1 SCOPE

1.1 This Service Level Agreement specifies the SaaS Solution owed by Turbit under the Agreement.

1.2 All performance specifications in this Service Level Agreement refer to the quality owed by Turbit of the SaaS Solution offered to the Customer for use at the Transfer Point in accordance with the Agreement. Impairments in the area of data transmission from Transfer Point to the Customer and/or in the area of the Devices itself shall not be taken into account.

SECTION I

Clause 1

PURPOSE AND SCOPE

(a) The purpose of this Data Processing Agreement (the "**Clauses**") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

INVARIABILITY OF THE CLAUSES

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

INTERPRETATION

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

HIERARCHY

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

DOCKING CLAUSE

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

DESCRIPTION OF PROCESSING(S)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

OBLIGATIONS OF THE PARTIES

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute

to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice. The controller shall make (and ensure that each of its auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to processor´s premises, equipment, personnel and business in the course of such audit. The controller shall bear the costs of such audit. The controller will provide the results of any audit to the processor. If an audit determines that the processor has breached its obligations under the Clauses, Processor will promptly remedy the breach at its own cost.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 4 weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent- the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a

specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

ASSISTANCE TO THE CONTROLLER

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

NOTIFICATION OF PERSONAL DATA BREACH

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679,

where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679 /, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679 /.

SECTION III – FINAL PROVISIONS

Clause 10

NON-COMPLIANCE WITH THE CLAUSES AND TERMINATION

(a) Without prejudice to any provisions of Regulation (EU) 2016/, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller:

The Controller is the Customer or Customer Affiliate identified in the Order Form(s).

The contact person's name, position and contact details are outlined in the Order Form(s).

Processor:

Name: Turbit Systems GmbH

Address: Kottbusser Damm 79, 10967 Berlin

Contact person's name, position and contact details: Michael Tegtmeier, CEO, m.tegtmeier@turbit.de

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

- Authorized Users of the Controller (employees/contractors) using Turbit Assistant.
- Individuals referenced in uploaded documents or chat prompts (e.g., "what did person X inspect…").

Categories of personal data processed

- Business contact data present in uploads/chats: names, business emails, business phone numbers, job titles.
- Account/operational data: user ID, roles/permissions, timestamps, IP address, user agent, usage events (security/operations).
- Content data: prompts, chat transcripts, uploaded/ingested documents and their derived embeddings.

Sensitive data processed (if applicable) and safeguards

- Not expected / not required for the service. If provided by the Controller, Turbit processes only on documented instructions with strict access limitation, logging, and purpose limitation.

Nature of the processing

Provision and operation of a RAG-based assistant (Turbit Assistant): ingest, store, index (embeddings), retrieve and generate answers over Controller-provided content; logging; backups; support on instruction.

Purpose(s) for which the personal data is processed on behalf of the Controller

- Use of personal data to set up, operate, monitor and provide the SaaS Solution (including technical support).
- Communication with Authorized Users.
- Storage of personal data in designated data centers.
- Uploads of updates or upgrades to the Software.
- Backups of personal data.
- Processing of personal data, including transmission, retrieval, and access.
- Execution of documented instructions of the Customer in accordance with the Agreement.

Duration of the processing

- For the term of the Agreement.

- Chats/transcripts: retained for the duration of the Agreement by default (“never deleted”) unless the Controller deletes or instructs deletion; deletions propagate to search indexes and backups subject to backup cycles below.

For processing by (sub-)processors, specify subject matter, nature and duration of the processing

See Annex IV (subject matter, nature, location/residency, duration).

Hosting and data residency

- Primary hosting on OVH bare-metal in Germany and France (application, databases, vector store).
- Model calls use OpenAI, Cohere, Anthropic, Microsoft Azure with EU endpoints where available; if extra-EEA processing occurs, transfers are safeguarded under SCCs/TIAs (see Annex IV).

ANNEX III: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Measures of pseudonymisation and encryption of personal data

- TLS 1.2+ for data in transit; AES-256 for data at rest (databases, object storage, vector indexes, backups).
- Key management via KMS/HSM; restricted key access; periodic key rotation.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- Logical tenant isolation across app/DB/vector layers; scoped service credentials and tokens.
- Role-based access control; least privilege; MFA required for Turbit admin access; break-glass with just-in-time elevation; quarterly access reviews.
- CIS-aligned baselines; timely patching; host firewalls/WAF; private networking on OVH EU (DE/FR).

Measures for ensuring the ability to restore availability and access in a timely manner

Encrypted GFS backups (daily, weekly, monthly, half-yearly) with periodic restore testing.

Targets: RPO ≤ 24h, RTO ≤ 24h.

Processes for regularly testing, assessing and evaluating the effectiveness of measures

Secure SDLC: code review, SAST/SCA in CI, DAST in staging; vulnerability scanning at least monthly and on critical disclosures.

Measures for user identification and authorisation

RBAC with per-tenant scoping; admin MFA; audit trails for privileged actions.

Customer SSO (SAML/OIDC): not currently offered.

Measures for the protection of data during transmission and storage

Network-level controls (firewalls/WAF), TLS everywhere; integrity checks for stored artifacts; secrets in vault; time-sync across systems.

Measures for ensuring physical security of locations at which personal data are processed

OVH data center physical security as per provider standards (access control, surveillance).

Measures for ensuring events logging

Centralised, tamper-resistant logs (app/DB/infra); SIEM alerts for auth anomalies, exfil patterns, model-API anomalies; time-stamped audit logs.

Measures for ensuring system configuration, including default configuration

Baseline hardening; immutable infrastructure where feasible; configuration as code; change management.

Measures for internal IT and IT security governance and management

ISMS with policies for access, device, change, incident, backup/restore; staff confidentiality and security awareness training.

Measures for ensuring data minimisation and quality

Prompt/output guardrails (pattern-based redaction options); attachment anti-virus scanning and file-type allowlists.

Retrieval strictly scoped to tenant corpus; no cross-tenant vector leakage.

Measures for ensuring limited data retention

Chats/transcripts: retained for the Agreement term (no automatic deletion) unless the Controller deletes/requests deletion.

Backups per GFS scheme; deletions cascade to backups per restore cycles.

Measures for allowing data portability and ensuring erasure (and DSAR assistance)

DSAR exports not available via self-service at present; Turbit will make reasonable efforts to search and extract relevant personal data from chats, documents and logs and provide it in a commonly used format upon instruction from the Controller within a reasonable timeframe.

Controller audits/assessments supported per the Agreement with reasonable cooperation.

Breach notification and assistance

Incident response with 24/7 on-call, triage, containment, forensics, post-mortems.

Notification to Controller without undue delay, with details sufficient for the Controller to meet GDPR Art. 33 obligations.

ANNEX IV: LIST OF SUB-PROCESSORS

The Controller provides a general authorisation for engagement from an agreed list; changes are notified ≥ 4 weeks in advance with a right to object.

1. OVHcloud (OVH Groupe SAS)

Address: 2 rue Kellermann, 59100 Roubaix, France (provider corporate HQ).

Description of the processing: IaaS bare-metal hosting (compute, storage, networking, backups) for Turbit Assistant application, databases, vector store.

Location / residency: Germany and France data centers (as provisioned).

Duration: Term of the Agreement.

Delimitation of responsibilities: Turbit controls OS/app stack; OVH provides facility and infrastructure services.

2. OpenAI (enterprise API)

Address: As per vendor DPA.

Description of the processing: LLM inference for prompts/completions within RAG; minimal necessary prompt/context fragments and model outputs; no training on Customer data; vendor retention disabled where supported.

Location / residency: EU endpoints where available; if extra-EEA, SCCs/TIAs apply.

Duration: Per-request processing.

3. Cohere (enterprise API)

Address: As per vendor DPA.

Description of the processing: Embeddings/inference within RAG; no training on Customer data; retention disabled where supported.

Location / residency: EU endpoints where available; if extra-EEA, SCCs/TIAs apply.

Duration: Per-request processing.

4. Anthropic (enterprise API)

Address: As per vendor DPA.

Description of the processing: LLM inference; no training on Customer data; retention disabled where supported.

Location / residency: EU endpoints where available; if extra-EEA, SCCs/TIAs apply.

Duration: Per-request processing.

5. Microsoft Azure (Azure AI Services)

Address: As per vendor DPA.

Description of the processing: LLM inference (and, if configured, embeddings) within RAG; minimal necessary prompt/context; no training on Customer data; enterprise privacy settings where available.

Location / residency: EU regions as configured (e.g., Germany West Central / France Central)

Duration: Per-request processing.

6. Atlassian (Jira Service Management Cloud)

Address: As per vendor DPA.

Description of the processing: Customer support ticketing; processes support contact details (name, business email) and ticket content (which may include limited logs/metadata).

Location / residency: EU data residency if enabled in your Atlassian org; otherwise safeguarded by SCCs/TIAs.

Duration: Term of the Agreement / per ticket lifecycle.