DATA PROCESSING AGREEMENT (DPA)

Between

The Customer as identified in the Main Agreement
(hereinafter **“Controller”**)

and

TNT Ventures GmbH
Venloer Str. 240
50823 Köln, Germany
Registered at Amtsgericht Köln, HRB 125080
Represented by its Managing Directors: Felix Schürholz, Lukas Schaefer
(hereinafter **“Processor”**)

(together the “Parties”).

1. Preamble

This Data Processing Agreement (“DPA”) forms part of the Terms of Service (“Main Agreement”) between the Parties regarding the use of the product **"drall.ai"**. It applies to the extent that the Processor processes Personal Data on behalf of the Controller in the course of providing the services defined in the Main Agreement (the "Services").

2. Scope and Responsibility

(1) The Processor shall process Personal Data solely on behalf of the Controller and in accordance with the Controller's documented instructions (Art. 28 GDPR). The Main Agreement and this DPA are the documented instructions.
(2) The Controller is solely responsible for the lawfulness of the data processing (e.g., obtaining necessary consent from users to be invited to and collaborate within the tool).

3. Obligations of the Processor

The Processor guarantees that it will:
(a) Process the Personal Data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country, unless required to do so by applicable law.
(b) Ensure that persons authorized to process the Personal Data have committed themselves to confidentiality.
(c) Take all measures required pursuant to Article 32 GDPR (Security of Processing).
(d) Assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR (Security, Breach Notification, DPIA). In accordance with GDPR (Art. 33), in the unlikely event of a verified security incident affecting customer personal data, the Processor guarantees written notification to the Controller without undue delay, and no later than 72 hours after becoming aware of the breach.
(e) Delete or return (at the choice of the Controller) all personal data to the Controller after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data. For the return of data, a self-service JSON export exists, and document files are provided as download links valid for 7 days.
(f) Not use Customer Content for training purposes and will ensure that its sub-processors are likewise prohibited from doing so under their respective API or data processing agreement (DPA) terms.

4. Sub-processing

(1) The Controller grants the Processor a general authorization to engage sub-processors. The current list of sub-processors is set forth in Annex III.
(2) The Processor shall inform the Controller of any intended changes concerning the addition or replacement of other sub-processors via email to the Controller's admin users and by updating the Processor's trust page. The Controller may object to such changes for reasonable cause within a 14-day objection window following the notification.
(3) Where the Processor engages a sub-processor, it shall do so by way of a written contract which imposes the same data protection obligations on the sub-processor as set out in this DPA.

5. Data Subject Rights

The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights (e.g., Right to Access, Erasure).

6. International Transfers

If the Processor transfers Personal Data to countries outside the EU/EEA (e.g., USA), it warrants that appropriate safeguards are in place, such as the EU-US Data Privacy Framework or Standard Contractual Clauses (SCCs).

7. Audit Rights

(1) The Processor shall make available to the Controller all information necessary to demonstrate compliance with this DPA.
(2) Audits and inspections may be conducted by the Controller or an auditor mandated by the Controller. To reduce burden, the Controller agrees to primarily rely on valid security certifications or audit reports provided by the Processor. While the Processor's own SOC 2 certification is currently in preparation, the Controller agrees to rely on fallbacks such as security questionnaires, remote reviews, or sub-processor audit reports.

8. Data Residency

(1) **Settings:** The Controller instructs the Processor during account setup to use either "Standard" or "EU" as data residency mode. This selection strictly applies to Content Data (prompts, documents, chats, transcripts, embeddings, and search queries).
(2) **"EU" Mode Commitment:** If "EU" is selected, the Processor guarantees that Content Data will solely be sent to the sub-processors listed in Annex III Part C. This is a strict technical guarantee, not merely a statement of intent: it is enforced server-side within the application code (data-residency.ts), which will immediately abort processing with an error if a violation is attempted.
(3) **"Standard" Mode Commitment:** If "Standard" is selected, the processing of Content Data may also occur in the United States by the sub-processors listed in Annex III Part B, based on Standard Contractual Clauses (SCCs) or the EU-US Data Privacy Framework (DPF).
(4) **Scope and Exclusions:** The data residency setting does not alter the use of core infrastructure. Sub-processors such as Supabase, Vercel, Render, and Resend apply to both modes (as listed in Annex III Part A). Furthermore, metadata, account data, and usage data do not fall under this data residency commitment. Selecting the "EU" mode therefore does not imply that all types of data remain exclusively within the EU, but all content data does.

ANNEX I: DETAILS OF PROCESSING

1. Subject matter and duration of the processing

The subject matter is the provision of an AI-powered consultancy/strategy tool (drall.ai) that enables users to plan, run and document consultancy/strategy projects and workflows. The duration of the processing corresponds to the term of the Main Agreement.

2. Nature and Purpose of the processing

- AI analysis of uploaded documents, prompts, chats and meeting transcripts.
- Creation of embeddings, deliverable generation, web research and transcription.
- Import from Microsoft 365.
- Creation of customized knowledge and contact databases.
- User account management and transactional email communication.

3. Categories of Data Subjects

- Employees, customers or suppliers of the Controller.
- Authorized admin users of the Controller.
- The Controller's clients' employees, interviewees, and people named in registry data.

4. Types of Personal Data

- **Contact Data:** First/Last Name, Email Address, potentially Mobile Phone Number.
- **Content Data:** Documents, chats, generated outputs, transcripts, and input provided by the Controller.
- **Usage Data:** Creation or editing of outputs, provision of inputs, timestamps, interaction logs.
- **Special Categories of Data (Art. 9 GDPR):** Processing of special categories of personal data is explicitly excluded.

ANNEX II: TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

The Processor has implemented the following measures to ensure a level of security appropriate to the risk:

1. **Access Control:** Multi-layered authentication security, including strong password policies (minimum 8 characters, upper- and lower-case letters and digits), two-factor authentication (TOTP) that can be enforced firm-wide, and support for enterprise Single Sign-On via SAML 2.0; restriction of access to data to authorized personnel on a "need-to-know" basis.
2. **Transmission Control:** Encryption of data in transit using TLS 1.2 or higher.
3. **Data Encryption:** Encryption of data at rest in the database (AES-256 or equivalent).
4. **Availability Control:** Regular automated backups. Deleted data stays in backups until they expire. Use of redundant cloud infrastructure to prevent data loss.
5. **Separation Rule:** Logical separation of data from different customers (Multi-tenancy architecture).

ANNEX III: LIST OF SUB-PROCESSORS

The Controller authorizes the engagement of the following sub-processors, with whom a standard DPA is in place. Which sub-processors process Content Data depends on the data residency agreed upon during account setup (see §8 in the main DPA document).

Part A: Used in both settings

Name	Purpose	Location	Certifications
Supabase / AWS	Database, file storage, vector search, authentication	Frankfurt, Germany (EU)	SOC 2 Type II, ISO/IEC 27001
Vercel	Application hosting & CDN	Frankfurt, Germany (EU) for application functions; global edge network for static content	SOC 2 Type II, ISO/IEC 27001
Render	Background worker hosting (agent runs, document and template processing)	Frankfurt, Germany (EU)	SOC 2 Type II, ISO/IEC 27001
Resend	Transactional and invitation emails	EU (Ireland)	DPA in place

Part B: Standard setting only

Under the "Standard" setting, Content Data may be processed by the following sub-processors, including in the United States.

Name	Purpose	Location	Safeguards
OpenAI, Anthropic, Google	Foundation models, embeddings, image generation and audio transcription	United States	Barred from training on Controller data by API contract; EU-US Data Privacy Framework or SCCs
Tavily	Web search for research workflows	United States	DPA in place; EU-US Data Privacy Framework or SCCs
Microsoft Foundry (Global Standard)	GPT and Claude models on the Processor's own Azure AI Foundry resource	Global processing	Microsoft Product Terms / DPA

Part C: EU setting only

Under the "EU" setting, the Processor sends Content Data only to the following sub-processors. The Processor enforces this restriction technically: a request that would leave the EU boundary is rejected and not silently routed elsewhere.

Name	Purpose	Location	Safeguards
melious.ai	Foundation models, image generation and audio transcriptio	EU / EEA	DPA in place
Microsoft Foundry (Data Zone Standard, EU)	GPT models and embeddings	EU Data Zone	Microsoft Product Terms / DPA
Linkup	Web search for research workflows	EU (France)	DPA in place

Part D: Only when the Controller connects the service

Name	Purpose	Location	Notes
Microsoft (Graph API)	Microsoft 365 integration	Controller's own Microsoft 365 tenant	SOC 1/2/3, ISO 27001, ISO 27018
Jamie, North Data, Statista, BvD (Orbis)	Connectors to the Controller's own accounts: meeting notes, company and market data	Depends on the provider	Used only when the Controller connects the integration
UK Companies House	Public company-registry lookups for UK entities (search terms and registry numbers only)	United Kingdom	Public government registry

Note: Transfers to the USA or other third countries are safeguarded by the EU-US Data Privacy Framework or Standard Contractual Clauses. The data residency setting governs Content Data (prompts, documents, chats, transcripts, embeddings and search queries). It does not change where account, usage and infrastructure data in Part A are processed.

Signatures

For the Controller:

(No signature needed, consent provided by digital acceptance of terms via checkbox at registration.)

For the Processor:

Lukas Schaefer

_____

Lukas Schaefer, Managing Director

TNT Ventures GmbH