Vendor Security Summary

For compliance officers and IT reviewers checking how ModelLayer protects their firm's data. It describes the security controls in place today and what stays with your firm.

Key Points

- The app, API, database, file storage, and AI summaries run on Cloudflare. Data is encrypted in transit, and stored data is encrypted at rest.
- Clients and reports are visible only to your firm's signed-in users. An automated test tries every data route from another firm.
- Sign-in needs a verified email address. Two-step sign-in with an authenticator app is available on every account and required for admin accounts.
- Card payments happen on Stripe's own checkout page. Card numbers never reach ModelLayer.
- Client names, dates of birth, and contact details are designed to be removed before any AI request. Every account can turn AI off.
- Account deletion runs on the server and removes clients, notes, reports, and firm records in one step.
- We notify your firm within 72 hours of becoming aware of an incident affecting your data.
- ModelLayer does not yet hold a SOC 2 report. Our hosting, payment, and email providers hold their own.

1 Data and Hosting

Area	How ModelLayer Handles It
Where Data Lives	• The app, API, database, and file storage run on Cloudflare. • The database and file storage were created in Cloudflare's Eastern North America location. Cloudflare treats the location as a placement preference, without a residency guarantee. Other requests, including AI requests, are handled on Cloudflare's network.
Encryption	• The app talks to the API over HTTPS (TLS), and the site tells browsers to use HTTPS only (HSTS, one year). • Cloudflare encrypts the database and file storage at rest with AES-256. • Password-protected PDF reports use AES-256 encryption.
Separation Between Firms	• All firms' data is held in one shared database. The server checks every request against the signed-in user: clients and reports are visible only to that firm's signed-in users, and notes only to the person who wrote them. • An automated test signs up accounts in separate firms and tries every route that holds client, report, note, or account data against another firm's records. Every attempt must be refused, and the test fails if a new route is added without being covered. • Beyond the firm's own users, access is limited to ModelLayer personnel and providers who need it to run, support, and secure the service. • Signed-in responses are marked private and no-store, so browsers and caches do not keep a copy.
Backups and Recovery	• The database keeps a continuous restore history for 30 days and can be restored to any minute in that window. • Both recovery paths, a point-in-time restore and a restore from an export, were last tested on October 6, 2026, on a throwaway copy.

2 Sign-In and Account Protection

Area	How ModelLayer Handles It
Accounts and Passwords	• A new account cannot sign in until its email address is verified. Following the verification link does not sign anyone in. • Passwords must be at least 8 characters. They are hashed with scrypt and never stored in plain text.
Sessions and Resets	• Sessions are held on the server. The browser keeps only a session token, in a cookie that is sent over HTTPS only and cannot be read by page scripts. Sessions expire after 30 days without use. • Password reset links expire after one hour and work once. Completing a reset signs the account out everywhere.
Two-Step Sign-In	• Available on every account and required for admin accounts: a code from an authenticator app after the password or after Google or Microsoft sign-in, with ten backup codes. The authenticator secret and backup codes are stored encrypted. • Five wrong codes end that sign-in. Ten wrong codes in an hour stop code entry on the account for the rest of the hour. • Turning two-step off needs the password or a current code, and forgets every trusted device.
Limits on Guessing	• Sign-in, sign-up, password reset, and two-step requests are rate limited per network address and counted in the database, for example 10 password attempts a minute. • Verification and reset emails are capped per account and per network address each hour.
Administrative Access	• Limited to a short list of verified email addresses set in the server's configuration, and each admin account must have two-step sign-in turned on. There is no path to admin access through sign-up.
Browser Protections	• Browsers can call the API only from ModelLayer's own site, and the API refuses changes sent from other websites. Other websites cannot show ModelLayer inside a frame. • Private Mode locks the screen to one client and hides the client list, for use in front of a client. It changes what the screen shows and does not change who can access data.

3 AI, Payments, and Email

Area	How ModelLayer Handles It
What the AI Receives	• The model's computed figures, the platform's instructions, any custom prompt, and in Chat the recent conversation. • Before any request leaves our servers, the names, dates of birth, emails, and phone numbers on the client record are designed to be removed, including from what the advisor types. Email addresses and phone numbers in typed text are masked whether or not a client is open. The AI is told not to invent client names or details. • Other identifiers, such as a child's name, are not caught, so advisors should not type them into prompts or Chat.
Where the AI Runs	• Google's Gemma 4 through Cloudflare Workers AI, inside the Cloudflare account that runs ModelLayer. Cloudflare states that it does not use customer content to train AI models. • The usage record we keep (account, time, tokens, cost) holds no request or reply text. A new summary is kept on our servers until the advisor puts it on a report or discards it, then removed about a day later. An unused one is removed after 30 days. On a report, it is kept with the saved report. Chat conversations are not stored on our servers.
AI Off Switch	• Every account can turn AI off in Settings. The server then refuses AI requests for that account, so nothing is sent.
Payments	• Pro is bought on Stripe's own checkout page. Card numbers go to Stripe and never reach ModelLayer's servers. • ModelLayer stores Stripe's references for the customer, checkout, and subscription, and the subscription status, never card details. A plan changes only when Stripe's signed webhook confirms it. • Stripe is certified as a PCI Service Provider Level 1.
Email	• Account emails, and reports an advisor sends, go out through Resend from ModelLayer's verified domain, which publishes SPF and DKIM records. • Emailed PDFs are built on the server. Each account can email up to 40 reports in any 24 hours. • Resend keeps copies of sent emails under its own retention settings. Account deletion does not remove them.

4 Deletion, Incidents, and Providers

Area	How ModelLayer Handles It
Deleting Data	• Advisors can delete clients, notes, and their own saved reports at any time. A client that holds a colleague's saved reports can be deleted once those are moved or deleted. • An account owner can delete the account in Settings once any subscription is cancelled, its paid period has ended, and no subscription is left unpaid. The server removes the firm's clients with their notes and reports, the account's own records, and the firm's records in one step, then the firm's logo files, and emails a confirmation. • Anonymous usage counts and a minimal record of Terms acceptance, with no name or IP address, are kept. Stripe keeps its own billing records, and Resend its copies of sent emails. Backups roll off within 30 days.
Incident Notice	• Affected firms are notified as soon as possible, and no later than 72 hours after we become aware of an incident affecting their data. • A written incident response plan is drafted and awaiting adoption.
Independent Review	• ModelLayer does not yet hold a SOC 2 report. Our providers Cloudflare, Stripe, and Resend maintain their own SOC 2 Type II reports.
Subprocessors	• Cloudflare (hosting, storage, AI, web analytics), Stripe (payments), Resend (email), Google Workspace (ModelLayer's own email), GetTerms (cookie consent), Google Analytics (website and app analytics after cookie consent, no client data), Premier Studio LLC (ModelLayer's developer), and Google or Microsoft only when a user chooses them to sign in. The full list is in the DPA.

What Stays With Your Firm

- Deciding who at your firm uses ModelLayer, and removing team members who leave.
- Turning on two-step sign-in and keeping passwords private.
- Keeping Social Security numbers, account numbers, and identifiers other than the client record out of notes, prompts, and Chat.
- Sending PDF passwords to clients separately from the report.
- Keeping your own copies of reports and client communications.
- Notifying your own clients and regulators after an incident, where required.

5 For Your Vendor File

Available on Request

- Data Processing Addendum: processing, subprocessors, security, breach notice, and deletion.
- A summary of our incident response plan.
- Answers to your firm's security or vendor due diligence questionnaire.

Related Documents

- Compliance Handout (Vendor Compliance Summary)
- Terms and Conditions of Sale: modellayer.app/terms
- Privacy Policy: modellayer.app/privacy
- Acceptable Use Policy: modellayer.app/acceptable-use

Security and Questionnaires: security@modellayer.app
General: team@modellayer.app

ModelLayer LLC (Ohio). This summary describes the platform as of November 2026 and may change. The Terms and Conditions of Sale, the Privacy Policy, and any signed Data Processing Addendum control. It is not legal or compliance advice.