StoryAudit

Data Processing Addendum & Subprocessor List (Draft)

For legal, procurement, and security review · Prepared July 22, 2026

This document describes StoryAudit's actual data-handling practices in standard DPA format, so a legal or procurement reviewer can evaluate them directly. It has not been reviewed by an attorney and is not represented as an executed or binding agreement. If your organization requires a signed DPA, email support@storyaudit.app to start that process — the terms below are the accurate starting point for that conversation, not a substitute for it.

1. Parties

This Data Processing Addendum ("DPA") is intended to form part of the agreement between the customer ("Customer," the organization or individual with a StoryAudit subscription) and the operator of StoryAudit ("StoryAudit," "we," "us") — Eric Allen, an independent software developer, operating as a sole proprietor — governing StoryAudit's processing of personal data in connection with the StoryAudit service.

2. Roles of the parties

For personal data relating to Customer's own account holders and team members (name, email address, authentication and billing metadata), StoryAudit acts as a data Processor and Customer acts as the data Controller. **StoryAudit does not process the content of Customer's course files (.story files) at all**: those files, and everything the app reads out of them (slide text, quiz answers, media, transcripts, variables), are parsed entirely client-side, in the Customer's own browser, using the File API, and are never transmitted to StoryAudit's servers in any form. Accordingly, StoryAudit has no processor relationship with respect to course-file content, because no such processing by StoryAudit occurs.

3. Subject matter, nature, and duration of processing

Subject matter: provision of the StoryAudit service, including account creation, authentication, and subscription billing.
Nature and purpose: identity verification, session management, subscription and payment processing, and standard hosting operation (serving the application over HTTPS).
Duration: for as long as Customer maintains an active StoryAudit account, plus a reasonable period thereafter for legal, tax, and dispute-resolution purposes, as described in StoryAudit's Privacy Policy (storyaudit.app/privacy.html).

4. Categories of data subjects and personal data

Data subjects: Customer's authorized users (individual account holders / team members).
Categories of personal data: name, email address, authentication credentials/tokens, IP address and browser type (standard access logs), and subscription/billing status. Full payment card numbers are never received or stored by StoryAudit — card details are collected and processed directly by Clerk's billing infrastructure (see Section 5).
Special categories of data: none knowingly processed by StoryAudit. Course file content — which may incidentally include personal data if a Customer's own course text, media, or scenario content contains it — is never transmitted to or processed by StoryAudit's infrastructure at all, per Section 2.

5. Subprocessors

Customer authorizes StoryAudit to engage the subprocessors listed below as of the date of this document. StoryAudit will update this list when a subprocessor is added or removed.

Subprocessor	Purpose	Data involved	Location
Clerk (Clerk, Inc.)	Authentication, session management, subscription & payment billing	Name, email, authentication tokens, billing/subscription status, payment card data (collected directly by Clerk)	United States — see Clerk's own compliance documentation
Vercel (Vercel Inc.)	Application hosting; edge/serverless functions for the authentication gate	Standard HTTP request/access logs (IP address, browser type)	United States — see Vercel's own compliance documentation

Google Fonts (Google LLC)	Web font delivery	IP address, browser type (standard font-request headers); no account data shared	Global CDN — see Google's own documentation

None of the above subprocessors receive, process, or store the content of a Customer's .story course files, generated reports, or exports — that content is never transmitted off the Customer's own device in the first place.

6. Security measures

- Course file content is never uploaded to or stored on StoryAudit's servers, which eliminates server-side data-at-rest risk for that entire category of data.
- All traffic is served over HTTPS/TLS.
- Authentication and billing are delegated to Clerk, which states SOC 2 Type II certification and GDPR/CCPA-aligned practices in its own published compliance documentation.
- StoryAudit does not use third-party analytics or advertising trackers.

See also StoryAudit's Security & Architecture Overview (storyaudit.app/assets/storyaudit-security-overview.pdf) for additional detail on the application's architecture.

7. Assistance with data subject requests

StoryAudit will provide reasonable assistance to Customer in responding to verified data subject requests (access, correction, deletion) concerning the account-level personal data described in Section 4, to the extent StoryAudit holds that data. Requests can be directed to support@storyaudit.app. Because course file content is never held by StoryAudit, no such assistance is applicable to that category of data.

8. Security incident notification

StoryAudit will notify Customer without undue delay upon becoming aware of a confirmed security incident affecting Customer's personal data held by StoryAudit or its subprocessors, and will provide information reasonably available at the time to help Customer meet its own notification obligations.

9. International data transfers

StoryAudit's subprocessors (Clerk, Vercel) are United States-based. Customer should consult those providers' own published compliance documentation for details on cross-border transfer safeguards relevant to Customer's jurisdiction.

10. Deletion / return of data

Course file content: not applicable — never held by StoryAudit in the first place. Account-level data: retained per Section 3 and StoryAudit's Privacy Policy; deletion requests are handled per Section 7.

11. Term

This DPA, once executed, remains in effect for as long as the underlying StoryAudit subscription agreement is in effect.

12. Governing law

This DPA is governed by the laws of the State of Ohio, USA, without regard to its conflict-of-laws principles, consistent with the governing law provision in StoryAudit's Terms of Use (storyaudit.app/terms.html).
