Data Processing Addendum (DPA)

Effective Date: [EFFECTIVE_DATE]

This Data Processing Addendum ("**DPA**") forms part of the Master Service Agreement or other written or electronic agreement between **KleonoxAI** ("**Processor**") and the entity identified as the customer in such agreement ("**Controller**") (together, the "**Parties**").

1. Definitions

1.1. "**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including the EU General Data Protection Regulation 2016/679 ("**GDPR**") and any applicable national implementing legislations (e.g., Greek Law 4624/2019). 1.2. "**Personal Data**", "**Data Subject**", "**Processing**", "**Controller**", "**Processor**", and "**Personal Data Breach**" shall have the meanings given to them in the GDPR. 1.3. "**Subprocessor**" means any third party appointed by or on behalf of Processor to process Personal Data on behalf of Controller.

2. Roles and Scope

2.1. **Roles**: The Parties acknowledge and agree that with regard to the Processing of Personal Data in connection with the Mentoros service, Controller is the Controller and KleonoxAI is the Processor. 2.2. **Instructions**: Processor shall process Personal Data only on the documented instructions of Controller, including with regard to transfers of personal data to a third country, unless required to do so by Union or Member State law to which the Processor is subject.

3. Processor Obligations

3.1. **Confidentiality**: Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. 3.2. **Security**: Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as set out in Annex 2. 3.3. **Assistance**: Taking into account the nature of the processing, Processor shall assist Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Controller's obligation to respond to requests for exercising the Data Subject's rights. 3.4. **Breach Notification**: Processor shall notify Controller without undue delay after becoming aware of a Personal Data Breach.

4. Subprocessing

4.1. **Authorization**: Controller grants a general written authorization to Processor to engage Subprocessors. A list of current Subprocessors is available in Annex 3. 4.2. **Notification**: Processor shall inform Controller of any intended changes concerning the addition or replacement of Subprocessors, thereby giving Controller the opportunity to object to such changes.

5. International Transfers

5.1. Processor shall not transfer Personal Data to a country outside the EU/EEA unless it ensures that the transfer is conducted in accordance with Applicable Data Protection Laws (e.g., via Standard Contractual Clauses or Adequacy Decisions).

6. Deletion or Return

6.1. Upon termination of the Agreement, Processor shall, at the choice of Controller, delete or return all Personal Data to Controller and delete existing copies unless Applicable Data Protection Laws require storage of the Personal Data.

7. Audit Rights

7.1. Processor shall make available to Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller.

Annex 1: Details of Processing

A. List of Parties

- **Controller**: [TENANT_NAME]
- **Processor**: KleonoxAI (Contact: [CONTACT_EMAIL])

B. Description of Processing

- **Subject Matter**: Provision of the Mentoros AI assistant service.
- **Nature and Purpose**: Processing chat messages and metadata to provide real-time AI responses, analytics, and customer support on behalf of the Controller.
- **Categories of Data Subjects**: End-users of Controller's website; Controller's employees/admins.
- **Categories of Personal Data**: Chat logs, IP addresses, browser/device metadata, names/emails (if provided by end-user).
- **Duration**: The term of the Agreement plus the period until deletion in accordance with Section 6.

Annex 2: Technical and Organizational Measures (TOMs)

Processor maintains the following measures:

1. **Encryption**: Personal Data is encrypted at rest (AES-256) and in transit (TLS 1.2+).
2. **Access Control**: Strict identity and access management (IAM) with Multi-Factor Authentication (MFA).
3. **Anonymization**: Use of pseudonymization and anonymization techniques for analytics where feasible.
4. **Resilience**: Regular backups and disaster recovery procedures.
5. **Logging**: Comprehensive audit logging of access to Personal Data.

Annex 3: Subprocessors

The following Subprocessors are engaged by Processor:

1. **Cloud Infrastructure**: [e.g., Microsoft Azure / AWS] (EU Regions)
2. **AI Model Providers**: [e.g., OpenAI / Anthropic] (via API, no training on data)
3. **Analytics**: [e.g., PostHog / Plausible] (Privacy-focused)

Notification Mechanism: Changes to this list will be communicated via [EMAIL/DASHBOARD] at least 30 days in advance.