

DATA PROCESSING ADDENDUM

Sycoindex — The Honesty Layer for Every LLM · Template v1.0 · April 2026

TEMPLATE NOTICE. This is a reference Data Processing Addendum for prospective Sycoindex customers. It is provided for pre-sales review by your Legal, Privacy, and InfoSec teams. Execution requires a signed Master Services Agreement and the completion of Schedule A (Customer Information) and Schedule C (Jurisdiction-Specific Terms). Nothing in this template constitutes legal advice.

1. Parties and Effective Date

This Data Processing Addendum (the "**DPA**") forms part of the Master Services Agreement (the "**Agreement**") between **Sycoindex** ("**Processor**") and the customer identified in Schedule A ("**Controller**"). The DPA is effective on the date the Agreement is executed and applies to any Personal Data that Processor processes on behalf of Controller in connection with the Sycoindex anti-sycophancy scoring services (the "**Services**").

2. Definitions

"**Personal Data**" means any information relating to an identified or identifiable natural person, as defined in Art. 4(1) GDPR and equivalent state laws including the CCPA/CPRA, VCDPA, CPA, CTDPA, and UCPA.

"**Processing**" means any operation performed on Personal Data, whether or not by automated means, including collection, storage, transmission, scoring, and deletion.

"**Sub-processor**" means any third party engaged by Processor to Process Personal Data on Controller's behalf, as listed in Schedule B.

"**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

"**Standard Contractual Clauses**" means the modular clauses adopted by the European Commission on 4 June 2021 (Decision (EU) 2021/914), including Module Two (Controller-to-Processor).

3. Subject Matter and Duration of Processing

3.1 Subject matter. Processor will Process Personal Data solely to provide the Services — namely, to score LLM prompt/response pairs submitted by Controller against the Stanford ELEPHANT sycophancy benchmark and return a structured verdict, dimensional scoring, and honest-rewrite suggestion.

3.2 Duration. Processing continues for the term of the Agreement plus any additional period required to return or delete Personal Data as specified in Section 12.

3.3 Nature and purpose. The Processing consists of: (a) transmission of prompt/response pairs via TLS 1.3 to the Sycoindex scoring endpoint; (b) computation of a sycophancy fingerprint; (c) return of the structured result; and (d) if Controller has enabled audit logging, append-only storage of the hashed prompt/response and resulting score in the region Controller selects.

4. Categories of Data Subjects and Personal Data

Category	Description
----------	-------------

Data Subjects	End users of Controller's LLM-powered application whose prompt/response pairs are submitted to the Services
Personal Data (general)	Any Personal Data embedded in the prompt or response text submitted by Controller to the Services.
Personal Data (special)	Controller is responsible for redacting special-category data (Art. 9 GDPR) prior to submission. Processor does not
Children's Data	Controller shall not knowingly submit Personal Data of children under 13 (or the applicable local age of consent)

5. Controller Instructions

Processor shall Process Personal Data only on documented instructions from Controller. The Agreement, this DPA, and Controller's configured API usage together constitute Controller's complete and final instructions. Processor shall notify Controller promptly if, in its opinion, an instruction infringes applicable data protection law.

6. Zero Training Clause

Processor covenants and warrants that Personal Data submitted to the Services shall not be used — directly or indirectly — to train, fine-tune, evaluate, benchmark, or otherwise improve any machine learning model, whether owned by Processor, its Sub-processors, or any third party. This covenant survives termination of the Agreement and is enforceable as a material breach.

For the avoidance of doubt: Processor's Sub-processor for the scoring model (Anthropic) operates under its own zero-training-on-API-input commitment, which Processor has contractually passed through to Controller under this Section.

7. Confidentiality of Personnel

Processor shall ensure that personnel authorized to Process Personal Data are bound by confidentiality obligations, have received data protection training, and are granted access on a strict need-to-know basis. Access to production systems requires MFA, hardware-backed keys, and audit logging.

8. Security of Processing

Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including those set out in Schedule D (Technical and Organizational Measures). At a minimum these measures shall include:

- **Encryption in transit** — TLS 1.3 only; HSTS enforced; no HTTP fallback.
- **Encryption at rest** — AES-256 for audit logs; customer-selected region.
- **Access control** — RBAC with least privilege; all production access MFA-gated.
- **Logging and monitoring** — append-only audit logs; tamper-evident hash chaining; 24/7 alerting.
- **Vulnerability management** — continuous dependency scanning; 48h patch SLA for critical CVEs.
- **Incident response** — documented runbook; 72h breach notification window (Section 11).
- **SIG-Lite** — Processor's SIG-Lite self-assessment is available on request.

9. Sub-processors

Controller provides general authorization for Processor to engage the Sub-processors listed in **Schedule B**. Processor shall notify Controller at least 30 days in advance of any intended addition or replacement of a Sub-processor. Controller may object in writing within 15 days, in which case the parties shall negotiate a commercially reasonable alternative or Controller may terminate the affected Services without penalty.

Sub-processor	Purpose	Location
Anthropic, PBC	LLM scoring model (Claude Haiku 4.5)	United States
Vercel, Inc.	Edge compute and static hosting	United States / Global CDN

The current Sub-processor list is maintained at sycoindex.ai/trust/sub-processors and updated as changes occur.

10. Assistance with Data Subject Rights

Taking into account the nature of the Processing, Processor shall assist Controller by appropriate technical and organizational measures in fulfilling Controller's obligation to respond to requests for exercising Data Subject rights (access, rectification, erasure, restriction, portability, objection) under GDPR Articles 15–22 and equivalent state laws. Requests routed directly to Processor will be forwarded to Controller without delay.

11. Personal Data Breach Notification

Processor shall notify Controller without undue delay, and in any event **within 72 hours of becoming aware of a Security Incident involving Personal Data**. The notification shall include, to the extent known: (a) the nature of the breach; (b) the categories and approximate number of Data Subjects and records concerned; (c) the likely consequences; and (d) the measures taken or proposed to address the breach. Processor shall cooperate with Controller's regulatory notification obligations.

12. Return or Deletion of Personal Data

Upon termination of the Agreement, Processor shall, at Controller's election, return or delete all Personal Data within 30 days, including all copies held by Sub-processors, unless retention is required by law. Deletion shall be confirmed in writing on request. Public-endpoint data (non-Enterprise tier) is purged automatically within 24 hours of receipt.

13. Audit Rights

Processor shall make available to Controller all information reasonably necessary to demonstrate compliance with this DPA, including annual SOC 2 Type II reports (available Q3 2026 and annually thereafter), SIG-Lite responses, and the results of third-party penetration tests. Controller may conduct an on-site audit no more than once per 12 months on 30 days' written notice, at its own expense, during business hours and without disrupting Processor's operations.

14. International Transfers

To the extent Processing involves the transfer of Personal Data from the European Economic Area, United Kingdom, or Switzerland to a third country not subject to an adequacy decision, the parties agree that the Standard Contractual Clauses (Module Two, Controller-to-Processor) are incorporated by reference into this DPA and shall govern such transfers. The UK International Data Transfer Addendum and the Swiss FDPIC approach apply as relevant.

15. Liability and Indemnification

The parties' liability under this DPA is governed by the limitations and exclusions set out in the Agreement, except that no limitation shall apply to Processor's breach of the Zero Training Clause (Section 6) or fraudulent misrepresentation of Sub-processor scope (Section 9).

16. Order of Precedence

In the event of a conflict between this DPA, the Agreement, and the Standard Contractual Clauses, the order of precedence shall be: (i) the Standard Contractual Clauses; (ii) this DPA; (iii) the Agreement.

Signatures

For Controller

For Processor — Sycoindex

Signature: _____

Signature: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

SCHEDULE A — Customer Information

To be completed by Controller at execution. Fields include: legal entity name, jurisdiction of incorporation, registered address, DPO contact (if applicable), technical contact, billing contact, selected service tier, and region preference for audit log storage.

SCHEDULE B — Sub-processor List (current)

Sub-processor	Purpose	Location
Anthropic, PBC	LLM scoring model (Claude Haiku 4.5)	United States
Vercel, Inc.	Edge compute and static hosting	United States / Global CDN

Updated list maintained at sycoindex.ai/trust/sub-processors. Material changes trigger 30-day advance notice per Section 9.

SCHEDULE C — Jurisdiction-Specific Terms

To be completed based on Controller's governing jurisdiction. Includes: CCPA/CPRA contractor addendum, Virginia CDPA controller obligations, UK IDTA, Swiss FDPIC addendum, and any sector-specific terms (HIPAA BAA, FERPA, GLBA).

SCHEDULE D — Technical and Organizational Measures

Control domain	Measure
Access control	RBAC, MFA, hardware keys for production, SSO on Enterprise
Encryption	TLS 1.3 in transit; AES-256 at rest
Network	Private subnets, WAF, DDoS protection, edge rate limiting
Logging	Append-only, hash-chained, tamper-evident audit logs
Backup	Encrypted daily snapshots, 30-day retention, tested quarterly
Incident response	24/7 on-call, 72h breach notification SLA
Vulnerability management	Continuous scanning, 48h critical patch SLA
Personnel	Background checks, NDA, annual security training
Physical security	Sub-processor (Vercel) SOC 2 controls inherited
Business continuity	Multi-region failover, documented DR runbook

— END OF DPA TEMPLATE —