LEGAL & COMPLIANCE

Data Processing Agreement

Version 1.0 · Effective June 2026 · Sentinel CPO LLC

> This Data Processing Agreement (DPA) is available for counter-signature by enterprise clients and corporate sponsors who require a formal DPA for procurement or compliance purposes.

This Data Processing Agreement ("**DPA**") is entered into between **Sentinel CPO LLC**, a Connecticut limited liability company ("**Processor**", "**Sentinel CPO**"), and the entity identified as the Controller in the signature block below ("**Controller**").

This DPA forms part of, and is subject to, the Sentinel CPO Private Client Agreement (or equivalent executed agreement between the parties). In the event of a conflict between this DPA and the main agreement on matters of personal data processing, this DPA controls.

1. Definitions

Terms used but not defined in this DPA have the meaning given in the applicable data protection law or the main agreement between the parties.

- **"Personal Data"** means any information relating to an identified or identifiable natural person that is processed by Sentinel CPO on behalf of the Controller under the main agreement.
- **"Processing"** means any operation performed on Personal Data, whether automated or manual, including collection, storage, use, disclosure, and deletion.
- **"Sub-processor"** means any third party engaged by Sentinel CPO to process Personal Data on behalf of the Controller.
- **"Data Subject"** means the individual whose Personal Data is processed — in this context, the executive enrolled in the Sentinel CPO platform.
- **"Applicable Law"** means GDPR (where applicable), CCPA/CPRA (where applicable), Connecticut CUBI, Illinois BIPA (where applicable), and any other data protection law applicable to the Controller or Processor.

2. Scope and Roles

The parties acknowledge that in connection with the provision of the Sentinel CPO service:

- The Controller determines the purposes and means of processing Personal Data (specifically: engaging the platform on behalf of or with consent of the Data Subject).
- Sentinel CPO processes Personal Data as Processor, acting only on the Controller's documented instructions and as necessary to provide the service.
- In certain contexts (e.g., where Sentinel CPO processes Data Subject data to fulfill its own legal obligations), Sentinel CPO may act as an independent Controller. This DPA does not govern processing in Sentinel CPO's capacity as an independent Controller.

The subject matter, duration, nature, and purpose of processing, as well as the types of Personal Data and categories of Data Subjects, are described in **Annex I** to this DPA.

3. Processor Obligations

Sentinel CPO agrees to:

1. Process Personal Data only on documented instructions from the Controller, except where required by applicable law (in which case Sentinel CPO will notify the Controller before processing, unless prohibited).
2. Ensure that personnel authorized to process Personal Data are bound by appropriate confidentiality obligations.
3. Implement technical and organizational security measures as described in **Annex II** to protect Personal Data against unauthorized access, disclosure, alteration, or destruction.
4. Not engage sub-processors without prior authorization from the Controller. The Controller hereby provides general authorization for the sub-processors listed on the Sub-Processor Disclosure page. Sentinel CPO will provide 14 days' written notice before engaging any new sub-processor and will impose equivalent data protection obligations on all sub-processors.
5. Assist the Controller in responding to Data Subject rights requests (access, rectification, erasure, portability, restriction, objection) to the extent technically feasible and operationally practicable.
6. Notify the Controller within 72 hours of becoming aware of a Personal Data breach likely to result in risk to Data Subject rights and freedoms.
7. Provide reasonable assistance to the Controller in ensuring compliance with applicable data protection law, including data protection impact assessments and prior consultation with supervisory authorities, where required.
8. Delete or return Personal Data on termination of the main agreement, and delete existing copies except where retention is required by applicable law. Sentinel CPO's standard deletion sequence (30–90 days post-termination) satisfies this obligation.
9. Make available to the Controller all information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits and inspections, subject to reasonable advance notice and confidentiality protections.

4. Controller Obligations

The Controller agrees to:

1. Ensure that it has a lawful basis for processing Personal Data and for instructing Sentinel CPO to process on its behalf.
2. Obtain any required consents from Data Subjects, including consent to biometric data processing where required by applicable law.
3. Ensure that any Personal Data provided to Sentinel CPO is accurate and limited to what is necessary for the service.
4. Notify Sentinel CPO promptly of any Data Subject rights request received directly by the Controller that relates to data processed by Sentinel CPO.

5. International Data Transfers

Sentinel CPO processes Personal Data in the United States. Where the Controller is subject to GDPR and transfers Personal Data from the European Economic Area to Sentinel CPO in the United States, such transfer is governed by the EU Standard Contractual Clauses (SCCs) as adopted by the European Commission, which are incorporated by reference into this DPA. Sentinel CPO will execute SCCs on request.

6. Term and Termination

This DPA is effective for the duration of the main agreement and terminates automatically upon termination or expiration of the main agreement. Obligations of confidentiality and data deletion survive termination.

7. Liability and Indemnification

Each party's liability under this DPA is subject to the limitations of liability set out in the main agreement. Sentinel CPO's aggregate liability under this DPA shall not exceed the fees paid by the Controller to Sentinel CPO in the twelve months preceding the event giving rise to the claim.

8. Governing Law

This DPA is governed by the laws of the State of Connecticut, USA, without regard to conflict of law principles, except that provisions required by GDPR or other applicable data protection law shall be interpreted in accordance with the law of the relevant jurisdiction.

ANNEX I

Description of Processing Activities

ITEM	DESCRIPTION
Subject matter	Provision of AI-powered executive performance intelligence services, including biometric data integration, behavioral session analysis, and delivery of intelligence briefings.
Duration	For the term of the main agreement, plus the post-termination data deletion period (up to 90 days).
Nature of processing	Collection, storage, retrieval, analysis, structuring, and deletion of personal data for the purpose of service delivery.
Purpose of processing	To provide the Sentinel CPO executive performance intelligence service as described in the main agreement.
Types of personal data	• Identity data: name, email address (billing/auth use only) • Biometric/physiological data: HRV, sleep architecture, readiness, activity metrics, respiratory rate, temperature deviation (via Oura Health API) • Behavioral session metadata: structured performance check-in outputs (no raw audio or transcripts retained) • AI-generated intelligence output: weekly briefings and baseline assessments • Billing data: handled by Stripe as independent processor; Sentinel CPO stores Stripe customer ID and subscription status only
Categories of data subjects	Business executives and senior professionals enrolled in the Sentinel CPO platform.
Special categories	Biometric data (health-adjacent physiological metrics). Processed under explicit consent obtained at enrollment and governed by Sentinel CPO's Biometric Privacy Policy.

ANNEX II

Technical and Organizational Security Measures

CONTROL	MEASURE
Encryption at rest	AES-256 (Supabase managed PostgreSQL and object storage)
Encryption in transit	TLS 1.2 minimum on all connections. No unencrypted data paths.
Access control	Row-Level Security at the database layer; minimum necessary access principle; role-based access controls; service-role key restricted to server-side processes only
Pseudonymization	All intelligence processing conducted against pseudonymous Client ID (CPO-XXXX). Real identity compartmentalized to billing and authentication records only.
Audit logging	Administrative and PM access to Client data logged in platform audit records.
Data minimization	Voice audio not retained (processed in real-time and discarded). Biometric data retrieved as aggregated daily metrics only (no raw sensor data). Behavioral data stored as structured metadata fields only.
Sub-processor controls	All sub-processors contractually prohibited from using Client data for their own purposes or model training. Sub-processor list publicly disclosed at sub-processors.html.
Incident response	Client notification within 72 hours of confirmed breach. Incident Response Policy published at security.html.
Data deletion	Automatic deletion within 30 days of license termination. Anonymized records deleted within 90 days. Irreversible — no recovery possible post-deletion.

Infrastructure security	Hosted on Vercel (SOC 2 Type II) and Supabase (SOC 2 Type II). Dependencies monitored for CVEs.

Signatures

By signing below, the parties agree to be bound by this Data Processing Agreement.

PROCESSOR	CONTROLLER
Sentinel CPO LLC	**[Organization Name]**
State of Connecticut, USA	[Jurisdiction]
Authorized Signature	Authorized Signature
Printed Name & Title	Printed Name & Title
Date	Date

Download the PDF above, sign it, and submit a DPA Request via the contact form. Sentinel CPO will countersign and return an executed copy within 5 business days.