DATA PROCESSING ADDENDUM (DPA)

Cension AB — Version: v1.5 — Effective Date: 2026-04-19

This Data Processing Addendum ("DPA") forms part of the Terms & Conditions or any applicable Service Agreement (the "Agreement") between Cension AB ("Cension") and the Customer.

The parties expressly acknowledge and agree that:

A. This DPA does not establish a joint controllership arrangement under Article 26 of the GDPR.

B. Each party remains solely responsible for its own compliance with Applicable Data Protection Laws in respect of its separate processing activities.

C. Cension processes Customer Personal Data solely on behalf of and under the documented instructions of the Customer.

D. Cension may process Service Data as an independent controller for the purposes set out in Section 9 (including operating, metering, billing, securing, supporting, and improving the Services; analytics; fraud and abuse prevention; and product development).

E. Cension does not engage in automated decision-making natively producing legal effects on Data Subjects.

Privacy, security, and DPA enquiries may be directed to **hello@cension.ai**.

1. DEFINITIONS

- **"Applicable Data Protection Laws"**: means applicable privacy or data protection laws, including the EU GDPR, UK GDPR, the EU–US Data Privacy Framework, and all applicable U.S. privacy statutes (including the CCPA) in force during the Term.
- **"Customer Personal Data"**: Any Personal Data processed by Cension or its Sub-processors on behalf of the Customer in connection with the Services.
- **"Service Data"**: Any data relating to the use, support, operation, or security of the Services, collected directly or indirectly by Cension from or about users of the Services or the Customer's use of the Services, for Cension's own purposes. Service Data includes, without limitation, application logs, request timings, error traces, model and provider

selections for generations, input and output token counts, credit accounting, usage and feature-engagement patterns, and similar operational, diagnostic, and telemetry signals.

- **"Sub-processor"**: Any processor engaged by Cension to process Personal Data on behalf of the Customer.
- **"Personal Data Breach"**: A confirmed breach of Cension's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data in Cension's possession, custody, or control. For the avoidance of doubt, a Personal Data Breach does **not** include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial-of-service attacks, or other network attacks on firewalls or networked systems.
- **"EU SCCs"**: The standard contractual clauses approved by the European Commission for transfers of personal data to third countries.

2. ROLES AND SUBJECT MATTER

1. **Roles:** For EU Personal Data, the Customer acts as a Controller and Cension acts as a Processor.
2. **Documented Instructions:** Cension shall Process Customer Personal Data only on the Customer's documented instructions to provide the Services. Cension may suspend or propose alternatives to any instruction it reasonably believes would breach Applicable Data Protection Laws or materially compromise the security of the Services.

3. CUSTOMER OBLIGATIONS

1. **Lawful Basis:** The Customer confirms it has a lawful basis and maintains all necessary rights, consents, and authorizations to provide Customer Personal Data to Cension.
2. **Appropriate Use:** The Customer is solely responsible for making appropriate use of the Services to maintain an appropriate level of security, including securing authentication credentials and systems.
3. **Backups:** The Customer is responsible for backing up Customer Personal Data it submits to the Services and for maintaining its own copies sufficient to meet its operational, regulatory, and business-continuity requirements. While Cension relies on provider-managed backup infrastructure as described in Section 10, Cension does not act as the Customer's system of record for backup and disaster-recovery purposes.
4. **Search-Driven Workflows:** The Customer acknowledges that where a Customer workflow builds a search query from Customer-provided inputs, the resulting query text may be transmitted to public search engines (for example, DuckDuckGo, Google Search, or Bing) to retrieve publicly available results. No Customer account identifier, end-user identifier, or session identifier is transmitted with such queries. The Customer is responsible for ensuring

it has a lawful basis, and any necessary consents, for including Personal Data in the inputs of any search-driven workflow, and shall not submit Special Categories of Personal Data (as defined in Article 9 GDPR) to such workflows except to the extent compatible with the Customer's own documented legal grounds.

4. CENSION'S OBLIGATIONS

1. **Processing Scope:** Cension shall process personal data solely to perform the Services, operate the underlying AI and software infrastructure, execute Customer instructions, and address technical issues.
2. **Confidentiality:** Cension will ensure that personnel processing personal data are contractually bound to maintain confidentiality and that access is strictly limited based on the principle of least privilege.
3. **Audits and Inspections:** Upon written request, Cension will provide information reasonably necessary to demonstrate compliance. If further audit is required by law, the Customer may conduct an audit no more than once per calendar year, upon providing at least thirty (30) days' advance written notice. All audits must be conducted during regular business hours, subject to strict confidentiality agreements, and at the Customer's sole expense. Any auditor engaged by the Customer must be mutually agreed in writing, must not be a competitor of Cension, and must be bound by written confidentiality obligations no less protective than those set out in the Agreement. The Customer shall not disclose any findings, data, or information obtained during an audit to any third party without Cension's prior written consent, except to the extent required by Applicable Law.
4. **Assistance (DSR & DPIA):** Cension shall, taking into account the nature of the processing, provide commercially reasonable assistance to the Customer through appropriate technical and organizational measures, to fulfill the Customer's obligation to respond to Data Subject Requests. If Cension receives a request directly from a Data Subject, Cension will promptly forward the request to the Customer. Cension will additionally assist the Customer in conducting Data Protection Impact Assessments (DPIAs) where required by Applicable Data Protection Laws.
5. **Government Agency Requests:** If Cension receives a formal legal request from any government intelligence or law enforcement agency for access to Customer Personal Data, Cension shall attempt to redirect the agency to request that data directly from the Customer. Cension shall give the Customer reasonable prior notice of the demand, unless legally prohibited from doing so.
6. **Extraordinary Assistance:** Where the Customer requests manual data export, bespoke deletion, custom audit support, Data Subject Request fulfilment beyond what Cension's standard self-service tools can deliver, or other similar extraordinary assistance, and fulfilment of such request requires more than a de minimis engineering or legal effort, Cension may charge the Customer its reasonable, documented costs at Cension's then-

current professional-services rates, except to the extent such charges are prohibited by Applicable Data Protection Laws.

5. SECURITY AND TECHNICAL MEASURES

1. **Appropriate Measures:** Cension shall maintain appropriate administrative, physical, technical, and organizational security measures intended to protect personal data against accidental or unauthorized access, disclosure, loss, or alteration, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing.
2. **Current Controls:** Today, Cension's controls include encryption in transit using industry-standard protocols (TLS 1.2 or higher), encryption at rest using industry-standard algorithms (e.g., AES-256) for managed databases and object storage, role-based access control (RBAC) for production systems, network-restricted access to cloud management consoles, structured audit logging, and end-user authentication via email-and-password (passwords stored using a strong, salted password-hashing function) or Sign-in with Google.
3. **Roadmap Controls:** Cension is actively strengthening its security posture. Multi-factor authentication (MFA) for all employee access to production infrastructure, migration of application secrets to a centralized secrets-management service, and customer-facing MFA (TOTP / WebAuthn) are on the near-term roadmap. Cension will publish updated Technical and Organizational Measures in Annex 2 as these controls are delivered.
4. **Information Security Program:** Cension is developing a formal, documented information security program aligned with recognized industry practices (for example, controls inspired by ISO/IEC 27001 and SOC 2). A formally documented program, together with third-party SOC 2 and ISO/IEC 27001 attestations, is on the roadmap; in the interim, Cension operates and maintains the technical and organizational controls described in this Section 5 and in Annex 2.

6. INCIDENT MANAGEMENT

1. **Notification:** Cension will inform the Customer **without undue delay** after confirming a Personal Data Breach under Applicable Data Protection Laws. To the extent such information is available to Cension at the time of notification, or becomes available thereafter, Cension’s notification will describe: (i) the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) the likely consequences of the Personal Data Breach; and (iii) the measures taken or proposed to be taken by Cension to address the Personal Data Breach and, where appropriate, to mitigate its possible adverse effects. Where and insofar as it is not possible

to provide all of the foregoing information at the same time, Cension may provide such information in phases as it becomes available.

2. **Cooperation:** Cension shall investigate the breach, take commercially reasonable measures to identify its root cause, and coordinate with the Customer regarding mandatory supervisory authority notifications.
3. **Customer-Caused Breaches:** The obligations in this Section do not apply to the extent a Personal Data Breach is caused by the Customer, the Customer's affiliates, or anyone acting on the Customer's behalf (for example, through compromise of Customer-side credentials, misconfiguration of Customer-managed systems, or the Customer's upload of content in violation of the Agreement or the Acceptable Use Policy). In such cases, Cension will inform the Customer of the information it discovers up to the point at which it identifies the Customer (or a party acting on the Customer's behalf) as the cause, and Cension may charge the Customer for any extraordinary assistance requested by the Customer in connection with the investigation or remediation of such a breach.
4. **No Admissions in Customer Notifications:** If the Customer determines to notify any supervisory authority, data subjects, or the public of a Personal Data Breach in a manner that refers to or identifies Cension, the Customer shall, where legally permitted, notify Cension in advance and consider in good faith any clarifications or corrections Cension may reasonably request concerning Cension's involvement.

7. SUB-PROCESSING

1. **General Consent:** The Customer provides general authorization for Cension to engage Sub-processors (for example, cloud hosting providers, foundation-model and AI providers, payment processors, and communications providers) to process Customer Personal Data in connection with the Services. Cension may continue to use Sub-processors already engaged as of the effective date of this DPA.
2. **Current List:** The current list of Sub-processors is published at https://cension.ai/sub-processors. Customers are encouraged to review the list periodically. Cension may update the list from time to time.
3. **Flow-Down:** Where Cension engages a Sub-processor to process Customer Personal Data, Cension shall impose on that Sub-processor data-protection obligations substantially equivalent to those set out in this DPA.
4. **Objection and Resolution:** If the Customer objects to a new Sub-processor on reasonable grounds relating to the protection of Personal Data, the Customer shall notify Cension in writing at hello@cension.ai. The parties shall cooperate in good faith to find a mutually acceptable resolution. If the parties are unable to reach a mutually acceptable resolution, the Customer's sole and exclusive remedy is to terminate the affected Services by providing written notice to Cension and to receive a pro-rata refund of any prepaid fees applicable to the unused portion of the then-current subscription term for those affected Services.

8. INTERNATIONAL DATA TRANSFERS

1. **Transfer Mechanisms:** Cension shall not transfer EU Personal Data outside the EU/EEA unless the transfer is covered by an adequacy decision or appropriate safeguards.
2. **Standard Contractual Clauses:** For transfers to third countries without an adequacy decision, the parties agree that the EU SCCs (Module 2: Controller to Processor) apply and are incorporated by reference. For the purposes of the EU SCCs, the governing law shall be the laws of Sweden, and the competent supervisory authority shall be the Swedish Authority for Privacy Protection (IMY).
3. **UK & Swiss Transfers:** For transfers subject to the UK GDPR or Swiss FADP, the EU SCCs shall apply as amended by the UK Information Commissioner's Office (ICO) International Data Transfer Addendum, or the Swiss Federal Data Protection and Information Commissioner's adaptations, respectively.
4. **US-Recipient Sub-processors:** The Customer acknowledges that delivering the Services necessarily involves routine transfers of Customer Personal Data to Sub-processors established in the United States. In particular:
    - **OpenAI OpCo, LLC** (foundation-model inference) — transfer mechanism: EU–US Data Privacy Framework (DPF) and, as fallback, EU SCCs Module 2.
    - **Google LLC** (foundation-model inference, Gmail SMTP fallback, Sign-in with Google, and Customer-authorized Google Drive read-only file retrieval) — transfer mechanism: EU–US Data Privacy Framework (DPF) and, as fallback, EU SCCs Module 2.
    - **Voyage AI, Inc.** (text embeddings) — transfer mechanism: EU SCCs Module 2.
    - **xAI Corp.** and **Groq, Inc.** (foundation-model inference) — transfer mechanism: EU SCCs Module 2.
    - **Stripe** (payments) — transfer mechanisms: Data Privacy Framework and/or EU SCCs as applicable to the contracting Stripe entity.
5. **Transfer Fallback:** If any transfer mechanism relied upon becomes invalid or ceases to apply, Cension will, in good faith, assess and implement an alternative lawful mechanism where commercially reasonable. Where no such alternative is available, Cension may suspend or reconfigure the affected processing activity without liability to the Customer.

9. USE OF CUSTOMER DATA AND ARTIFICIAL INTELLIGENCE

1. **Service Data Usage:** Cension may collect and process Service Data as an independent controller for its own business purposes, including to operate, meter, bill, secure, support, and improve the Services; to investigate fraud, spam, or wrongful or unlawful use of the Services; to develop, optimize, and maintain the Services; and as otherwise permitted or required by Applicable Data Protection Laws. For the avoidance of doubt, Service Data is distinct from Customer Personal Data, and the deletion, export, and isolation obligations applicable to Customer Personal Data do not apply to Cension's internal processing of

Service Data. Aggregated, de-identified, and non-identifying patterns derived from Service Data may be retained and used by Cension indefinitely for operating, securing, and improving the Services and for related analytics and product development. To the extent Service Data contains personal data, Cension processes such personal data on the basis of its legitimate interests in operating, securing, and improving the Services, and statutory data subject rights under Applicable Data Protection Laws remain unaffected by this Section. The Customer acknowledges that no royalty, fee, or other remuneration is due for Cension's processing of Service Data under this Section, and the Customer has no right to opt out of Cension's processing of Service Data for the purposes set out in this Section so long as the Customer continues to use the Services.

2. **AI / ML Training Commitment and Isolation:** Cension does not train, fine-tune, or maintain any proprietary AI or ML model (global, shared, or per-account) on Customer Personal Data. Customer Personal Data processed through third-party foundation-model Sub-processors is transmitted on the commercial tier that, per each Sub-processor's then-current published terms, does not authorize the Sub-processor to use API inputs to train its generally-available models. If a Sub-processor changes its default training posture, Cension will re-evaluate its use of that provider and update the Sub-processor list accordingly. Customer Personal Data is logically isolated at the application layer within a shared multi-tenant environment; dedicated single-tenant environments, customer-managed encryption keys, and additional isolation controls are available under a separately signed Enterprise Service Agreement. Cension may derive aggregated, product-agnostic operational heuristics (for example, column-name patterns and context-type aliases) from processing activity; no user-identifying or account-identifying data is persisted in those reference datasets. For the avoidance of doubt, this Section 9.2 applies only to Customer Personal Data; Cension's use of non-personal Content (as defined in the Agreement) for operating, developing, and improving the Services — including the training, fine-tuning, evaluation, and operation of Cension's proprietary AI and ML models, search, indexing, and ranking systems, and other internal components of the Services — is governed by the license granted under Section 3.1 of the Agreement and is not restricted by this DPA.
3. **U.S. Privacy Laws:** To the extent Cension's processing of Customer Personal Data under the Agreement is subject to the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act) or other substantially similar U.S. state privacy statutes (collectively, "U.S. Privacy Laws"), Cension acts as a "Service Provider" or "Contractor" (as defined in the applicable U.S. Privacy Laws). In that capacity, Cension shall:
    - use, retain, and disclose Customer Personal Data only as necessary to perform the business purposes specified in the Agreement or as otherwise permitted by U.S. Privacy Laws;
    - provide the same level of privacy protection for Customer Personal Data as is required of a "Service Provider" or "Contractor" under each applicable U.S. Privacy Law;
    - notify the Customer without undue delay if Cension determines it can no longer meet its obligations under U.S. Privacy Laws in respect of Customer Personal Data; and

- cooperate in a commercially reasonable manner with the Customer to stop and remediate any unauthorized use of Customer Personal Data.

Cension shall **not**:

- "sell" or "share" Customer Personal Data (as such terms are defined in the CCPA);
- retain, use, or disclose Customer Personal Data for any purpose other than the business purposes specified in the Agreement, or for a commercial purpose other than those business purposes, except as otherwise permitted by U.S. Privacy Laws; or
- combine Customer Personal Data received from the Customer with Personal Data received from or on behalf of another person, or Personal Data Cension collects from its own interactions with a consumer, except as permitted by U.S. Privacy Laws.

10. DELETION AND RETURN

1. **Post-Termination:** For a period of at least ninety (90) days following termination of the Agreement, Cension will retain Customer Personal Data in an accessible form to allow the Customer to export such data using Cension's then-available self-service export tools. After the expiry of that ninety (90) day period, Cension may delete or irreversibly anonymize Customer Personal Data in accordance with Section 10.2, without further notice. Any non-standard export format, delivery medium, or engineering assistance beyond self-service is subject to Section 4.6 (Extraordinary Assistance).
2. **Data Deletion:** Following this export period, or upon explicit written instruction from the Customer, Cension shall securely delete or irreversibly anonymize Customer Personal Data from its primary application records. Cension is in the process of rolling out complete cascade deletion across all subordinate application tables and blob-level deletion of uploaded files; until that rollout is complete, Cension will action deletion requests manually where necessary.
3. **Backups:** Cension relies on provider-managed backup retention, including point-in-time recovery over the provider's managed retention window and geo-redundant backups within the EEA. Customer Personal Data contained in such backups expires on the provider-managed schedule. Cension does not selectively purge individual Customer Personal Data from backup media; superseded backups are overwritten in the ordinary course.
4. **Legal Holds:** Cension may retain Customer Personal Data to the extent, and for the period, required by Applicable Law or to establish, exercise, or defend legal claims.

11. CUSTOMER INDEMNITY

1. **Scope:** The Customer hereby releases Cension and its affiliates, officers, directors, employees, and agents, and shall defend, indemnify, and hold the foregoing harmless, from and against any claim, investigation, regulatory enforcement action, fine, loss, or reasonable legal cost arising out of or in connection with: (i) the Customer's instructions,

configurations, or data provided to Cension; (ii) the Customer's failure to secure a lawful basis, required consents, or required notices for the processing of Customer Personal Data under the Services; (iii) the Customer's use of the Services in violation of the Agreement, this DPA, the Acceptable Use Policy, or Applicable Data Protection Laws; (iv) the Customer's upload of content in violation of Annex 1 (D) (prohibited categories of personal data); or (v) any other breach by the Customer, the Customer's affiliates, or anyone acting on the Customer's behalf of this DPA or Applicable Data Protection Laws.

2. **Exclusions:** The foregoing indemnity does not extend to fines or liabilities imposed on Cension to the extent directly caused by Cension's own acts or omissions that are independently found to constitute a material breach of this DPA.
3. **Procedure:** Cension shall give the Customer prompt written notice of any claim subject to indemnification under this Section and shall provide reasonable cooperation in the defense of such claim at the Customer's expense. The Customer may control the defense and settlement of any such claim, provided that the Customer may not settle any matter that admits fault on the part of Cension or imposes non-monetary obligations on Cension without Cension's prior written consent.
4. **Caps and Limits of Liability:** Each party's liability arising under or in connection with this DPA is subject to the exclusions and limitations of liability set out in the Agreement. Neither party shall be liable to the other for any loss of profits, revenue, goodwill, business interruption, or for any indirect, special, incidental, punitive, exemplary, or consequential damages of any kind, regardless of the theory of liability.

12. MISCELLANEOUS

1. **Order of Precedence:** In case of conflict between this DPA and any other term of the Agreement with respect to the processing of Customer Personal Data, this DPA shall prevail to the extent of the conflict. To the extent the EU SCCs are incorporated under Section 8, they shall prevail over this DPA in case of any conflict with respect to the matters they govern.
2. **Governing Law and Jurisdiction:** This DPA shall be governed by and construed in accordance with the laws of Sweden, consistent with the governing-law provisions of the Agreement. The parties agree that the competent courts of Sweden shall have exclusive jurisdiction to resolve any disputes arising under or in connection with this DPA, except as otherwise required by Applicable Data Protection Laws.
3. **Severability:** If any provision of this DPA is held invalid or unenforceable, the remaining provisions shall remain in full force and effect, and the parties shall replace the invalid provision with a valid one that most closely reflects the parties' original intent.
4. **Survival:** The provisions of Sections 9 (Use of Customer Data), 10 (Deletion and Return), 11 (Customer Indemnity), and this Section 12 shall survive termination of the Agreement for so long as Cension retains any Customer Personal Data.

5. **Entire Addendum:** This DPA, together with the Agreement and the Annexes attached hereto, constitutes the entire understanding between the parties with respect to the processing of Customer Personal Data and supersedes all prior agreements or understandings on that subject, whether written or oral.

ANNEX 1: Details of Processing

A. List of Parties

Data Exporter (Controller):

- **Name:** The Customer, as identified in the Agreement or Order Form (acting on behalf of itself and its Permitted Affiliates).
- **Address:** The Customer's address as set out in the Agreement, Order Form, or Cension account.
- **Contact person:** The administrative or privacy contact designated by the Customer in its Cension account.
- **Role:** Controller.
- **Activities relevant to the data transferred:** Processing of Customer Personal Data in connection with the Customer's use of the Services, as described in Section B below.

Data Importer (Processor):

- **Name:** Cension AB (Swedish Org. No. 559470-4768).
- **Address:** Rådmansgatan 80A, 113 60 Stockholm, Sweden.
- **Contact person:** hello@cension.ai.
- **Role:** Processor.
- **Activities relevant to the data transferred:** Processing of Customer Personal Data in connection with providing, securing, and maintaining the Services, as described in Section B below.

B. Nature and Purpose of Processing

Cension is an AI-powered automation and data-enrichment platform. The processing comprises the hosting, storage, compilation, API-transmission, and AI-assisted generation of commerce and operational metadata to provide, secure, and maintain the Services.

C. Categories of Data Subjects

Customer's authorized users (e.g., employees, contractors), and end-users or individuals whose data may be incidentally contained in product catalogs, text fields, or datasets uploaded by the Customer to the platform.

D. Categories of Personal Data

Names, email addresses, contact details, operational metadata, and any text or dataset contents freely uploaded or synchronized to the Cension API by the Customer. Cension expressly prohibits the uploading of protected health information (PHI), primary payment-card data (PAN / CVV), biometric identifiers, government-issued identifiers, and any other special-category personal data under GDPR Article 9, unless expressly authorized under a separately signed Enterprise Service Agreement.

ANNEX 2: Technical and Organizational Measures (TOMs)

Cension implements the following measures to protect Customer Personal Data. Controls identified as **(roadmap)** are in active development and will be delivered in a future release; Cension will update this Annex when they ship.

- **Encryption in transit:** Industry-standard protocols (TLS 1.2 or higher) at all application ingress points.
- **Encryption at rest:** Industry-standard algorithms (e.g., AES-256) for managed databases and object storage, using the cloud provider's transparent-data-encryption facilities.
- **Access control:** Role-based access control (RBAC) inside the application (tiered, with owner, admin, and member roles); network-restricted access to cloud management consoles for engineering staff, on a least-privilege basis.
- **Authentication:** End-user authentication via email-and-password or Sign-in with Google; passwords stored using a strong, salted password-hashing function; customer-facing multi-factor authentication (TOTP / WebAuthn) **(roadmap — in development)**.
- **Infrastructure MFA:** Enforcement of multi-factor authentication for all employee access to production infrastructure **(roadmap — in development)**.
- **Secrets management:** Application secrets are currently managed via environment configuration; migration to a centralized secrets-management service **(roadmap — in development)**.
- **Logging and monitoring:** Structured application audit logging; centralized platform telemetry via the cloud provider's monitoring service.
- **Resiliency:** Cloud-native architecture hosted within the EEA with provider-managed point-in-time recovery and geo-redundant backups within the EEA.
- **Vulnerability management:** Systematic tracking and remediation of identified vulnerabilities based on severity scoring; third-party penetration testing **(roadmap)**.

- **Certifications:** SOC 2 Type I / ISO/IEC 27001 **(roadmap)**.