DATA PROCESSING ADDENDUM

Aragon AI, Inc.

This Data Processing Addendum ("**DPA**") forms part of the Customer Terms of Service (the "**Agreement**") between Aragon AI, Inc. ("**Aragon**" or "**Vendor**") and the entity identified during registration ("**Customer**"). This DPA applies where Aragon Processes Customer Personal Data as a Processor on behalf of Customer in connection with providing the Services. This DPA is effective as of the effective date of the Agreement and terminates automatically upon termination of the Agreement.

Capitalized terms used but not defined in this DPA have the meanings given to them in the Agreement or in Attachment 1 (Definitions).

1. Data Processing and Protection

1.1 Scope and Roles. Customer is the Controller and appoints Aragon as Processor to Process Customer Personal Data on Customer's behalf for the purposes set out in Attachment 2 (Scope of Processing). Where Customer is itself a processor acting on behalf of a third-party controller, Customer: (a) is the single point of contact for Aragon; (b) is responsible for obtaining all necessary authorizations from such third-party controller; and (c) undertakes to issue all instructions and exercise all rights on behalf of such third-party controller.

1.2 Instructions. Aragon will Process Customer Personal Data only: (a) pursuant to Customer's documented instructions, including the Agreement, this DPA, and any configuration settings selected by Customer through the Services; and (b) as required by applicable law, in which case Aragon will inform Customer of the legal requirement before Processing unless prohibited from doing so. Aragon will promptly inform Customer if, in Aragon's reasonable opinion, an instruction infringes Data Protection Law.

1.3 Compliance. Each party will comply with its obligations under Data Protection Law with respect to its role.

1.4 Confidentiality. Aragon will ensure that personnel authorized to Process Customer Personal Data are bound by appropriate confidentiality obligations and receive appropriate data protection training.

1.5 Security. Aragon will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against Security Incidents, as set out in Attachment 3 (Technical and Organizational Measures). Aragon may update these measures from time to time, provided the updated measures do not reduce the overall level of security.

1.6 Deletion and Return. If the Agreement expires or is terminated by either party for any reason other than Customer's material breach, Customer may continue to access the Services solely for the purpose of retrieving Customer Personal Data for thirty (30) days following the effective date of expiration or termination. Upon termination for Customer's material breach, Aragon has no obligation to make Customer Personal Data available for retrieval. Unless retention is required under this Section 1.6, Aragon will delete all remaining copies of Customer Personal Data within sixty (60) days after the earlier of the end of the retrieval period or the effective date of termination for Customer's material breach; provided that, with respect to Face Data, the deletion timeframe in Section 2.3 controls. Aragon may retain Customer Personal Data to the extent required by applicable law, regulation, legal process, or governmental request, or as necessary in connection with any actual or reasonably anticipated litigation, audit, or regulatory investigation; either party may suspend deletion where a litigation hold or regulatory preservation obligation requires retention, and such retained data will be segregated from active Processing and deleted promptly upon expiration of the hold. Customer Personal Data retained in Aragon's standard backups remains subject to the confidentiality and security obligations in this DPA until deletion in the ordinary course of backup

rotation.

1.7 US State Privacy Laws. With respect to Customer Personal Data subject to the CCPA or other US State Privacy Laws, Aragon acts as a Service Provider or Contractor. Aragon will not: (a) Sell or Share Customer Personal Data within the meaning of the CCPA; (b) retain, use, or disclose Customer Personal Data for any purpose other than the specific purposes set out in Attachment 2 or as otherwise permitted by the CCPA; (c) retain, use, or disclose Customer Personal Data outside the direct business relationship between the parties; or (d) combine Customer Personal Data with personal information from other sources, except as permitted by the CCPA. The exchange of Customer Personal Data between the parties does not constitute a Sale. Aragon will promptly notify Customer if it determines it can no longer meet its obligations under the CCPA, and upon notice from Customer will take reasonable steps to stop and remediate any unauthorized Processing.

1.8 Deidentified Data. Aragon may Process Deidentified Data for its internal business purposes, including to improve the Services. Aragon will (a) maintain reasonable measures to ensure Deidentified Data cannot be associated with an individual, (b) publicly commit to maintain and use Deidentified Data in deidentified form, and (c) not attempt to reidentify Deidentified Data except as permitted by Data Protection Law.

1.9 Aragon as Controller. Aragon Processes certain operational data relating to the Services — including billing records, account management data, support communications, security and audit logs, and analytics and usage data — for its own business purposes as a Controller. Such Processing is outside the scope of this DPA. Aragon will handle such data in accordance with applicable law.

2. Face Data

This Section 2 applies in addition to, and without limiting, the other provisions of this DPA. "**Face Data**" means photographs End Users upload through Aragon's photo generation features for the sole purpose of generating AI content depicting the individual shown in those photographs, which may, depending on applicable law, constitute biometric identifiers, biometric information, or Sensitive Personal Information. Aragon does not identify or authenticate people in the images or videos End Users upload, nor does Aragon train its technology to do so.

2.1 Purpose Limitation. Aragon Processes Face Data to generate AI-generated content depicting the End User from whom the Face Data was collected, for use by that End User and by Customer in connection with Customer's internal business purposes ("**Permitted Face Data Processing**"). Aragon does not: (a) use Face Data to train or otherwise develop any general-purpose or foundation AI or machine learning model; or (b) combine Face Data from different End Users to create pooled training datasets.

2.2 No Sale or Monetization. Aragon does not sell, lease, trade, or otherwise profit from Face Data.

2.3 Retention. Aragon will permanently delete or anonymize Face Data in accordance with the retention schedule set out in Aragon's Privacy Policy. Notwithstanding the foregoing, Face Data will be deleted within thirty (30) days after the earliest of: (a) completion of any shorter automated retention cycle configured on Customer's account; (b) deletion by Customer through the Services; or (c) closure of Customer's account or termination of the End User's access to the Services. In no event will Face Data be retained longer than one (1) year from collection. When Face Data is deleted, it is permanently erased such that it cannot be recovered or reconstructed. Upon termination of the Agreement, Face Data is deleted in accordance with Section 1.6. Aragon maintains a written Face Data retention and destruction policy, publicly available at https://aragon.ai/privacy.

2.4 Subprocessor Flow-Down. Aragon will contractually prohibit all Subprocessors that Process Face Data from (a) training or otherwise developing general-purpose or foundation AI models on Face Data, (b) creating pooled Face Data training datasets, and (c) using Face Data for any purpose other than providing

the Services to Aragon.

2.5 Multi-User Account Consent. Where Customer accesses the Services under a Multi-User Account on behalf of its End Users, Customer represents and warrants that, prior to any End User uploading content from which Face Data may be derived, Customer has obtained all consents and provided all notices required under applicable law for: (a) the collection, storage, use, and processing of such Face Data by Aragon for the purpose of generating AI-generated content; (b) Customer's subsequent use, storage, distribution, and disclosure of the AI-generated content; and (c) the retention periods applicable to such Face Data.

2.6 Direct Collection from End Users. Where Aragon collects Face Data directly from an End User (rather than through a Customer's Multi-User Account), Aragon will obtain written consent from the End User prior to collection in a manner consistent with applicable law, including any applicable US state biometric privacy statutes, and will provide notice of the purpose, duration, and processing of the Face Data.

3. Processing Assistance

3.1 Data Subject Requests. Customer is responsible for responding to requests from Data Subjects to exercise rights under Data Protection Law (each, a "**Data Subject Request**"). To the extent permitted by law, Aragon will notify Customer without undue delay if Aragon receives a Data Subject Request directed to Customer's Processing. Taking into account the nature of Processing and the information available to Aragon, Aragon will provide commercially reasonable assistance to Customer in responding to Data Subject Requests that Customer cannot address through existing Services functionality. Aragon may charge a reasonable fee for assistance requiring material effort beyond Aragon's existing capabilities.

3.2 Security Incidents. Aragon will notify Customer of a Security Incident involving Customer Personal Data as soon as reasonably practicable after Aragon becomes aware of it, and in any event within any shorter or fixed timeframe required by applicable Data Protection Law. The notification will include, to the extent then known: (a) the nature of the Security Incident; (b) the categories and approximate number of Data Subjects and records affected; (c) the likely consequences; and (d) the measures taken or proposed to address it. Where full information is not available at the time of initial notification, Aragon will provide available information and supplement it promptly as additional information becomes known. Aragon will take commercially reasonable steps to mitigate the effects of the Security Incident and will cooperate with Customer's response and notification obligations.

3.3 Data Protection Impact Assessments. Taking into account the nature of Processing and the information available to Aragon, Aragon will provide commercially reasonable assistance to Customer in conducting data protection impact assessments and prior consultations with supervisory authorities, where required under Data Protection Law.

3.4 Records of Processing. Aragon will maintain records of its Processing of Customer Personal Data in accordance with Data Protection Law.

4. Audits

4.1 Reports. Aragon maintains SOC 2 Type II certification and may procure additional third-party audits to assess its compliance with applicable security standards. Upon Customer's written request, and subject to the confidentiality obligations in the Agreement, Aragon will provide Customer with summaries of its then-current audit reports ("**Reports**").

4.2 Customer Audits. Customer's audit rights are satisfied by Aragon's provision of the Reports under Section 4.1. Customer may request additional information only to the extent the Reports are not reasonably sufficient to evaluate Aragon's compliance with this DPA. On-site audits are not permitted except as required by applicable Data Protection Law. Any permitted on-site audit will be: (a) limited to documents and facilities

relevant to the Processing of Customer Personal Data; (b) conducted on at least thirty (30) days' advance written notice; (c) conducted during normal business hours with minimal business disruption; (d) conducted no more than once per twelve-month period; and (e) conducted by Customer or a mutually agreed independent auditor subject to confidentiality obligations. Customer will bear the costs of any on-site audit, including Aragon's reasonable internal costs. Audit findings are Aragon's Confidential Information.

5. Subprocessors

5.1 Authorization. Customer authorizes Aragon to engage Subprocessors. Aragon's current Subprocessors are listed at https://www.aragon.ai/legal/subprocessors.

5.2 Flow-Down. Aragon will enter into written agreements with each Subprocessor imposing data protection obligations no less protective than those set out in this DPA, including the applicable requirements of GDPR Article 28.

5.3 Changes. Aragon will notify Customer by email, or by updating the Subprocessor list, at least fifteen (15) days before a new Subprocessor begins Processing Customer Personal Data, or such shorter period (in no event less than ten (10) days) as is reasonably necessary to align with the notice period Aragon receives from its upstream subprocessors with respect to that Subprocessor. Customer may object in writing within ten (10) days on reasonable grounds relating to Data Protection Law. If Customer objects, the parties will cooperate in good faith to resolve the objection. If they cannot resolve it within thirty (30) days, either party may terminate the affected portion of the Services without liability. Aragon will not permit a new Subprocessor to begin Processing Customer Personal Data until the objection period has elapsed without objection or the objection has been resolved.

6. International Data Transfers

6.1 Transfer Mechanism. Where Customer Personal Data is transferred from the EEA, United Kingdom, or Switzerland to a country not subject to an adequacy decision, such transfers will be conducted pursuant to the SCCs (for EEA transfers) or the UK IDTA (for UK transfers), each of which is incorporated and deemed executed by this reference. If an alternative transfer mechanism (such as an adequacy decision or the EU–US Data Privacy Framework) becomes available and applicable to the transfer, the parties may rely on such mechanism instead.

6.2 SCC Implementation. The parties agree to Module 2 (Controller to Processor) of the SCCs, or Module 3 (Processor to Subprocessor) where Customer is itself a processor acting on behalf of a third-party controller. If Customer does not specify, Module 2 applies by default. The parties make the following choices: (a) the optional docking clause in Clause 7 applies; (b) in Clause 9, Option 2 applies and the notice period for Subprocessor changes is as set out in Section 5.3; (c) in Clause 11, the optional redress clause does not apply; (d) in Clause 17, Option 1 applies and the governing law is the law of Ireland; (e) in Clause 18(b), disputes will be resolved in the courts of Dublin, Ireland; and (f) Annexes I, II, and III to the SCCs are Attachments 2, 3, and 4 to this DPA, respectively.

6.3 Swiss FADP. For transfers subject to the Swiss Federal Act on Data Protection, the SCCs apply with the following modifications: the competent supervisory authority is the Federal Data Protection and Information Commissioner; references to "Member State" will not be read to prevent Data Subjects in Switzerland from exercising rights in Switzerland; and references to "GDPR" will be understood as references to the FADP.

6.4 UK IDTA. For transfers subject to the UK GDPR, the UK IDTA applies. Neither party may terminate the UK IDTA under Table 4 and Section 19 thereof without the written consent of the other.

6.5 Canada (PIPEDA). With respect to personal information of Canadian residents, Aragon will comply with applicable provisions of the Personal Information Protection and Electronic Documents Act (PIPEDA),

including notification to the Office of the Privacy Commissioner of Canada and to affected individuals of any breach of security safeguards involving a real risk of significant harm.

7. Liability

Each party's liability under this DPA is subject to the limitations of liability set out in the Agreement. Nothing in this DPA limits the rights of Data Subjects under Data Protection Law.

8. Miscellaneous

8.1 Conflict. To the extent of any conflict between this DPA and the Agreement with respect to the Processing of Customer Personal Data, this DPA controls. To the extent of any conflict between this DPA and the SCCs or UK IDTA, the SCCs or UK IDTA (as applicable) control.

8.2 Amendment. Aragon may amend this DPA from time to time by posting an updated version at aragon.ai/legal/dpa. Amendments are effective upon posting unless a later effective date is specified. Aragon will use reasonable efforts to notify Customer of material amendments by email or in-app notice. Customer's continued use of the Services after an amendment is effective constitutes acceptance. If Customer does not agree to an amendment, Customer's exclusive remedy is to discontinue use of the Services. Aragon will not amend this DPA in a manner that materially reduces the protections required by Article 28 of the GDPR (or equivalent provisions of other applicable Data Protection Law) for Processing subject to such law, and the SCCs and UK IDTA may be modified only as expressly permitted by their terms.

8.3 Notices. Notices under this DPA will be given to the addresses set out in the Agreement. Notices to Aragon's legal department may be sent to: Aragon AI, Inc., Attn: Legal Department, 440 N Barranca Ave #4760, Covina, CA 91723.

8.4 Survival. The obligations in this DPA survive termination of the Agreement to the extent required to give effect to Data Protection Law or to the parties' rights and obligations under the Agreement.

ATTACHMENT 1 — DEFINITIONS

"**Customer Personal Data**" means Personal Data that Aragon Processes on behalf of Customer in connection with providing the Services, as described in Attachment 2.

"**Controller**" means "controller" and "business" (and analogous terms) under Data Protection Law.

"**Data Protection Law**" means any law, regulation, or binding guidance relating to data protection or privacy that applies to the Processing described in this DPA, including the GDPR, the UK GDPR, the FADP, the CCPA, and other US State Privacy Laws, each as amended or replaced from time to time.

"**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates. Corresponds to "Consumer" under the CCPA and equivalent terms under other Data Protection Law.

"**Deidentified Data**" means information that cannot reasonably be linked to or associated with an identified or identifiable natural person.

"**End User**" means an individual authorized by Customer to access and use the Services on Customer's behalf.

"**FADP**" means the Swiss Federal Act on Data Protection of 19 June 1992, as amended.

"**Face Data**" has the meaning given in Section 2.

"**GDPR**" means Regulation (EU) 2016/679.

"**Multi-User Account**" means a Customer account under which multiple authorized End Users access the Services on behalf of a single Customer entity.

"**Personal Data**" means information relating to an identified or identifiable natural person, and includes "Personal Information" under the CCPA and equivalent terms under other Data Protection Law.

"**Process**" / "**Processing**" means any operation performed on Personal Data, whether or not by automated means, including collection, storage, use, disclosure, transmission, and erasure.

"**Processor**" means "processor," "service provider," and "contractor" (and analogous terms) under Data Protection Law.

"**SCCs**" means the Standard Contractual Clauses annexed to EU Commission Implementing Decision 2021/914 of June 4, 2021, as amended or replaced.

"**Security Incident**" means any unauthorized access to, or acquisition, use, disclosure, modification, or destruction of, Customer Personal Data, including any reasonably suspected unauthorized access, acquisition, use, disclosure, modification, or destruction of Customer Personal Data. Corresponds to "personal data breach" under the GDPR.

"**Services**" means the services provided by Aragon under the Agreement.

"**Subprocessor**" means any third party engaged by Aragon to Process Customer Personal Data on Aragon's behalf.

"**UK GDPR**" means the GDPR as incorporated into UK law by the Data Protection Act 2018, as amended.

"**UK IDTA**" means the UK International Data Transfer Addendum to the EU SCCs (version B1.0, in force 21 March 2022).

"**US State Privacy Laws**" means the CCPA and other US state comprehensive privacy laws applicable to the Processing described in this DPA.

ATTACHMENT 2 — SCOPE OF PROCESSING

Data Exporter (Customer)
Name, address, and contact: As identified in Customer's account at registration. Role: Controller (or Processor on behalf of a third-party controller); Business under the CCPA.

Data Importer (Aragon)
Name: Aragon AI, Inc. Address: 440 N Barranca Ave #4760, Covina, CA 91723. Contact: support@aragon.ai. Role: Processor; Service Provider or Contractor under the CCPA.

Subject Matter and Duration
The subject matter of Processing is the provision of AI content generation services as described in the Agreement. Processing continues for the duration of the Agreement, subject to the retention and deletion terms in Section 1.6 and Section 2.3.

Nature and Purpose of Processing
Collection, storage, transmission, AI content generation, and deletion in connection with providing the Services.

Categories of Data Subjects
End Users authorized by Customer to access the Services, including employees and contractors of Customer using the Services for business purposes.

Categories of Personal Data
Customer Personal Data Processed under this DPA may include: (a) account and profile information (such as name, email address, and company name); (b) device and session identifiers (such as User ID, Device ID, user agent, and IP address); (c) User Content uploaded by End Users (such as images and associated metadata); (d) demographic data provided to generate AI content (such as age range, gender, hair type, body type, and similar descriptive attributes); (e) Face Data (as defined in Section 2); (f) AI-generated output content; (g) query, chat, and prompt data submitted through the Services; and (h) payment processor identifiers. Aragon does not collect or store payment card data, which is processed directly by third-party payment processors.

Sensitive Categories
Face Data, which may, depending on applicable law, constitute biometric identifiers, biometric information, or Sensitive Personal Information. Face Data is Processed subject to the restrictions and safeguards in Section 2.

Frequency of Transfer
Continuous.

Retention Period
Face Data is retained as set out in Section 2.3. Other Customer Personal Data Processed under this DPA — including User Content (excluding Face Data), AI-generated output content, and query, chat, and prompt data — is retained for the duration of the Agreement, subject to Customer's deletion instructions through the Services, and thereafter in accordance with Section 1.6. Longer retention applies where required by law (including tax and anti-fraud recordkeeping), to prevent fraud or abuse, to honor Data Subjects' prior choices (including consent logs and opt-out preferences), or in connection with Aragon's Processing as a Controller as described in Section 1.9 (which is outside the scope of this DPA).

Competent Supervisory Authority
For EEA transfers, the Irish Data Protection Commission (subject to one-stop-shop rules). For UK transfers, the UK Information Commissioner's Office. For Swiss transfers, the Federal Data Protection and Information Commissioner.

ATTACHMENT 3 — TECHNICAL AND ORGANIZATIONAL MEASURES

Aragon's Services operate entirely in cloud infrastructure. Aragon does not operate physical servers; physical access controls apply to Aragon's cloud infrastructure providers and are governed by those providers' security certifications. Aragon's direct technical and organizational measures are set out below.

Access Control	Role-based access controls; multi-factor authentication for systems Processing Customer Personal Data; automatic session timeouts; access logging and monitoring; principle of least privilege; prompt termination of access when no longer required.
Encryption	Data in transit encrypted using TLS 1.2 or higher; data at rest encrypted using AES-256; encrypted backup media; secure management of encryption keys.
Network Security	Firewalls and intrusion detection systems; network segmentation; anti-malware controls; vulnerability scanning and patch management.
Vulnerability Management	Automated vulnerability scanning; prioritized remediation by severity; periodic penetration testing; evaluation of software updates before deployment.
Incident Response	Documented incident response plan; post-incident review; notification procedures consistent with Section 3.2.
Business Continuity	Regular data backups; disaster recovery plan with periodic testing; redundant infrastructure.
Personnel	Confidentiality obligations; data protection training; disciplinary procedures for unauthorized access.
Vendor Management	Contractual security requirements imposed on Subprocessors; periodic assessment of Subprocessor security practices.
Certification	Aragon maintains SOC 2 Type II certification. Current status is available at Aragon's Trust Center.

ATTACHMENT 4 — SUBPROCESSORS

Aragon’s current list of authorized Subprocessors is published at https://www.aragon.ai/legal/subprocessors and is incorporated by reference. Updates to this list are governed by Section 5.3 of this DPA.