Verantwortlichen alle personenbezogenen Daten an den Verantwortlichen löscht oder zurückgibt und vorhandene Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(f) Kundinhalte nicht zu Trainingszwecken verwendet und sicherstellt, dass auch seine Unterauftragsverarbeiter dies gemäß den Bedingungen ihrer jeweiligen API- oder Auftragsverarbeitungsverträge (AVV) nicht tun dürfen.

4. Unterauftragsverarbeitung

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zur Beauftragung von Unterauftragsverarbeitern. Die aktuelle Liste der Unterauftragsverarbeiter ist in Anlage III aufgeführt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder des Austauschs weiterer Unterauftragsverarbeiter. Der Verantwortliche kann solchen Änderungen innerhalb von 14 Tagen aus wichtigem Grund widersprechen.

(3) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter, erfolgt dies auf Grundlage eines schriftlichen Vertrags, der dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegt, die in diesem AVV festgelegt sind.

5. Rechte betroffener Personen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, bei der Erfüllung der Pflicht des Verantwortlichen, Anträge zur Ausübung der Rechte betroffener Personen zu beantworten (z. B. Recht auf Auskunft, Löschung).

6. Internationale Datenübermittlungen

Übermittelt der Auftragsverarbeiter personenbezogene Daten in Länder außerhalb der EU/des EWR (z. B. USA), gewährleistet er, dass geeignete Garantien bestehen, etwa das EU-US Data Privacy Framework oder Standardvertragsklauseln (SCCs).

7. Auditrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung dieses AVV nachzuweisen.

(2) Audits und Inspektionen können durch den Verantwortlichen oder einen von ihm beauftragten Prüfer durchgeführt werden. Zur Verringerung des Aufwands erklärt sich der Verantwortliche damit einverstanden, vorrangig auf gültige Sicherheitszertifizierungen oder Auditberichte zurückzugreifen, die vom Auftragsverarbeiter bereitgestellt werden.

ANLAGE I: EINZELHEITEN DER VERARBEITUNG

1. Gegenstand und Dauer der Verarbeitung

Gegenstand ist die Bereitstellung eines KI-gestützten Beratungs-/Strategietools (drall.ai), mit dem Nutzer Beratungs-/Strategieprojekte und Workflows planen, durchführen und dokumentieren können. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags.

2. Art und Zweck der Verarbeitung

- Erstellung individualisierter Wissens- und Kontaktdatenbanken.
- Verwaltung von Nutzerkonten und transaktionale E-Mail-Kommunikation.

3. Kategorien betroffener Personen

- Mitarbeiter, Kunden oder Lieferanten des Verantwortlichen.
- Autorisierte Administratoren des Verantwortlichen.

4. Arten personenbezogener Daten

- **Kontaktdaten:** Vor-/Nachname, E-Mail-Adresse, gegebenenfalls Mobiltelefonnummer.
- **Inhaltsdaten:** Eingaben, die der Verantwortliche bei der Einladung von Nutzern bereitstellt.
- **Nutzungsdaten:** Erstellung oder Bearbeitung von Ergebnissen, Bereitstellung von Eingaben, Zeitstempel, Interaktionsprotokolle.

ANLAGE II: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMs)

Der Auftragsverarbeiter hat die folgenden Maßnahmen umgesetzt, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

1. **Zugriffskontrolle:** Mehrstufige Authentifizierungssicherheit, einschließlich strenger Passwortrichtlinien und Unterstützung für Enterprise-Single-Sign-On-(SSO)-Lösungen (einschließlich SAML 2.0 und OIDC, soweit verfügbar); Beschränkung des Datenzugriffs auf autorisiertes Personal nach dem „Need-to-know“-Prinzip.
 2. **Übertragungskontrolle:** Verschlüsselung von Daten während der Übertragung mittels TLS 1.2 oder höher.
 3. **Datenverschlüsselung:** Verschlüsselung ruhender Daten in der Datenbank (AES-256 oder gleichwertig).
 4. **Verfügbarkeitskontrolle:** Regelmäßige automatisierte Backups; Nutzung redundanter Cloud-Infrastruktur zur Vermeidung von Datenverlust.
 5. **Trennungsgebot:** Logische Trennung der Daten verschiedener Kunden (Multi-Tenancy-Architektur).
-

ANLAGE III: LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche genehmigt die Beauftragung der folgenden Unterauftragsverarbeiter, mit denen jeweils ein Standard-AVV besteht:

Name	Zweck	Standort	Zertifizierungen
Supabase / AWS	Datenbank, Dateispeicherung, Vektorsuche	Frankfurt, Deutschland (EU)	SOC 2 Type II, ISO/IEC 27001
Vercel	Anwendungshosting & CDN	Globales Edge-Netzwerk, EU priorisiert	SOC 2 Type II, ISO/IEC 27001
Microsoft	Microsoft-365-Integration (Graph API)	Eigener Microsoft-365-Tenant Ihres Unternehmens	SOC 1/2/3, ISO 27001, ISO 27018
OpenAI, Anthropic, Google	Anbieter von Foundation Models (Standard-Routing)	Vereinigte Staaten	Training mit Ihren Daten gemäß API-Vertrag ausgeschlossen
melious.ai	EU-gehostete Foundation Models (Enterprise-Option)	EU / EWR	Nur bei aktiviertem EU-only-Routing verwendet
Tavily	Websuche für Recherche-Workflows (Standard-Routing)	Vereinigte Staaten	AVV vorhanden
Linkup	Websuche für Recherche-Workflows (EU-gehostete Alternative zu Tavily)	EU (Frankreich)	Nur bei konfigurierter EU-gehosteter Suche verwendet
LangSmith	KI-Beobachtbarkeit und Debugging	Vereinigte Staaten	AVV vorhanden
Resend	Transaktions- und Einladungs-E-Mails	EU (Irland)	AVV vorhanden

(Hinweis: Übermittlungen in die USA/Drittländer werden durch das EU-US Data Privacy Framework oder Standardvertragsklauseln abgesichert.)

Unterschriften

Für den Verantwortlichen:

(Unterschrift durch digitale Annahme der Bedingungen mittels Kontrollkästchen)

Für den Auftragsverarbeiter:

Lukas Schaefer

Lukas Schaefer, Geschäftsführer
TNT Ventures GmbH