

## **Annex C: Data Processing Agreement Terms**

These Data Processing Agreement Terms ("DPA") form an integral part of the AGREEMENT to the extent PROVIDER processes personal data of the CUSTOMER based on CUSTOMER's instructions under the Agreement. As per this DPA, CUSTOMER is acting as the controller of personal data as defined in the General Data Protection Regulation ("**CONTROLLER**") whilst the PROVIDER is acting as the processor as stipulated in the General Data Protection Regulation ("**PROCESSOR**"). Both are hereinafter collectively referred to as the "**PARTIES**" and individually a "**PARTY**".

Unless otherwise defined in this DPA, the definitions of the AGREEMENT apply to this DPA.

### **1. General Provisions**

- 1.1 The PROCESSOR shall process personal data only on behalf of and in accordance with the documented instructions of the CONTROLLER, under and for the purposes of the AGREEMENT and in compliance with the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and any other applicable data protection laws.
- 1.2 The CONTROLLER has selected the PROCESSOR as a supplier in accordance with the duty of care under applicable data protection laws. This DPA constitutes the data processing agreement within the meaning of Art. 28 GDPR, governing the rights and obligations of the PARTIES with respect to data processing.
- 1.3 "PERSONAL DATA" or "DATA" means any information relating to an identified or identifiable natural person (hereinafter referred to as "DATA SUBJECT").
- 1.4 The term "PROCESSING", term shall be understood in a broad sense. This includes any operation or series of operations carried out with or without the use of automated procedures in connection with PERSONAL DATA, such as collection, gathering, organization, arrangement, storage, adaptation or modification, reading, retrieval, use, disclosure by transmission, dissemination or any other form of provision, matching or linking, restriction, deletion or destruction.
- 1.5 "INSTRUCTION" means an instruction by the CONTROLLER to the PROCESSOR, issued in a documented form, to perform a specific action regarding PERSONAL DATA (e.g. anonymization, blocking, deletion, disclosure). If necessary, an INSTRUCTION can be issued orally or by telephone; such INSTRUCTIONS shall be confirmed by the CONTROLLER without undue delay in a documented form.
- 1.6 The CONTROLLER retains all rights in the DATA. At the request or upon termination of the Agreement, PROCESSOR shall return or delete the DATA in accordance with this DPA. The PROCESSOR shall not assert any right of retention over the CONTROLLER's DATA, except where required by applicable law.

### **2. Scope and Purpose of PROCESSING**

- 2.1 The purpose of this DPA is to set out the scope, purpose and subject matter of the DATA PROCESSING carried out by the PROCESSOR on behalf of the CONTROLLER under the Agreement.

- 2.2 The PROCESSOR shall process PERSONAL DATA solely to the extent necessary for providing, administering, and operating the SOFTWARE under the Agreement and only in accordance with the CONTROLLER's INSTRUCTIONS.
- 2.3 The categories of DATA SUBJECTS and types of PERSONAL DATA processed are specified in Appendix 1.
- 2.4 The PROCESSING of special categories of PERSONAL DATA within the meaning of Art. 9 GDPR may occur where necessary for the provision of the services and where the CONTROLLER has lawfully collected such DATA and provided INSTRUCTIONS for their processing.

### **3. CONTROLLER's Rights and Obligations**

- 3.1 The CONTROLLER is the controller in the meaning of applicable data protection laws with respect to PROCESSOR's PROCESSING of the DATA. The CONTROLLER will decide about the admissibility of the PROCESSING.
- 3.2 The CONTROLLER may at any time issue additional or amended INSTRUCTIONS regarding the purpose, type and scope of PROCESSING.
- 3.3 The CONTROLLER will be responsible for ensuring DATA SUBJECTS' rights. DATA SUBJECTS' rights are to be exercised towards the CONTROLLER.
- 3.4 The CONTROLLER may inform the PROCESSOR of any error of irregularity in the PROCESSING of the DATA by the PROCESSOR.

### **4. PROCESSOR's Obligations and Responsibilities**

- 4.1 The PROCESSOR shall process DATA only within the scope of the Agreement and this DPA, including any INSTRUCTIONS issued by the CONTROLLER.
- 4.2 The PROCESSOR shall not make copies of PERSONAL DATA for its own purposes. Copies may be made only where necessary to provide the services, ensure proper PROCESSING (including backups and redundancy), or comply with legal obligations.
- 4.3 The PROCESSOR shall support the CONTROLLER in any inspections or information requests by competent supervisory authorities relating to the PROCESSING under this DPA and shall promptly inform the CONTROLLER of any such inquiries or measures that concern the CONTROLLER's DATA.
- 4.4 Where required by law, the PROCESSOR shall appoint a data protection officer and provide the CONTROLLER with the officer's contact details. If no DPO is required, the PROCESSOR shall designate a contact point for data protection matters.
- 4.5 The PROCESSOR shall, without undue delay, inform the CONTROLLER if and why the PROCESSOR deems certain INSTRUCTIONS unlawful.
- 4.6 The PROCESSOR shall, upon reasonable request, provide the CONTROLLER with the information necessary to enable the CONTROLLER to maintain accurate and up-to-date records of processing activities in accordance with Art. 30 GDPR and other applicable data protection laws.
- 4.7 The PROCESSOR shall, to the extent reasonably required, assist the CONTROLLER in fulfilling its obligations under Art. 32 to 36 GDPR, including data security, data protection impact assessments, and prior consultations with supervisory authorities. Such assistance shall consist of providing relevant documentation, technical information, or cooperation as reasonably necessary

to demonstrate compliance, taking into account the nature of the PROCESSING and the information available to the PROCESSOR.

- 4.8 If the PROCESSOR is required to disclose the DATA or information about the PROCESSING or this DPA, the PROCESSOR shall inform the CONTROLLER in writing and prior to such disclosure about the recipients, the time and the content of the disclosure as well as the legal grounds.
- 4.9 The PROCESSOR shall, upon reasonable request, correct, delete or block DATA in accordance with the CONTROLLER's INSTRUCTIONS and applicable law. The PROCESSOR shall confirm completion upon request by the CONTROLLER. Legal data retention obligations remain unaffected.
- 4.10 The PROCESSOR shall implement and maintain procedures to ensure compliance with this DPA and applicable data protection laws. Upon reasonable request, the PROCESSOR shall provide evidence of compliance (e.g., ISO 27001, SOC 2, or equivalent documentation).
- 4.11 If the CONTROLLER's PERSONAL DATA stored by the PROCESSOR were to become endangered due to attachment or sequestration, insolvency or composition proceedings or other events or measures by third parties, the PROCESSOR shall inform the CONTROLLER hereof without undue delay. The PROCESSOR shall inform all persons responsible in this context without undue delay that the rights to and ownership of the DATA lie solely with the CONTROLLER.

## **5. Data Breach Notification**

- 5.1 In the event of a breach of PERSONAL DATA, the PROCESSOR shall notify the CONTROLLER without undue delay, and in any case no later than 48 hours after becoming aware of the breach.
- 5.2 The notification shall at least:
  - 5.2.1 describe the nature of the breach of PERSONAL DATA including, where possible, the categories and approximate number of DATA SUBJECTS and data records concerned;
  - 5.2.2 communicate the name and contact details of the PROCESSOR's data protection officer or other contact point;
  - 5.2.3 describe the likely consequences of the breach of PERSONAL DATA; and
  - 5.2.4 describe the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects.
- 5.3 The PROCESSOR shall cooperate fully with and assist the CONTROLLER in complying with the CONTROLLER's obligations under Art. 33 and 34 GDPR.

## **6. DATA SUBJECTS' Rights**

- 6.1 If a DATA SUBJECT contacts the PROCESSOR directly for the purpose of access, correction, deletion or blocking, restriction of processing or objection with regard to DATA concerning him, the PROCESSOR shall immediately forward this request to the CONTROLLER. The PROCESSOR will not contact the DATA SUBJECT concerned, unless the CONTROLLER has instructed the PROCESSOR to do so. Information may only be provided upon prior instruction by the CONTROLLER.
- 6.2 Upon first request, the PROCESSOR shall support the CONTROLLER in fulfilling the claims of DATA SUBJECTS for access, correction, blocking or deletion, restriction of processing or

objection. This includes in particular that the PROCESSOR informs the CONTROLLER within a reasonable timeframe, of the information required to fulfil the claim.

## **7. Sub-Processors**

- 7.1 The PROCESSOR may engage sub-processors based on the CONTROLLER's general written authorization. The PROCESSOR shall inform the CONTROLLER of any intended changes concerning the addition or replacement of sub-processors, thereby giving the CONTROLLER the opportunity to object as stipulated under Clause 7.7.
- 7.2 The PROCESSOR shall carefully select sub-processors and ensure that they provide sufficient guarantees to implement appropriate technical and organizational measures.
- 7.3 The PROCESSOR shall ensure that sub-processors are bound by written contracts imposing the same data protection obligations as set out in this DPA, in particular with respect to security and confidentiality. The PROCESSOR shall remain fully liable for the performance of sub-processors.
- 7.4 Upon request, the PROCESSOR shall provide the CONTROLLER with the main data protection terms agreed with the sub-processor.
- 7.5 The PROCESSOR shall exercise towards its sub-processors the same audit and control rights that the CONTROLLER has towards the PROCESSOR under this DPA. The PROCESSOR shall monitor its sub-processors' compliance on a regular basis and provide relevant evidence to the CONTROLLER upon request. Upon the CONTROLLER's request, the PROCESSOR shall provide copies of such audit documentation or other relevant evidence. The CONTROLLER's audit rights under Clause 9 remain unaffected and may also be exercised in relation to sub-processors through the PROCESSOR.
- 7.6 Insofar as the involvement of a sub-processor involves the transfer of data to third countries, this transfer is covered by the approval pursuant to Clause 7.1 and requires appropriate safeguards in accordance with Art. 44 et seq. GDPR. The PROCESSOR shall ensure that appropriate safeguards (e.g., standard contractual clauses, adequacy decision of the EU Commission) are implemented for international data transfers and shall provide evidence of this upon request.
- 7.7 If the PROCESSOR engages additional sub-processors or changes sub-processors during the term of the DPA, the PROCESSOR shall inform the CONTROLLER in an appropriate manner before granting access to the CONTROLLER's PERSONAL DATA. If the CONTROLLER has justified data protection concerns regarding the involvement or change, the CONTROLLER may object to the proposal within fifteen (15) days of receiving this notification (written form is sufficient). If no objection is made within the above period, the CONTROLLER's consent shall be deemed to have been given. If the CUSTOMER objects to the use of a new sub-processor, the CONTROLLER and the PROCESSOR shall cooperate in good faith to find a mutually acceptable solution to the objection raised by the CONTROLLER.
- 7.8 All sub-processors engaged at the time of the execution of the AGREEMENT, are to be named in Appendix 2.

## **8. Audit Rights**

- 8.1 Audits shall primarily be conducted remotely, and may include the review of existing certifications, audit reports, or equivalent documentation. On-site audits shall be permitted only where remote audits do not provide sufficient assurance or in case of a justified suspicion of non-compliance.
- 8.2 Audits may be carried out no more than once per year, unless required by a supervisory authority or justified by a specific incident.

- 8.3 The PROCESSOR shall make available to the CONTROLLER all information reasonably necessary to demonstrate compliance with this Agreement and Art. 28 GDPR.
- 8.4 The CONTROLLER may request relevant information from the PROCESSOR's data protection officer or another qualified privacy contact regarding data protection compliance and technical and organizational measures.
- 8.5 The CONTROLLER may engage third parties to exercise audit rights. The PROCESSOR must tolerate and support the actions of such a third party in the same way as actions by the CONTROLLER. Audits shall be carried out during regular business hours, upon reasonable notice, and in a manner that does not unreasonably disrupt the PROCESSOR's operations.

## **9. Data Secrecy**

- 9.1 The PROCESSOR is under the obligation to protect data secrecy when PROCESSING DATAf or the CONTROLLER.
- 9.2 The PROCESSOR shall ensure that all personnel authorized to process PERSONAL DATA are subject to appropriate confidentiality obligations and receive adequate data protection training.

## **10. Technical and Organizational Measures**

- 10.1 The PROCESSOR shall implement technical and organizational measures necessary to ensure compliance with the applicable data protection law.
- 10.2 Since technical and organizational measures are subject to technological developments, the PROCESSOR shall be entitled to modifying the technical and organizational measures provided such modification does not decrease the level of data protection and data security beneath what is required by law and under this DPA.
- 10.3 Upon request, the PROCESSOR shall provide documentation demonstrating that appropriate technical and organizational measures are in place and kept up to date.
- 10.4 The PROCESSOR shall immediately inform the CONTROLLER in writing, without request, of any significant changes in the technical and organizational measures.

## **11. Term**

- 11.1 This DPA automatically terminates upon expiration or termination of the AGREEMENT.

## **12. Destruction, Deletion and Return of Data**

- 12.1 Upon termination of this DPA, the PROCESSOR is prohibited from collecting or using the CONTROLLER's DATA. Further storage of DATAcollected during the term of the DPA is only permitted to the extent necessary for the purpose of deletion, destruction or return to the CONTROLLER.
- 12.2 Unless instructed otherwise, the PROCESSOR shall irretrievably delete or destroy PERSONAL DATA using industry-standard secure deletion methods (e.g., DIN 66399, NIST SP 800-88, or comparable).
- 12.3 The PROCESSOR shall inform the CONTROLLER prior to permanent deletion of PERSONAL DATA, unless otherwise instructed. The PROCESSOR shall document deletion or destruction and provide such documentation to the CONTROLLER upon request. Statutory retention obligations remain unaffected.

**Appendices:**

Appendix 1: DATA SUBJECTS and Data Categories

Appendix 2: Sub Processors

Appendix 3: Technical and Organizational Measures

## Appendix 1: Data Subjects and Data Categories

This Appendix describes the scope of the PERSONAL DATA PROCESSING carried out by the PROCESSOR on behalf of the CONTROLLER under this DPA.

### 1. Purpose of Processing

The PROCESSOR processes PERSONAL DATA solely for the purpose of performing, administering, and operating the SOFTWARE as defined in the AGREEMENT.

### 2. Categories of DATA SUBJECTS

The PROCESSING may concern the following categories of DATA SUBJECTS:

- End users of the CONTROLLER who interact with the SOFTWARE (e.g., customers, clients, or website visitors);
- Employees, contractors, or other representatives of the CONTROLLER who use or administer the SOFTWARE;
- Employees or contractors of the PROCESSOR with authorized access, limited to what is necessary for operation, support, or maintenance;
- Other individuals whose PERSONAL DATA are submitted to the PROCESSOR by or on behalf of the CONTROLLER through the SOFTWARE.

### 3. Categories of PERSONAL DATA

The PROCESSING may include the following categories of PERSONAL DATA:

- **User master data** (e.g. name, account details, contact details);
- **Content data** (e.g. text entries, uploaded files, prompts, outputs);
- **Usage data** (e.g. logs of interactions, timestamps, frequency of use);
- **Technical data** (e.g. IP address, device type, browser information);
- **Payment data** (e.g. billing details, transaction IDs – if applicable)

### 4. Special Categories of DATA

The PROCESSING of special categories of PERSONAL DATA within the meaning of Art. 9 GDPR (e.g. health, biometric, or other sensitive data) may occur only where such DATA are lawfully collected and provided by the CONTROLLER and where the CONTROLLER has instructed the PROCESSOR to process such DATA.

In such cases, the PROCESSOR shall implement appropriate technical and organizational measures to ensure a level of protection corresponding to the sensitivity of the DATA.

### 5. Nature and Purpose of PROCESSING Activities

The PROCESSING includes, as necessary for the provision of the contracted SOFTWARE and related platform services, the collection, storage, transmission, and limited use of PERSONAL DATA, as well as related activities required for support, maintenance, and compliance with legal obligations. All PROCESSING is strictly limited to what is necessary for the operation and provision of the SOFTWARE and the underlying infrastructure as described in the AGREEMENT.

### 6. Duration of Processing

PERSONAL DATA shall be processed for the duration of the AGREEMENT, and shall be deleted or returned in accordance with Clause 12 of this DPA upon termination, unless longer retention is required by applicable law or agreed in writing by the Parties.

**Appendix 2: Sub Processors**

The PROCESSOR shall keep this list up to date and notify the CONTROLLER in writing at least thirty (30) days in advance of any intended addition or replacement of sub-processors, thereby allowing the CONTROLLER to object in accordance with Clause 7.7 of this DPA.

<b>Name of Sub-Processor</b>	<b>Registered Address/Country</b>	<b>Legal Transfer Safeguard (if outside EU/EEA)</b>
O3 (OpenAI, L.L.C.)	San Francisco, CA, USA	
AWS (Amazon Web Services, Inc.)	Seattle, WA, USA	
AWS S3 (Amazon Web Services, Inc.)	Seattle, WA, USA	
Exa (Exa Labs, Inc.)	San Francisco, CA, USA	

### **Appendix 3: Technical and Organizational Measures**

The PROCESSOR shall implement and maintain appropriate technical and organizational measures ("TOMs") as required under Art. 32 GDPR to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of PROCESSING.

The PROCESSOR shall provide a comprehensive description of the TOMs implemented for the PROCESSING under this DPA. The description must address, at a minimum, the following areas:

- access control and user management;
- physical and environmental security;
- encryption and pseudonymisation;
- system and network security;
- incident response and business continuity; and
- data protection by design and by default.

The TOMs described below form an integral part of this DPA and shall be kept up to date by the PROCESSOR. Any material changes to the TOMs that may affect the level of data protection or information security shall be notified to the CONTROLLER in advance.