AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

zwischen

Dem im Hauptvertrag genannten Kunden
(im Folgenden **„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
(im Folgenden **„Auftragsverarbeiter“**)

(gemeinsam die **„Parteien“**).

1. Präambel

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

2. Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Auftrag des Verantwortlichen und in Übereinstimmung mit 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. Einholung der erforderlichen Einwilligung von Nutzern, die in das Tool eingeladen werden und darin zusammenarbeiten).

3. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter garantiert, dass er:
(a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeitet, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland, sofern er nicht durch anwendbares 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 (Sicherheit der Verarbeitung) erforderlichen Maßnahmen ergreift.
(d) den Verantwortlichen bei der Einhaltung der Pflichten gemäß den Artikeln 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung) unterstützt. Gemäß DSGVO (Art. 33) garantiert der Auftragsverarbeiter im unwahrscheinlichen Fall einer verifizierten Sicherheitsverletzung, die personenbezogene Kundendaten betrifft, eine schriftliche Benachrichtigung an den Verantwortlichen ohne unangemessene Verzögerung und spätestens 72 Stunden, nachdem er von der Verletzung Kenntnis erlangt hat.

(e) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen löscht oder an diesen zurückgibt und vorhandene Kopien löscht, es sei denn, das Unionsrecht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der personenbezogenen Daten vor. Für die Rückgabe von Daten steht ein Self-Service-JSON-Export zur Verfügung, und Dokumentdateien werden als für 7 Tage gültige Download-Links bereitgestellt.
(f) Inhaltsdaten des Kunden (Customer Content) nicht für Trainingszwecke verwendet und sicherstellt, dass seinen Unterauftragsverarbeitern dies ebenfalls durch deren jeweilige API- oder AVV-Bedingungen untersagt ist.

4. Unterauftragsverhältnisse

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, Unterauftragsverarbeiter in Anspruch zu nehmen. Die aktuelle Liste der Unterauftragsverarbeiter ist in Anhang III aufgeführt.
(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder den Ersatz anderer Unterauftragsverarbeiter per E-Mail an die Administratoren des Verantwortlichen und durch Aktualisierung der Trust-Seite des Auftragsverarbeiters. Der Verantwortliche kann solchen Änderungen aus wichtigem Grund innerhalb einer Frist von 14 Tagen nach der Benachrichtigung widersprechen.
(3) Nimmt der Auftragsverarbeiter einen Unterauftragsverarbeiter in Anspruch, so geschieht dies im Wege eines schriftlichen Vertrags, der dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegt, die in diesem AVV festgelegt sind.

5. Rechte der betroffenen Personen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen dabei, dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person (z. B. Recht auf Auskunft, Löschung) nachzukommen.

6. Internationale Datenübermittlungen

Wenn der Auftragsverarbeiter personenbezogene Daten in Länder außerhalb der EU/des EWR (z. B. USA) übermittelt, sichert er zu, dass geeignete Garantien vorhanden sind, wie z. B. das EU-US Data Privacy Framework oder Standardvertragsklauseln (SCCs).

7. Überprüfungsrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung, um die Einhaltung dieses AVV nachzuweisen.
(2) Überprüfungen und Inspektionen können vom Verantwortlichen oder einem vom Verantwortlichen beauftragten Prüfer durchgeführt werden. Um den Aufwand zu verringern, erklärt sich der Verantwortliche bereit, sich in erster Linie auf gültige Sicherheitszertifikate oder Auditberichte des Auftragsverarbeiters zu stützen. Solange sich die eigene SOC-2-Zertifizierung des Auftragsverarbeiters noch in Vorbereitung befindet, erklärt sich der Verantwortliche bereit, auf

Alternativen wie Sicherheitsfragebögen, Remote-Reviews oder Auditberichte von Unterauftragsverarbeitern zurückzugreifen.

8. Datenresidenz

(1) **Einstellungen:** Der Verantwortliche weist den Auftragsverarbeiter bei der Kontoeinrichtung an, als Datenresidenz-Modus entweder „Standard“ oder „EU“ zu verwenden. Diese Auswahl gilt strikt für Inhaltsdaten (Prompts, Dokumente, Chats, Transkripte, Embeddings und Suchanfragen).
(2) **Zusage beim Modus „EU“:** Wird „EU“ gewählt, garantiert der Auftragsverarbeiter, dass Inhaltsdaten ausschließlich an die in Anhang III Teil C genannten Unterauftragsverarbeiter gesendet werden. Dies ist eine strikte technische Garantie, nicht nur eine reine Absichtserklärung: Sie wird serverseitig im Anwendungscode (data-residency.ts) erzwungen, der die Verarbeitung bei einem Verstoß sofort mit einem Fehler abbricht.
(3) **Zusage beim Modus „Standard“:** Wird „Standard“ gewählt, kann die Verarbeitung von Inhaltsdaten durch die in Anhang III Teil B genannten Unterauftragsverarbeiter auch in den Vereinigten Staaten erfolgen, auf Grundlage von Standardvertragsklauseln (SCCs) oder dem EU-US Data Privacy Framework (DPF).
(4) **Umfang und Ausschlüsse:** Die Einstellung der Datenresidenz ändert nichts an der Nutzung der Kerninfrastruktur. Unterauftragsverarbeiter wie Supabase, Vercel, Render und Resend gelten für beide Modi (wie in Anhang III Teil A aufgeführt). Darüber hinaus fallen Metadaten, Kontodaten und Nutzungsdaten nicht unter diese Datenresidenz-Zusage. Die Wahl des „EU“-Modus bedeutet daher nicht, dass alle Arten von Daten ausschließlich in der EU verbleiben, wohl aber sämtliche Inhaltsdaten.

ANHANG I: DETAILS DER VERARBEITUNG

1. Gegenstand und Dauer der Verarbeitung
Gegenstand ist die Bereitstellung eines KI-gestützten Beratungs-/Strategie-Tools (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

- KI-Analyse von hochgeladenen Dokumenten, Prompts, Chats und Besprechungstranskripten.
- Erstellung von Embeddings, Generierung von Arbeitsergebnissen (Deliverables), Web-Recherche und Transkription.
- Import aus Microsoft 365.
- Erstellung von maßgeschneiderten Wissens- und Kontaktdatenbanken.
- Verwaltung von Benutzerkonten und transaktionale E-Mail-Kommunikation.

3. Kategorien betroffener Personen

- Mitarbeiter, Kunden oder Lieferanten des Verantwortlichen.
- Autorisierte Administratoren des Verantwortlichen.
- Mitarbeiter der Kunden des Verantwortlichen, Interviewpartner und in Registerdaten genannte Personen.

4. Arten personenbezogener Daten

- **Kontaktdaten:** Vor-/Nachname, E-Mail-Adresse, ggf. Mobiltelefonnummer.
- **Inhaltsdaten:** Dokumente, Chats, generierte Ergebnisse, Transkripte und vom Verantwortlichen bereitgestellte Eingaben.
- **Nutzungsdaten:** Erstellung oder Bearbeitung von Ergebnissen, Bereitstellung von Eingaben, Zeitstempel, Interaktionsprotokolle.
- **Besondere Datenkategorien (Art. 9 DSGVO):** Die Verarbeitung besonderer Kategorien personenbezogener Daten ist ausdrücklich ausgeschlossen.

ANHANG II: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMs)

Der Auftragsverarbeiter hat die folgenden Maßnahmen ergriffen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten:

1. **Zugangskontrolle:** Mehrschichtige Authentifizierungssicherheit, einschließlich strenger Passwortrichtlinien (mindestens 8 Zeichen, Groß- und Kleinbuchstaben und Ziffern), Zwei-Faktor-Authentifizierung (TOTP), die firmenweit erzwungen werden kann, und Unterstützung für Enterprise Single Sign-On (SSO) über SAML 2.0; Beschränkung des Datenzugriffs auf autorisiertes Personal nach dem „Need-to-know“-Prinzip.
2. **Weitergabekontrolle:** Verschlüsselung von Daten bei der Übertragung mittels TLS 1.2 oder höher.
3. **Datenverschlüsselung:** Verschlüsselung von ruhenden Daten in der Datenbank (AES-256 oder gleichwertig).
4. **Verfügbarkeitskontrolle:** Regelmäßige automatisierte Backups. Gelöschte Daten verbleiben in Backups, bis diese ablaufen. Nutzung redundanter Cloud-Infrastruktur zur Vermeidung von Datenverlusten.
5. **Trennungsgebot:** Logische Trennung von Daten verschiedener Kunden (Mandantenfähigkeit / Multi-Tenancy-Architektur).

ANHANG III: LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche genehmigt die Beauftragung der folgenden Unterauftragsverarbeiter, mit denen ein Standard-AVV abgeschlossen wurde.
Welche Unterauftragsverarbeiter Inhaltsdaten verarbeiten, hängt von der Datenresidenz ab, die während der Kontoeinrichtung vereinbart wurde (siehe §8 im Hauptdokument des AVV).

Teil A: In beiden Einstellungen verwendet

Name	Zweck	Standort	Zertifizierungen
Supabase / AWS	Datenbank, Dateispeicherung, Vektorsuche, Authentifizierung	Frankfurt, Deutschland (EU)	SOC 2 Type II, ISO/IEC 27001
Vercel	Anwendungs-Hosting & CDN	Frankfurt, Deutschland (EU) für Anwendungsfunktionen; globales Edge-Netzwerk für statische Inhalte	SOC 2 Type II, ISO/IEC 27001
Render	Hintergrund-Worker-Hosting (Agentenläufe, Dokumenten- und Vorlagenverarbeitung)	Frankfurt, Deutschland (EU)	SOC 2 Type II, ISO/IEC 27001
Resend	Transaktions- und Einladungs-E-Mails	EU (Irland)	AVV abgeschlossen

Teil B: Nur Standard-Einstellung

Unter der Einstellung „Standard“ können Inhaltsdaten von den folgenden Unterauftragsverarbeitern verarbeitet werden, einschließlich in den Vereinigten Staaten.

Name	Zweck	Standort	Garantien
OpenAI, Anthropic, Google	Foundation Models, Embeddings, Bildgenerierung und Audio-Transkription	Vereinigte Staaten	Vertragliches Verbot des Trainings mit Daten des Verantwortlichen per API-Vertrag; EU-US Data Privacy Framework oder SCCs
Tavily	Web-Recherche für Forschungs-Workflows	Vereinigte Staaten	AVV abgeschlossen; EU-US Data Privacy Framework oder SCCs

Microsoft Foundry (Global Standard)	GPT- und Claude-Modelle auf der eigenen Azure AI Foundry-Ressource des Auftragsverarbeiters	Globale Verarbeitung	Microsoft Product Terms / AVV

Teil C: Nur EU-Einstellung

Unter der Einstellung „EU“ sendet der Auftragsverarbeiter Inhaltsdaten nur an die folgenden Unterauftragsverarbeiter. Der Auftragsverarbeiter erzwingt diese Einschränkung technisch: Eine Anfrage, die die EU-Grenze verlassen würde, wird abgelehnt und nicht stillschweigend woandershin geroutet.

Name	Zweck	Standort	Garantien
melious.ai	Foundation Models, Bildgenerierung und Audiotranskription	EU / EWR	AVV abgeschlossen
Microsoft Foundry (Data Zone Standard, EU)	GPT-Modelle und Embeddings	EU Data Zone	Microsoft Product Terms / AVV
Linkup	Web-Recherche für Forschungs-Workflows	EU (Frankreich)	AVV abgeschlossen

Teil D: Nur wenn der Verantwortliche den Dienst verbindet

Name	Zweck	Standort	Hinweise
Microsoft (Graph API)	Microsoft 365 Integration	Eigener Microsoft 365 Mandant des Verantwortlichen	SOC 1/2/3, ISO 27001, ISO 27018
Jamie, North Data, Statista, BvD (Orbis)	Konnektoren zu den eigenen Konten des Verantwortlichen: Besprechungsnotizen, Unternehmens- und Marktdaten	Abhängig vom Anbieter	Wird nur verwendet, wenn der Verantwortliche die Integration verbindet

UK Companies House	Öffentliche Firmenregisterabfragen für britische Unternehmen (nur Suchbegriffe und Registernummern)	Vereinigtes Königreich	Öffentliches Regierungsregister

Hinweis: Übermittlungen in die USA oder andere Drittländer sind durch das EU-US Data Privacy Framework oder Standardvertragsklauseln abgesichert. Die Einstellung zur Datenresidenz regelt Inhaltsdaten (Prompts, Dokumente, Chats, Transkripte, Embeddings und Suchanfragen). Sie ändert nichts daran, wo Konto-, Nutzungs- und Infrastrukturdaten in Teil A verarbeitet werden.

Unterschriften

Für den Verantwortlichen:
(Keine Unterschrift nötig, digitale Zustimmung zu den Bedingungen per Checkbox bei Registrierung)

Für den Auftragsverarbeiter:

Lukas Schaefer

Lukas Schaefer, Geschäftsführer
TNT Ventures GmbH