TEMPLATE · V1.0 · 2026

Data Processing Addendum — template

This template is provided as a starting point for institutional procurement review. It is not executed until both parties countersign. Institutional counsel must review and mark up. Not legal advice. Final executable version available on request from support@dissertationeditingcenter.com.

1. Parties & scope

This addendum supplements the Master Services Agreement between Dissertation Editing Center ("Processor") and the contracting institution ("Controller") and governs the Processor's handling of Personal Data on the Controller's behalf.

2. Categories of data & data subjects

- Manuscript files uploaded by Authorized Users (doctoral candidates, faculty)
- Authentication identifiers (institutional email, SSO subject claim)
- Review metadata (timestamps, agent invocation logs, readiness scores)
- No payment data (Stripe is a separate processor on the Controller's behalf)

3. Purpose

Processor will process Personal Data solely to (i) execute the chapter-grade review workflow described in the MSA, (ii) maintain a per-job audit log, and (iii) provide program-level analytics to the Controller. Processor will not use Personal Data for training, profiling, or marketing.

4. Sub-processors

The current sub-processor list is maintained at dissertationeditingcenter.com/security/subprocessors and includes: Anthropic PBC (US, no-train), Supabase Inc. (US-region Postgres), Upstash Inc. (US-region Redis), Vercel Inc. (US-region edge), Resend Inc. (US transactional email). Material changes communicated to Controller at least 30 days in advance.

5. Security measures

- TLS 1.3 in transit; AES-256 at rest in single-tenant US-region Postgres
- SSO (SAML/OIDC) and SCIM provisioning available on Enterprise tier
- Role-based access controls; least-privilege production access
- SOC 2 Type II audit in progress (target Q4 2026)
- FERPA-aware controls; retention configurable per program

6. Data subject rights

Processor will assist Controller in responding to data subject requests for access, rectification, erasure, restriction, and portability within five (5) business days of a documented request from the Controller.

7. Retention & deletion

Manuscript bytes are retained per the Controller-selected program policy. Hard deletion is honoured on demand within twenty-four (24) hours of an authorized request from the Controller or the data subject, with email confirmation. On termination of the MSA, all Personal Data will be deleted within ninety (90) days.

8. Breach notification

Processor will notify Controller within seventy-two (72) hours of becoming aware of a Personal Data Breach affecting Controller's data. Notice will include scope, impact, containment status, and remediation timeline.

9. International transfers

Personal Data is stored and processed in the United States. For Controllers with EU data subjects, Standard Contractual Clauses (Module 2, Controller-to-Processor) are incorporated by reference and available as Annex A on request.

10. Audit rights

On reasonable notice and no more than once per twelve (12) months, Controller may request a copy of the most recent SOC 2 Type II attestation (when issued) and a written summary of the Processor's information security program. On-site audits available for Enterprise customers under separate engagement.

Signatures

Controller signatory: _____ Date: _____

Processor signatory: _____ Date: _____