KRETA AI – DATA PROCESSING ADDENDUM (DPA) *Effective Date: June 1, 2025*

This Data Processing Addendum ("**DPA**") forms part of the Master Subscription Agreement ("**Agreement**") between **Kreta Inc**, a Delaware corporation with its principal office at 8407 Central Ave, Newark, CA 94560, USA ("**Kreta**"), and the entity identified as "Customer" in the Agreement ("**Customer**"). This DPA reflects the parties' agreement regarding the processing of Personal Data in accordance with applicable Data Protection Laws.

1. DEFINITIONS

1.1. **"Personal Data"** means any information relating to an identified or identifiable natural person that is processed by Kreta on behalf of Customer as part of the Services.

1.2. **"Data Protection Laws"** means all applicable laws relating to data protection and privacy including, where applicable, the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the UK GDPR, the California Consumer Privacy Act ("**CCPA**"), and any other similar laws.

1.3. **"Data Subject"** means the individual to whom Personal Data relates.

1.4. **"Sub-processor"** means any third party engaged by Kreta to process Personal Data on behalf of Customer.

1.5. The terms "Controller," "Processor," "Processing," and "Supervisory Authority" shall have the meanings given in the GDPR.

2. ROLE OF THE PARTIES

2.1. For the purposes of this DPA, Customer is the Controller and Kreta is the Processor with respect to Personal Data.

2.2. Customer determines the purposes and means of Processing Personal Data. Kreta shall process Personal Data only in accordance with Customer's documented instructions unless otherwise required by law.

3. PROCESSING DETAILS

Subject Matter	The provision of procurement and contract automation services to Customer
Duration of Processing	For the duration of the Agreement and as necessary to meet data retention obligations

Subject Matter	The provision of procurement and contract automation services to Customer
Nature & Purpose	Hosting, storing, processing, analyzing, and transmitting Personal Data to provide the Services
Types of Personal Data	Names, emails, job titles, transaction records, communication data, documents containing personal information
Categories of Data Subjects	Customer employees, contractors, vendors, and individuals whose data appears in Customer-provided documents

4. KRETA'S OBLIGATIONS

4.1. **Confidentiality.** Kreta shall ensure that all persons authorized to process Personal Data are bound by confidentiality obligations.

4.2. **Security.** Kreta shall implement appropriate technical and organizational measures to protect Personal Data against unauthorized access, loss, destruction, or disclosure in accordance with Annex 1.

4.3. **Sub-processors.** Kreta may use Sub-processors listed in Annex 2. Kreta will notify Customer of any intended changes to its Sub-processor list and allow objection within 10 days. Objections must be reasonable and based on data protection concerns.

4.4. **Data Subject Requests.** Kreta will assist Customer in responding to Data Subject requests to exercise rights under Data Protection Laws (e.g., access, deletion, rectification).

4.5. **Data Breach Notification.** In the event of a confirmed Personal Data Breach, Kreta shall notify Customer without undue delay and provide information to assist Customer in fulfilling breach notification obligations.

4.6. **Audit Rights.** Upon Customer's written request, Kreta will make available relevant information necessary to demonstrate compliance with this DPA and allow for audits or inspections under mutually agreed conditions.

5. CUSTOMER OBLIGATIONS

5.1. Customer represents and warrants that it has the right to provide Kreta with Personal Data and that such Processing is lawful.

5.2. Customer shall not use the Services to process special categories of personal data (as defined in Article 9 of the GDPR), unless explicitly agreed in writing.

7. RETURN OR DELETION OF DATA

Upon termination or expiration of the Agreement, Kreta shall delete or return all Personal Data within 30 days unless retention is required by applicable law.

8. LIABILITY

The liability of each party under this DPA shall be subject to the limitations of liability set forth in the Agreement.

9. GOVERNING LAW

This DPA shall be governed by and construed in accordance with the governing law specified in the Agreement.

Annex 1 – Security Measures

Kreta maintains the following minimum security measures: - Encryption of Personal Data in transit and at rest - Access control and authentication - Security incident response procedures - Regular penetration testing and vulnerability assessments - Employee training and background checks - Secure development practices

Annex 2 – Sub-processor List

Kreta uses the following Sub-processors to support delivery of its Services:

Name	Purpose	Location	Data Processed	Safeguards
Amazon Web Services, Inc. (AWS)	Cloud hosting, infrastructure, storage	USA, EU, Australia	Personal data stored and processed	ISO 27001, SOC 2, SCCs if applicable
Microsoft Azure	Cloud computing, backup, storage	USA, EU, Australia	Encrypted data at rest and in transit	ISO 27001, SOC 2, SCCs, access control
Pinecone Systems, Inc.	Vector database for semantic search	USA	Encrypted embeddings, metadata	ISO 27001, SOC 2, SCCs
Google	Internal email and	USA	Names, emails,	SCCs, ISO 27001,

Name	Purpose	Location	Data Processed	Safeguards
LLC (Workspace)	document management		contact metadata	access controls
OpenAI, L.L.C. (optional)	AI inference & language model use	USA	Prompt content, text snippets	No retention, pseudonymization, DPA
MongoDB, Inc.	Managed database services	USA, globally distributed regions	Application and user data	ISO 27001, SOC 2, encryption at rest

---

IN WITNESS WHEREOF, this DPA is entered into and becomes legally binding upon execution of the Agreement or applicable Order Form that references it.