Data Processing Addendum

Version 2026-07-13 · Last updated July 13, 2026. This is a good-faith template and is not legal advice; have counsel review before signing.

This Data Processing Addendum ("DPA") supplements the Terms of Service or other written agreement (the "Agreement") between Epitaph LLC ("Processor," "we," or "us"), operator of Scribe, and the customer identified below ("Controller," "Customer," or "you"). It governs the processing of Personal Data that we perform on your behalf when you use the Service. Where this DPA conflicts with the Agreement on the subject of data protection, this DPA controls.

1. The parties

Processor: Epitaph LLC, [COMPANY ADDRESS — Epitaph LLC, Pennsylvania — TO BE SUPPLIED]. Notices: legal@epitaph.llc; privacy matters: privacy@epitaph.llc.

Controller (Customer): _____

Address: _____ Contact: _____

Signed: _____ Name/Title: _____ Date: _____

2. Definitions

"Personal Data," "processing," "controller," "processor," and "personal data breach" have the meanings given under applicable U.S. data-protection law. "Customer Data" means data you or your users submit to the Service, including injury and illness records and related attachments. "Subprocessor" means a third party engaged by us to process Customer Data.

3. Roles and scope

You are the controller (or business) of Customer Data and we are your processor (or service provider). We process Customer Data only to provide, secure, and maintain the Service and on your documented instructions, which the Agreement, this DPA, and your use of the Service constitute. We do not sell Customer Data, do not share it for cross-context behavioral advertising, and do not retain, use, or disclose it for any purpose other than performing the Service. The Service is provided from, and Customer Data is processed and stored in, the United States.

Subject matter: provision of the Service. Duration: the term of the Agreement plus the retention and deletion periods below. Nature and purpose: hosting and processing of workplace safety, injury, and illness recordkeeping data. Categories of data subjects: your employees, contractors, and personnel. Categories of Personal Data: identity and contact data; role and organizational data; injury and illness details including limited health information (e.g., OSHA Form 301 fields such as body part, treatment, and treating facility); incident narratives; photos and attachments; and usage data.

4. Your responsibilities

You are responsible for the accuracy, quality, and legality of Customer Data and for having a lawful basis and any required notices or consents to collect it and have us process it. Your instructions must comply with applicable law. You remain solely responsible for your OSHA recordkeeping and compliance determinations, as described in the Agreement.

5. Confidentiality

We treat Customer Data as confidential and ensure that personnel authorized to process it are bound by appropriate confidentiality obligations and access it only as needed to provide the Service.

6. Security measures (Annex)

We implement and maintain technical and organizational measures appropriate to the risk, including at least the following:

- Tenant isolation via PostgreSQL row-level security, scoping access to the caller's organization on every query.
- Role-based access controls and PII walls limiting who can view injury and illness detail; support for anonymous safety reporting with sealed reporter identity.
- Organization-enforceable multi-factor authentication (TOTP); passwords stored hashed and screened against known-breached-password lists.
- Encryption of data in transit (HTTPS/HSTS) and at rest.
- Private storage buckets served only via short-lived, server-mediated signed URLs.
- Append-only audit logging of sensitive actions; immutable, amendment-tracked injury records; signed outbound webhooks.

7. Subprocessors

You authorize us to engage the Subprocessors listed below to process Customer Data to provide the Service. Each Subprocessor is bound by a written contract imposing data-protection obligations no less protective than those in this DPA, and we remain responsible for their performance. We will maintain a current list (also published at /legal/subprocessors) and give you a reasonable opportunity to object to a new Subprocessor before it begins processing, as described in the Agreement.

- Supabase, Inc. — Database, authentication, and file/attachment storage (United States).
- Vercel, Inc. — Application hosting and content delivery (United States).
- Stripe, Inc. — Subscription billing and payment processing (United States).
- Resend (Plus Five Five, Inc.) — Transactional email delivery (invitations, password resets, alert digests) (United States).
- Functional Software, Inc. (Sentry) — Error monitoring and diagnostics (United States).
- Anthropic, PBC — AI-assisted safety summaries — engaged only when an organization on a plan with AI features generates a summary. The payload is aggregated/de-identified safety metrics; individual injury PII is not sent. (United States).

8. Personal data breach notification

We will notify you of a personal data breach affecting your Customer Data without undue delay after becoming aware of it, targeting notification within seventy-two (72) hours. The notice will describe, to the extent known, the nature of the breach, the categories and approximate number of data subjects and records affected, likely consequences, and the measures taken or proposed. We will provide reasonable cooperation to help you meet your own notification obligations. Notices will be sent to your designated contact; keep it current at privacy@epitaph.llc.

9. Assistance

Taking into account the nature of the processing and the information available to us, we will provide reasonable assistance to help you respond to data-subject requests and to meet your security, breach-notification, and (where applicable) data-protection-assessment obligations. Requests about the content of injury or incident records are directed to you as controller; we assist as your processor.

10. Audits

On reasonable written request, no more than once per year (unless required by a regulator or following a breach), we will make available information reasonably necessary to demonstrate compliance with this DPA,

including relevant documentation about our security measures and Subprocessors, subject to confidentiality.

11. Return and deletion

On termination of the Agreement, you may export Customer Data using the Service's tools for thirty (30) days, after which we will delete Customer Data in the ordinary course, except where retention is required by law. Because injury records may be subject to multi-year OSHA retention duties, you are responsible for exporting and retaining the records you must keep. Residual copies in backups cycle out over a limited period.

12. International transfers

The Service is U.S.-only and Customer Data is processed in the United States. This DPA does not contemplate transfers subject to the GDPR or other non-U.S. transfer mechanisms.

13. Liability and term

Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement. This DPA takes effect when both parties accept the Agreement (or on the signature date above) and remains in effect for as long as we process Customer Data. It is governed by the laws of the Commonwealth of Pennsylvania, consistent with the Agreement.

To execute this DPA, complete the party details in Section 1 and return a signed copy to legal@epitaph.llc.