

Appendix A | Data handling

SENSATE ORIGIN DESIGN SERVICES - FZCO

For IT review. Technical disclosure, not a certification or a contractual SLA. Source: the current /security disclosure. No customer records are included.

Legible stores the public pages it reads, the business details and files you add, research results, drafts and generated media. If you use Customers or connect a form, it also stores contact details, messages, consent records and activity. Use public business information for a pilot. Do not upload passwords, payment card details or sensitive personal records as content.

Storage and access

Legible runs on Railway. Workspace files are kept on a persistent data volume, separated by site. The production region code checked for this review was sfo. This is not a promise that all processing stays in that region: connected services and AI providers process data separately.

The workspace's account and authorised Sensate operators can access it. Server routes check site access before returning private workspace data. Operator access is for running and supporting the service; this is not end-to-end encryption that prevents Sensate from reading your data. Shared reports and published deck links can be read by people who hold those links.

The production service uses HTTPS. Session cookies are HttpOnly, Secure in production and SameSite=Lax, with a 12-hour lifetime; sessions are signed.

What is encrypted

Platform credentials and connected-service tokens held in the credential vault use AES-256-GCM encryption. Customer names, email addresses, phone numbers, company, role, notes, messages and private event text are encrypted by the application. Public-page records, uploaded decks, drafts, generated files and all record metadata are not all encrypted by the application. We do not claim that every stored file has the same protection as a credential.

Export, retention and deletion

Your workspace's Connections > Your data panel shows saved-record counts and links to the available customer CSV and latest client report. These are partial exports: they are not a complete archive of every workspace file. Uploaded decks and generated outputs remain available through their own screens.

Workspace records generally remain until removed. We have not verified a single automatic deletion period covering every kind of workspace data. The Privacy Policy describes deleting audit data within 30 days after a subscription ends; automation that enforces that deadline has not been verified in this technical review. Contact us to confirm completion of a deletion request. Removing a site from an operator dashboard moves it to recoverable trash; it is not permanent erasure. Eligible account owners can use Settings > Profile & appearance > Close your account to delete their workspace data. Paid accounts must cancel first. Payment, support and third-party records are handled separately; closing a workspace does not erase them everywhere. For an export or deletion request, contact hello@sensate.design (mailto:hello@sensate.design).

Limits of this assurance

No automated volume backups yet; the data volume is b0778ac2 on Railway; restore = redeploy from git + this volume.

Railway's Backups screen showed no snapshots when checked on 14 October 2026. This recovery path depends on the existing volume surviving; it cannot recover a lost volume. A successful recovery exercise, console MFA and independent penetration-test results have not been verified. We do not claim SOC 2 or ISO 27001 certification. Ask us to resolve a requirement before using Legible for data that depends on it.

Report a suspected vulnerability privately to hello@sensate.design (mailto:hello@sensate.design?subject=Legible%20security%20report). Include the affected URL and reproduction steps, without sending credentials or other people's personal data.