# DATA PROCESSING ADDENDUM

*Personal data processing under the MSA*

NOCTARA, INC. · PUPUL, INC. · MARIETTA, OHIO

EFFECTIVE 2026-05-16

# NOCTARA, INC.

*Status: DRAFT for counsel review.*

This Data Privacy Addendum ("DPA") supplements every services agreement between Noctara, Inc. ("Noctara") and any customer ("Customer") and governs the processing of personal data under those agreements.

*Effective:* [Effective Date of underlying MSA]

## 1. DEFINITIONS

- *Personal Data* has the meaning given in GDPR (Regulation (EU) 2016/679) and CCPA (California Civil Code §§1798.100 et seq.).
- *Process / Processing* means any operation performed on Personal Data, manual or automated.
- *Controller* means the entity that determines the purposes and means of Processing.
- *Processor* means the entity that Processes Personal Data on behalf of a Controller.
- *Subprocessor* means a third party engaged by Noctara to Process Personal Data.
- *Participant* means an individual who takes a Reading through Noctara's platform.

## 2. ROLES

2.1. With respect to *each Participant's Individual Data* (their answers, raw text, behavioral biometric, account profile), Noctara is the Controller. The Participant is the data subject. The Participant has direct rights against Noctara.

2.2. With respect to *aggregate signals delivered to Customer's leadership* (the Readout), Noctara is the Processor and Customer is the Controller of the resulting business analytics.

2.3. Customer is not a Controller of Individual Data and has no contractual right to access it. The architecture enforces this.

## 3. CATEGORIES OF DATA

3.1. Noctara processes the following categories of Personal Data:

- Identity data: name, email, account password hash
- Reading data: answers to six prompts, raw text input
- Behavioral biometric data: keystroke timing, edit patterns, pause distributions
- Derived data: word, mark, rhythm, force, daily lines, dumps
- Telemetry: device fingerprint, IP, language, referrer, page events

3.2. Noctara does *not* process: payment card data (handled by Stripe under Stripe's PCI compliance), photographs of faces, voice recordings beyond user-initiated voice notes, biometric identifiers as enumerated under BIPA (fingerprints, retina/iris scans, voiceprints, face/hand geometry).

## 4. LAWFUL BASIS & CONSENT

4.1. Noctara processes Personal Data on the following lawful bases:

- *Consent* for the Reading itself (Article 6(1)(a) GDPR). Each Participant clicks an explicit consent at the start of the Reading.
- *Performance of a contract* for ongoing Reading Room services (Article 6(1)(b) GDPR).

- *Legitimate interest* for security, fraud prevention, and product analytics (Article 6(1)(f) GDPR).

4.2. CCPA: Noctara honors verifiable consumer requests under §1798.100 et seq.

## 5. DATA SUBJECT RIGHTS

5.1. Noctara provides Participants with the following rights, exercisable through `privacy\@noctaracorp.com`:

- *Access* to their Individual Data (export within 30 days)
- *Rectification* of inaccurate data
- *Erasure / "Right to be forgotten"* (deletion within 30 days)
- *Restriction* of Processing
- *Portability* in a machine-readable format
- *Objection* to Processing for direct marketing (instant unsubscribe)
- *Opt-out of sale* (Noctara does not sell Personal Data; included for CCPA completeness)

5.2. Customer may not exercise these rights on behalf of Participants. Each Participant exercises rights directly with Noctara.

## 6. SUBPROCESSORS

6.1. Noctara engages the following Subprocessors as of the date of this DPA:

| Subprocessor | Role | Location | |—|—|—| | Vercel, Inc. | Hosting, edge compute | USA | | Supabase Inc. | Database (Postgres), object storage | USA | | Clerk Inc. | Authentication, MFA, session management | USA | | Stripe Inc. | Payment processing | USA | | Resend Inc. | Transactional email | USA | | Anthropic PBC | Claude API for compression and digest | USA |

6.2. Each Subprocessor is bound by its own Data Processing Addendum with Noctara.

6.3. Anthropic does not train on Customer or Participant data per Anthropic's API terms.

6.4. Noctara provides Customer with thirty (30) days' written notice before adding a new Subprocessor.

## 7. INTERNATIONAL TRANSFERS

7.1. All Subprocessors are US-hosted. EU residency is available on annual contracts.

7.2. For EU/UK Personal Data, Noctara relies on Standard Contractual Clauses (SCCs) where applicable.

## 8. SECURITY

8.1. *Encryption in transit:* TLS 1.3. HSTS preload. No HTTP fallback. 8.2. *Encryption at rest:* AES-256 for database and object storage. 8.3. *Authentication:* SSO (Google, Microsoft, Apple) via Clerk; MFA available; magic-link fallback. Noctara does not store passwords. 8.4. *Access control:* Row-level security on every table. Service-role keys held in Vercel env, rotated on key events. No production credentials in source. 8.5. *Backups:* Daily, 30-day retention, point-in-time recovery. 8.6. *Logging:* App logs 30-day retention. Access logs separated. PII excluded from logs by policy. 8.7. *Vulnerability response:* `security\@noctaracorp.com`. Acknowledgment within 1 business day. Patch SLAs follow CVSS severity.

## 9. BREACH NOTIFICATION

9.1. Noctara notifies Customer within 72 hours of confirmed material breach affecting Personal Data Customer is Controller of.

9.2. Notification includes nature of breach, categories of data affected, contact for further information, likely consequences, measures taken.

## 10. AUDIT

10.1. Customer may, on reasonable notice and at most once per calendar year, request Noctara's then-current SOC 2 attestation (in observation window as of execution; Type 1 readiness audit complete). Customer may not conduct on-site audits.

## 11. DATA DELETION ON TERMINATION

11.1. On termination of the underlying services agreement, Noctara deletes Customer's data within thirty (30) days, except:

- Aggregate, non-individual statistical artifacts retained indefinitely for benchmarks
- Backup retention per Section 8.5 (auto-purges within 30 days post-termination)
- Records required to be retained by law

11.2. Participant data is governed by the individual Participant's account, not Customer's termination. Participants retain their accounts and data unless they themselves delete.

## 12. LIABILITY & INDEMNIFICATION

12.1. Each Party's liability under this DPA is governed by the underlying services agreement, including any limitation of liability.

12.2. Noctara indemnifies Customer for fines or damages levied against Customer by a regulator due to Noctara's material breach of this DPA.

## 13. GOVERNING LAW

13.1. Delaware, USA, except where overridden by mandatory data protection law of the data subject's jurisdiction.

---

## COUNSEL REVIEW CHECKLIST

- [ ] BIPA carve-out language in Section 3.2 is defensible
- [ ] Consent language at Section 4.1 ties correctly to in-product consent UI
- [ ] Subprocessor list at Section 6 matches actual stack
- [ ] SCC reference in Section 7 should be specific (Module 2 Controller-to-Processor for participant data; Module 3 Processor-to-Processor for some subprocessor relationships)
- [ ] Breach notification window of 72 hours is GDPR-aligned but should be hardcoded in MSA too
- [ ] Section 11 retention policy needs to align with underlying MSA termination clause
- [ ] Confirm Cole's `privacy\@noctaracorp.com`, `security\@noctaracorp.com`, `legal\@noctaracorp.com` aliases are routed

END OF DOCUMENT . NOCTARA, INC.