

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.

(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. The Controller may object to such changes for reasonable cause within 14 days.
- (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.

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

- 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.

4. Types of Personal Data

- **Contact Data:** First/Last Name, Email Address, potentially Mobile Phone Number.
- **Content Data:** Input provided by the Controller when inviting users.
- **Usage Data:** Creation or editing of outputs, provision of inputs, timestamps, interaction logs.

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 and support for enterprise Single Sign-On (SSO) solutions (including SAML 2.0 and OIDC as available); 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; 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:

Name	Purpose	Location	Certifications
Supabase / AWS	Database, file storage, vector search	Frankfurt, Germany (EU)	SOC 2 Type II, ISO/IEC 27001
Vercel	Application hosting & CDN	Global edge, EU-prioritized	SOC 2 Type II, ISO/IEC 27001
Microsoft	Microsoft 365 integration (Graph API)	Your firm's own Microsoft 365 tenant	SOC 1/2/3, ISO 27001, ISO 27018
OpenAI, Anthropic, Google	Foundation model providers (standard routing)	United States	Barred from training on your data by API contract
melious.ai	EU-hosted foundation models (Enterprise option)	EU / EEA	Used only when EU-only routing is enabled
Tavily	Web search for research workflows (standard routing)	United States	DPA in place
Linkup	Web search for research workflows (EU-hosted alternative to Tavily)	EU (France)	Used only when EU-hosted search is configured
LangSmith	AI observability and debugging	United States	DPA in place
Resend	Transactional and invitation emails	EU (Ireland)	DPA in place

(Note: Transfers to the USA/Third Countries are safeguarded by the EU-US Data Privacy Framework or Standard Contractual Clauses)

Signatures

For the Controller:

(Signature provided by digital acceptance of terms via checkbox)

For the Processor:

Lukas Schaefer

Lukas Schaefer, Managing Director
TNT Ventures GmbH