

Security & Data Protection Overview

How GleanMark protects the confidential work of trademark practices.

This sheet is written for security and IT reviewers: plain statements, real numbers, and nothing aspirational — we publish the posture we have, not the one we plan to have.

THE COMMITMENTS

Never used to train AI

Our business agreements with every AI provider we use prohibit training their models on customer content. Every provider that processes customer data is disclosed at gleanmark.com/subprocessors.

Isolated at the database layer

Each customer workspace is separated with row-level security — access rules enforced inside the database on every query, not only in application code. One customer can never read another's data.

Deletable by the customer

Account deletion is self-serve and permanent: billing is cancelled safely, then data is actually purged. It is not a hidden "deactivated" flag.

US data residency

The production database and document storage run in the AWS US East (N. Virginia) region. Customer data does not leave US data centers at rest.

ARCHITECTURE

- **Tenant isolation, continuously checked.** Row-level security plus per-workspace scoping, recurring internal security audits (most recently July and August 2026), and a daily job that alerts us if any table appears with row-level security switched off while still reachable by the public API key. It has run every day since 15 August 2026 and has never found an exposed table.
- **Encryption.** All traffic is encrypted in transit over TLS; data is encrypted at rest by our cloud infrastructure provider.
- **Authentication.** Sign-in via Google, Microsoft, or one-time email codes. No GleanMark account has a password, so there is nothing to phish or reuse from another breach.
- **Session controls.** Firm administrators can enforce automatic sign-out after a chosen period of inactivity (15 minutes to 24 hours, with a one-minute warning) and an optional maximum session length for every member. Sensitive actions (inviting or removing members, changing roles, transferring ownership, changing the session policy, exporting or deleting an account) require a fresh one-time code; admins can sign any member out of every device; every user can see the devices signed in to their account and sign out any one of them, or all others with one click.
- **Role-based access.** Five workspace roles (owner, admin, staff, contractor, client) gate 19 distinct permissions covering members, billing, portfolios, and client access — enforced in the application and again in the database.
- **Document storage.** Documents uploaded to a matter live in a private bucket, reachable only through short-lived signed links generated for authorized users. Two deliberate exceptions: filing-wizard images (specimens and design marks) and firm logos sit at unguessable public URLs so they render in the product and in filings.

DATA LIFECYCLE & RETENTION

CONTROL	BEHAVIOR
AI diagnostic logs	Raw AI prompts and outputs retained for troubleshooting are automatically deleted after 90 days by a scheduled job. The Privacy Policy states the same ceiling.
Deleted AI chats	24-hour undo window, then permanently purged by a daily job — attachments included.
Account deletion	Self-serve and permanent from Settings. A reversible archive option exists separately.
Full data export	One click in Settings downloads everything GleanMark holds about the user as JSON (optionally with uploaded files as a zip). Generated in the browser under the user's own permissions; never stored on GleanMark servers.
Per-feature export	Portfolios, deadlines, and alerts export to CSV, with calendar .ics for deadlines. Clearance reports export to Excel, PDF, and Word; AI drafts to PDF and Word.

AI DATA HANDLING

- Outside AI providers are used for search analysis, drafting, and the Markus assistant. All are disclosed at gleanmark.com/subprocessors.
- The no-training commitment is contractual: it is written into our business agreements with each provider, and we hold vendors to it.
- We do not claim AI output is always accurate. Nothing in GleanMark replaces an attorney's own judgment — the duty to verify is non-delegable.

COMPLIANCE STATUS

Stated plainly: GleanMark does not hold SOC 2 or ISO 27001 certification today, and we do not claim otherwise. Our cloud infrastructure providers hold their own certifications. Our privacy program includes a public privacy policy, a public subprocessors list, cookie-consent controls, self-serve permanent deletion, and enforced retention limits. A data processing addendum is available on request.

DOCUMENTS & CONTACT

RESOURCE	LOCATION
Security overview	gleanmark.com/security
Privacy Policy	gleanmark.com/privacy
Subprocessor list	gleanmark.com/subprocessors
Terms of Service	gleanmark.com/terms
Security questionnaires	privacy@gleanmark.com — we answer them directly