

Data Processing Agreement (Pilot)

Encephlo, Inc., a Delaware corporation ("Processor" or "Encephlo") [Customer Legal Name] ("Controller" or "Institution")

Important — please read. This document is a **template** Encephlo provides to prospective institutional customers as a starting point for the Data Processing Agreement that will accompany the pilot service order. It is **not legal advice** and is not a binding offer until executed by both parties. The Institution's Office of General Counsel and Encephlo's counsel should review and red-line before signature. Square-bracketed text [like this] is intended to be replaced or confirmed at execution time.

Effective Date: [Effective Date] **Pilot Term:** [Pilot Term – e.g., Fall 2026 academic semester, ending Dec 20, 2026] **Underlying Agreement:** the pilot order form / letter of engagement between the parties, dated [Order Date] (the "Pilot Agreement").

1. Definitions

For the purposes of this Data Processing Agreement (this "DPA"):

- **"Customer Data"** means any data, including Personal Data and Education Records, that the Institution or its Authorized Users provide to, upload to, or generate within the Encephlo Service, and any data that Encephlo derives from it in providing the Service.
 - **"Education Records"** has the meaning given in the U.S. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and 34 CFR Part 99 ("FERPA").
 - **"Personal Data"** means information relating to an identified or identifiable natural person, including as defined under applicable U.S. state privacy laws (e.g., California CCPA/CPRA, Colorado CPA, Connecticut CTDPA, Virginia VCDPA, Texas TDPSA).
 - **"Authorized User"** means a faculty member, staff member, or student of the Institution authorized by the Institution to use the Service.
 - **"Service"** means the Encephlo B2B Educator Pilot product, comprising the Educator Studio, Student Web Tutor, Canvas LMS sync, and Insights, as described at [security-and-data-flow.md](#) §1.
 - **"Subprocessor"** means a third party engaged by Encephlo to process Customer Data, as listed in [subprocessors.md](#).
 - **"Security Incident"** means any confirmed unauthorized access to, disclosure of, alteration of, or loss of Customer Data in Encephlo's custody.
-

2. Roles of the Parties

2.1. The Institution is the data **controller** of Customer Data and, where applicable, the **educational agency or institution** under FERPA.

2.2. Encephlo acts solely as a data **processor / service provider / school official**, processing Customer Data only on the Institution's documented instructions to deliver the Service.

2.3. **FERPA — School Official Designation.** The Institution designates Encephlo as a "school official" with a "legitimate educational interest" in Customer Data that constitutes Education Records, in accordance with FERPA 34 CFR § 99.31(a)(1)(i)(B)(1). Encephlo will:

- (a) perform a service for which the Institution would otherwise use employees;
 - (b) be under the direct control of the Institution with respect to the use and maintenance of Education Records;
 - (c) use Education Records only for authorized purposes; and
 - (d) not redisclose Education Records to any party other than the Institution or its authorized agents, except as permitted by FERPA or expressly authorized in writing by the Institution.
-

3. Scope, Nature, and Purpose of Processing

3.1. **Subject matter.** Provision of the AI tutoring Service to the Institution's Authorized Users.

3.2. **Duration.** The Pilot Term, plus any deletion / return period under §10.

3.3. **Categories of data subjects.** Faculty members, staff members, and students of the Institution who are Authorized Users.

3.4. **Categories of Personal Data.** Account profile (name, email), authentication metadata, tutor configurations, course materials uploaded or synced from Canvas, student-tutor chat transcripts, AI-derived engagement summaries, server-side logs (UID, timestamps, request metadata). For the full schema, see `security-and-data-flow.md` §3.

3.5. **Sensitive data.** No special-category personal data (health, biometric, precise geolocation, financial account, government ID) is intentionally processed. The Institution shall not knowingly upload such data to the Service.

3.6. **Purpose.** Processing is solely for the purposes of (i) delivering the Service, (ii) providing customer support, (iii) maintaining and securing the Service, and (iv) complying with the parties' legal obligations.

4. Encephlo's Obligations as Processor

Encephlo will:

- 4.1. Process Customer Data only on the documented instructions of the Institution, which are deemed to include the Pilot Agreement, this DPA, and the Institution's reasonable subsequent written instructions.
- 4.2. **Not sell** Customer Data and **not share** it for cross-context behavioral advertising (as those terms are defined in U.S. state privacy laws).
- 4.3. **Not use Customer Data to train, fine-tune, or improve any general-purpose foundation model**, whether Encephlo's own or any third party's. Encephlo's AI inference subprocessor (Google LLC, Vertex AI) is contractually committed to not using Customer Data submitted to Vertex AI to train its foundation models, per Google's Cloud Data Processing Addendum and Vertex AI service-specific terms.
- 4.4. Restrict access to Customer Data to personnel with a documented need-to-know, subject to written confidentiality obligations.
- 4.5. Implement and maintain the technical and organizational security measures described in §6 and Annex A.
- 4.6. Promptly notify the Institution of any legally binding request for disclosure of Customer Data by a law-enforcement authority or regulator, unless prohibited by law from doing so.
- 4.7. Cooperate, at the Institution's reasonable expense, with the Institution's response to data-subject requests, regulatory inquiries, and audits per §7.
-

5. Subprocessing

- 5.1. The Institution provides general written authorization for Encephlo to engage Subprocessors, subject to this section.
- 5.2. The current list of Subprocessors is at `subprocessors.md`. Encephlo will provide at least **30 days' prior written notice** to the Institution before engaging any new Subprocessor that materially changes how Customer Data is processed.
- 5.3. The Institution may object in good faith on documented privacy or security grounds within 15 days of notice. If the parties cannot in good faith agree on a remediation, either party may terminate the affected portion of the Service without penalty.
- 5.4. Encephlo will impose data-protection obligations on each Subprocessor no less protective than those in this DPA, and Encephlo remains responsible for each Subprocessor's compliance.
-

6. Security

- 6.1. Encephlo will maintain a written information security program with administrative, technical, and physical safeguards designed to protect Customer Data, including those summarized in **Annex A** (Security Measures). Annex A is derived from `security-and-data-flow.md` and `hecvat-lite.md`, which are

incorporated here by reference.

6.2. Encephlo will not materially weaken the safeguards in Annex A during the Pilot Term.

6.3. **Encryption.** All Customer Data is encrypted in transit (TLS 1.2+) and at rest (AES-256, Google-managed keys) by default.

6.4. **Access control.** Authorization is enforced by Firestore Security Rules and Cloud Storage Security Rules in addition to application-level checks. Per-tenant data isolation is described in `security-and-data-flow.md` §7.

7. Audits

7.1. Encephlo will, on the Institution's reasonable written request and no more than once per twelve-month period (except in connection with a Security Incident), provide:

- (a) the then-current `security-and-data-flow.md` and `hecvat-lite.md`;
- (b) a current `subprocessors.md`;
- (c) any then-current third-party security attestations (e.g., SOC 2) Encephlo holds; and
- (d) reasonable written responses to a security questionnaire from the Institution.

7.2. If the Institution's reasonable security review demonstrates that the above documentation is insufficient, the parties will discuss a mutually agreeable on-site or virtual audit at the Institution's expense, subject to reasonable confidentiality, scheduling, and scope constraints.

8. Data Subject Rights

8.1. Encephlo will provide the Institution with reasonable assistance, by appropriate technical and organizational measures, to enable the Institution to respond to requests by data subjects to exercise their rights under applicable law (access, correction, deletion, portability, opt-out).

8.2. Where a data subject contacts Encephlo directly, Encephlo will, unless prohibited by law, redirect the request to the Institution.

9. Security Incident Notification

9.1. **Notification commitment.** Encephlo will notify the Institution of a confirmed Security Incident affecting the Institution's Customer Data **without undue delay and in any case within 72 hours** of confirmation.

9.2. The notification will include, to the extent then known: the nature of the incident, the categories and approximate number of data subjects and records affected, the likely consequences, and the measures taken or proposed to address the incident.

9.3. Encephlo will cooperate in good faith with the Institution's investigation and reasonable mitigation steps, and will provide updates as material new facts become available.

10. Return / Deletion of Customer Data

10.1. **At the Institution's request** during the Pilot Term, or **within 30 days of termination or expiration**, Encephlo will, at the Institution's option, return or **permanently delete** Customer Data, except where retention is required by applicable law (in which case Encephlo will continue to protect such data per this DPA until deletion is permitted).

10.2. Deletion includes Customer Data in Firestore, Cloud Storage, embedding chunks, and the Insights cache, and applies to live systems within 30 days and to operational backups within 90 days from the deletion date.

10.3. Encephlo will provide written confirmation of deletion on request.

11. International Data Transfers

11.1. Encephlo's primary processing occurs in the United States (Cloud Firestore `nam5`, Cloud Functions and App Hosting in `us-central1`, Cloud Storage US multi-region).

11.2. **AI inference disclosure.** Vertex AI inference currently uses Google's `global` endpoint, as required by current model availability. Per Google's CDPA, Google's confidentiality, security, and sub-processing commitments apply globally and Customer Data is not used to train Google's foundation models. Encephlo will pin Vertex AI to a U.S. regional endpoint once the production model becomes available there.

12. FERPA-Specific Provisions

12.1. **No redisclosure.** Encephlo will not redisclose Education Records except (i) back to the Institution, (ii) to its authorized Subprocessors as permitted by this DPA, (iii) as authorized in writing by the Institution, or (iv) as compelled by lawful process (with notice to the Institution where legally permitted).

12.2. **Use limitation.** Education Records will be used solely to provide the Service to the Institution.

12.3. **De-identification.** Encephlo may use de-identified data (stripped of direct and indirect identifiers per FERPA's de-identification guidance) to operate, analyze, and improve the Service. AI-derived engagement summaries that the educator views in the Insights tab are **not** de-identified for that educator's purposes; Encephlo will not use them outside the educator's tenant.

12.4. **Directory information.** The Institution remains responsible for designating directory-information categories under FERPA. Encephlo treats all Education Records as non-directory by default.

13. State-Specific Privacy Provisions

To the extent applicable to the Institution and its data subjects:

13.1. **California (CCPA/CPRA service-provider).** Encephlo acts as a "service provider" and will not (i) sell or share Personal Information, (ii) retain, use, or disclose Personal Information for any purpose other than the business purposes specified in the Pilot Agreement, or (iii) combine Personal Information with personal information that Encephlo receives from another source, except as permitted under §1798.140(j).

13.2. **Other state laws.** To the extent Colorado CPA, Connecticut CTDPA, Virginia VCDPA, Texas TDPSSA, or other applicable state privacy laws apply, Encephlo acts as a "processor" and will comply with its obligations as such, including assistance with controller assessments and data-subject rights.

14. Term and Termination

14.1. This DPA takes effect on the Effective Date and continues for the Pilot Term and any deletion / return period under §10.

14.2. Sections 1, 4.2, 4.3, 9, 10, 12, 14, and 15 survive termination.

15. Miscellaneous

15.1. **Order of precedence.** In the event of conflict between this DPA and the Pilot Agreement, this DPA controls with respect to Customer Data processing.

15.2. **Amendments.** This DPA may be amended only in a writing signed by both parties.

15.3. **Counterparts.** This DPA may be executed in counterparts, including electronic signatures, each of which is an original.

Signatures

Encephlo, Inc. Name: [Authorized Signatory] Title: [Title] Date: [Date] Signature:

[Customer Legal Name] Name: [Authorized Signatory] Title: [Title] Date: [Date] Signature:

Annex A — Security Measures

This Annex summarizes the technical and organizational measures Encephlo maintains. The full description is at `security-and-data-flow.md` and `hecvat-lite.md`, which are incorporated by reference.

Control area	Measure
Encryption in transit	TLS 1.2+ for all client/server and server/Google traffic.
Encryption at rest	AES-256 with Google-managed keys (Firestore, Cloud Storage, Cloud Logging).
Identity & authentication	Firebase Authentication (email/password, Google, Microsoft); Firebase ID tokens (short-lived JWTs).
Authorization & tenant isolation	Firestore Security Rules + Cloud Storage Security Rules; per-educator data isolation; server-only access to Canvas tokens, vector chunks, and roster writes.
Application security	Code review on all changes; dependency tracking via <code>npm audit</code> ; least-privilege Cloud Functions service account.
Network security	Google's edge protections; HTTPS-only; no public Firestore/Storage paths.
Logging & monitoring	Cloud Logging, default 30-day retention; Cloud Functions error alerts.
Backup & recovery	Firestore PITR (Point-in-Time Recovery) available within 7 days for production.
Incident response	Founder is incident commander; reachable at suraj@encephlo.com ; 72-hour notification commitment per §9.
Data isolation testing	Firestore rules unit tests for B2B paths exist in the repo; new B2B paths gated by review.

Data deletion	<code>deleteEducatorTutor</code> cascade for educator-initiated; institution-initiated under §10.
Personnel	Founder-led; all contributors under written confidentiality obligations.

Annex B — Subprocessor List

See `subprocessors.md` . The list there as of the Effective Date is incorporated by reference and treated as Annex B for purposes of §5.

Template version: 0.2 (September 18, 2026). Generated from `security-and-data-flow.md` v1.