



StratIQ AI Privacy Policy

Last Updated: October 11, 2026

StratIQ AI, LLC

1095 Dollar Street, West Linn, OR 97068

info@stratiquai.com · stratiquai.com

Contents

1	Summary	3
2	Our role: customers and their data	3
3	Information we collect	4
4	How we use information	5
5	Where your data is stored	6
6	How we share information	6
7	AI models and model providers	7
8	Security	7
9	Data retention and deletion	8
10	Your choices	9
11	U.S. state privacy rights (including California)	9
12	EEA, UK, and Swiss users (GDPR)	10
13	Children	10
14	Cookies and similar technologies	10
15	Third-party services and links	10
16	Changes to this policy	11
17	Contact us	11

This Privacy Policy explains how StratIQAI, an LLC organized under the laws of Oregon ("StratIQAI," "we," "us," or "our"), collects, uses, shares, and protects personal information. It applies to everyone who interacts with StratIQAI, including website visitors, people who request information, trials, or audits, trial users, paying customers, users of firm or organization accounts, and StratIQSphere community members.

It covers:

- our website at <https://www.stratiqai.com> (the "Site");
- the StratIQAI application, available at our app domain, and our AI agents, workflows, and integrations (the "App");
- StratIQSphere, our community hosted on Circle; and
- our communications, support, and events.

Together, these are the "Service." Read this policy together with our Terms of Service. If your organization has signed an order form, master services agreement (MSA), or Data Processing Agreement (DPA) with us, that agreement controls where it conflicts with this policy. Our [StratIQAI Security Whitepaper](#) describes our security controls in more detail.

1. Summary

- **A dedicated environment for every customer.** Each customer's App, working data, and agents run in a dedicated, hardware-isolated virtual machine with its own encrypted volume, private network, and encryption key.
- **Your data is yours.** You keep ownership of what you provide, and we process it only to operate your agents and provide the Service.
- **We don't sell personal information.**
- **AI model calls.** To generate responses, agents send requests to the AI model selected, through our AI model gateway, OpenRouter. Model providers have their own data practices (see Section 7).
- **You control your connections.** Agents access your CRM, email, calendar, documents, and deal tools only after they are connected. Connections start read-only, and disconnecting a tool deletes its stored credentials.
- **People approve risky actions.** By default, agents must get a person's approval before running actions flagged as risky, and a fixed set of dangerous operations is always refused.
- **Set retention.** Conversations and agent activity are deleted automatically after a set period that depends on your plan (see Section 9).

2. Our role: customers and their data

StratIQAI is a business-to-business service for commercial real estate and finance professionals.

- **Customer Data.** Files, conversations, connected-tool data, agent memory, and agent outputs in the App ("Customer Data") may include personal information about other people, such as clients, prospects, tenants, owners, investors, and other contacts. We process Customer Data on behalf of our

customer (the individual subscriber or the firm or organization that holds the account) and only according to its instructions. For Customer Data, we act as a "service provider" or "processor," and the customer acts as the "business" or "controller."

- **Firm and organization accounts.** If you use the App through an account provided by your employer or firm, that organization is our customer and controls the Customer Data in its account, which may include your conversations and files. Each organization has owner, admin, and member roles. Billing, settings, team membership, agent hiring, and connected-system changes are limited to the roles that need them. Owners and admins may be able to manage your access and the organization's data. Your organization's own policies may also apply.
- **Our own data.** For information about website visitors, account holders, trial requests, billing, support, and community members, we act as the "business" or "controller."

If your information is contained in a StratiqAI customer's Customer Data, please contact that customer directly with privacy requests. We will help our customers respond as required by law.

Customers that need contractual data protection terms may request our DPA: info@stratiqai.com.

3. Information we collect

3.1 Information you provide

- **Account information.** Name, email address, and password, or basic profile information from a single sign-on provider (such as Google) if you sign in that way. For organization accounts, this also includes your organization, membership, role, and invitations.
- **Content you upload.** Files such as PDFs, Word documents, spreadsheets, and images (for example, offering memoranda, rent rolls, leases, underwriting packs, and LOIs).
- **Conversations and instructions.** Messages and instructions you give agents, team chat, tasks, and activity, the workflows, scheduled jobs, and proactive tasks you set up, and the outputs agents produce.
- **Billing information.** For paid plans: billing contact, plan, subscription and transaction history, and AI credit balance and usage. Payments are handled through our payment processor's hosted checkout and billing portal. Card numbers never touch StratiqAI systems.
- **Feedback and support.** Ratings of agent responses, bug reports (including any screenshots you attach), support requests, and emails.
- **Inquiries.** Information you submit when you request a trial, AI audit, demo, or enterprise briefing, or otherwise contact us (such as name, email, company, and details of your request).
- **Community content.** Your StratiqSphere profile, posts, and comments.

3.2 Information from tools you connect

When you connect a third-party tool (such as Microsoft 365, Google Workspace, a CRM, document storage, or a data provider), you authorize your agents to access that tool's data to do the work you request.

Depending on the tool and the access granted, this may include contacts, notes, activity history, pipeline and deal records, email messages, calendar events, and documents. The scope of access depends on what each tool's API supports.

- **Read-only by default.** Connections start read-only. Writing to an outside system must be turned on for that connection, and each agent must also be given write access individually. Otherwise, write tools are not offered to that agent at all.
- **OAuth connections.** The provider's sign-in starts and finishes at our central control plane, because providers require a fixed return address. Your environment then collects the encrypted connection bundle, stores it in its own encrypted vault, and confirms it has done so. The control plane then deletes its temporary copy. Refreshed tokens are stored only in your environment.
- **API key connections.** API keys are entered in a secure form separate from chat and go straight to your environment. We check the key with the vendor and store it only in your environment's encrypted vault. The key is never returned to the browser, written to logs, or sent to the control plane. The control plane only learns that the connection exists and whether it is healthy.

StratiqAI's use and transfer of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

3.3 Information collected automatically

When you use the Service, we and our service providers may automatically collect technical information, such as IP address, browser and device type, pages viewed, timestamps, and activity and security logs, to operate, secure, and troubleshoot the Service. Our logs automatically redact cookies, API keys, credential values, encryption keys, and payment secrets. By default, the App's security policy allows only first-party scripts.

3.4 Information from other sources

StratiqAI does not obtain information about prospects or users from third parties.

4. How we use information

We use information to:

- provide, operate, and maintain the Service, including running agents and the tasks, workflows, scheduled jobs, and proactive tasks you set up;
- provision, monitor, back up, and restore each customer's dedicated environment;
- send requests to the AI model selected so agents can generate responses;
- connect to and act within third-party tools you authorize, at your direction;
- let agents keep long-term memory and skills within your environment so they can adapt to how you work (when enabled, changes to an agent's memory or skills require approval);

- manage accounts, organizations, trials, subscriptions, billing, and AI credit balances;
- provide support, investigate bug reports, and follow up on fixes;
- improve the Service, using feedback, ratings, and usage information;
- communicate with you about your account, product updates, release notes, and, where permitted, marketing (you can opt out of marketing at any time);
- protect the security and integrity of the Service, prevent fraud and abuse, and enforce our Terms of Service; and
- comply with legal obligations.

Customer Data is used only to operate your agents. We process Customer Data only to operate your agents and provide the Service to you. We do not use Customer Data to train AI models. See Section 7 for third-party model providers.

We do not sell personal information or share it for cross-context behavioral advertising.

5. Where your data is stored

StratiqAI separates a central control plane, which handles accounts, billing, and fleet operations, from your dedicated environment, which handles your work.

- **In your dedicated environment** (on its encrypted volume): conversations and messages; team chat, tasks, and activity; attachment records; your sessions; your connected-system credentials (encrypted again with a key unique to your environment); and agent memory and working files. Your working data is stored in a database inside your environment and never shares a runtime, database, or network with another customer's.
- **In encrypted object storage:** the files you upload, and backup archives.
- **In the control plane:** user accounts and sign-in; organizations, memberships, and invitations; subscriptions, billing, and the AI credit ledger; fleet provisioning and monitoring; workspace settings and agent roster; and the audit log of administrative actions.

Location. Customer environments and the control-plane database run in United States regions by default.

6. How we share information

- **Service providers** who help us host and operate the Service, under contracts that allow them to use the information only to provide services to us.
- **AI model providers.** Requests are sent to the selected model through our model gateway (Section 7).
- **Tools you connect.** When an agent acts in a connected tool at your direction, information is sent to that tool, under that provider's own terms and privacy policy.
- **Your organization.** For organization accounts, the account holder and its owners and admins.
- **Community.** StratiqSphere content is visible to other members.
- **Legal and safety.** When we believe disclosure is required by law or legal process, or necessary to protect the rights, property, or safety of StratiqAI, our users, or others.

- **Business transfers.** In connection with a merger, acquisition, financing, reorganization, or sale of assets, subject to confidentiality protections.
- **With your consent or at your direction.**

7. AI models and model providers

- **Model choice.** Agents have default models, and customers can choose other models available through our AI model gateway.
- **What is sent.** To generate a response, an agent sends a request, which may include relevant parts of your files, connected-tool data, memory, and conversations, to the selected model. Agents see only your environment's data.
- **Spending controls.** Each customer has its own key for the AI model gateway, capped by a spending limit tied to its prepaid AI balance. When the balance runs out, new AI work pauses.
- **Model providers.** Our model provider forwards requests to the provider of the selected model. Model providers have their own data practices, and some may retain prompts or outputs or use them to train or improve their models. We plan to adopt zero data retention with AI model providers, so that prompts and outputs are not retained by them, but this is not yet in place. Review the data practices of the provider of any model you select.
- **Your own model keys.** Organizations with their own model provider agreements may be able to supply their own keys. If you do, your agreement with that provider governs data sent using your keys.

8. Security

We design StratiqAI so that your deal, property, and client data is isolated by design, not just by policy. Key controls include:

- **Dedicated environment per customer.** Each customer's App and agents run in a dedicated, hardware-virtualized virtual machine (microVM) with its own kernel, its own encrypted volume, and its own private network. Private networks for different customers have no route or private DNS between them. Inside your environment, the agent runtime listens only on the local machine. Your App is the only service exposed, over HTTPS.
- **No cross-customer credentials.** No customer environment holds credentials that could read another customer's data. Your environment talks to the control plane over a single authenticated, customer-scoped HTTPS channel that accepts only an allowlist of operations.
- **Encryption.** Traffic is encrypted in transit with TLS, and browsers are told to use HTTPS only. Customer volumes, object storage, and the control-plane database are encrypted at rest.
- **Credential protection.** Credentials for connected systems, such as OAuth tokens and API keys, get a second layer of encryption. Each secret is encrypted with its own 256-bit data key using AES-256-GCM. That key is wrapped with a key-encryption key unique to your environment, which is never stored in the control-plane database. Each secret is bound to your organization and its purpose. Keys are versioned and can be rotated. A sealed copy of each environment key is kept for recovery, and the recovery key is held offline.

- **Sign-in and sessions.** You sign in with email and password or a supported single sign-on provider such as Google. Sessions last at most 8 hours and end after 1 hour of inactivity. Sensitive actions, such as rotating credentials or disconnecting a connected system's key, require a recent sign-in. When a team member is removed, their administrative access ends on their next request. Multi-factor authentication is planned but not yet available.
- **Agent safeguards.** By default, agents must get a person's approval before running actions flagged as risky. Workspace admins can choose a less strict mode, but a fixed set of dangerous operations, such as accessing credential files or wiping the data volume, is always refused. Each agent has its own profile, memory, and access keys.
- **Audit logging.** Operator actions and sensitive administrative changes, such as credential and connection changes, are written to an append-only audit log.
- **Backups and monitoring.** Customer environments are backed up through volume snapshots and separate off-platform encrypted archives. Environments are continuously health-checked, and failures alert our operations team.

StratiqAI's controls are designed to align with the AICPA SOC 2 Trust Services Criteria. StratiqAI has **not** yet completed an independent SOC 2 audit and does not claim any certification or attestation of its own. An independent SOC 2 Type II audit is on our roadmap. No method of transmission or storage is completely secure.

Access by StratiqAI personnel. StratiqAI support access is limited to a named allowlist of staff accounts that sign in through single sign-on. Every operator change must include a written reason and is recorded in the audit log, and destructive operations require additional confirmation. Infrastructure credentials are scoped to a single environment.

Security incidents. If we become aware of a security incident affecting your personal information, we will notify affected customers and individuals as required by applicable law.

To report a suspected vulnerability or security concern, contact us immediately at info@stratiqai.com or the App's bug reporting tools. We appreciate responsible disclosure: please give us a reasonable chance to fix an issue before sharing it publicly.

9. Data retention and deletion

- **Conversations and agent activity.** Chat messages and agent tool activity are kept for 90 days on base plans and 365 days on pro plans, then deleted automatically.
- **Other Customer Data.** Customers can export or delete their own Customer Data.
- **Disconnecting tools.** Disconnecting a tool deletes its stored credentials from your environment. Files agents already created remain in your library and projects until deleted.
- **Removing an agent.** Removing an agent deletes that agent's profile and keys from your environment.
- **Cancellation.** After a subscription is cancelled, there is a 7-day grace period. Then the environment, including its virtual machine and volume, is deprovisioned.
- **Backups.** Volume snapshots are kept for 60 days, and off-platform archives are kept for 90 days. Deleted data may remain in backups until they expire.

- **Control-plane and other records.** Control plane and other data records are kept for 90 days.
- We may retain information as required by law, to resolve disputes, or to enforce our agreements.

10. Your choices

- **Export or delete Customer Data** as described in Section 9, or by contacting us. In organization accounts, some controls are limited to owners or admins.
- **Disconnect tools** at any time, which deletes their stored credentials.
- **Control write access** for each connection and each agent.
- **Choose models** for your agents, subject to your plan.
- **Revoke Google access** in your Google Account settings if you signed in with Google.
- **Opt out of marketing emails** with the unsubscribe link or by contacting us. We may still send account, billing, and service messages.
- **Close your account** as described in our Terms of Service.

11. U.S. state privacy rights (including California)

Depending on where you live, you may have the right to:

- know about and access the personal information we have collected about you;
- correct inaccurate personal information;
- delete personal information;
- obtain a portable copy of your personal information;
- opt out of the sale or sharing of personal information or its use for targeted advertising or profiling (we do not sell or share personal information for these purposes); and
- not be discriminated against for exercising these rights.

California notice at collection (CCPA/CPRA). In the past 12 months we have collected the following categories of personal information, for the purposes in Section 4, and disclosed them to the categories of recipients in Section 6:

- identifiers (such as name, email address, IP address);
- customer records and professional or employment-related information (such as company, organization role, and membership);
- commercial information (such as plan, subscription, transaction history, and AI credit usage);
- internet or other electronic network activity (such as usage and security logs);
- audio, electronic, or visual information (such as uploaded images and screenshots);
- sensitive personal information limited to account login credentials and integration credentials, used only to provide the Service; and
- other information contained in Customer Data that customers upload or connect.

We retain each category as described in Section 9.

How to submit a request. Email info@stratiqai.com with the subject "Privacy Request." We will verify your request using information associated with your account. You may use an authorized agent, who must provide proof of authorization. Requests about Customer Data held on behalf of a StratiqAI customer (including your employer's organization account) should go to that customer.

12. EEA, UK, and Swiss users (GDPR)

Where GDPR or UK GDPR applies:

- **Controller.** StratiqAI, LLC is the controller of the data described in Section 2 as "our own data." For Customer Data, we act as a processor on behalf of the customer.
- **Legal bases.** Performance of our contract with you; our legitimate interests (securing and improving the Service and communicating with business users); compliance with legal obligations; and consent where required (for example, certain marketing or cookies).
- **International transfers.** We are based in the United States. Customer environments and the control-plane database run in United States regions by default, and our providers may process data in the United States and other countries.
- **Your rights.** Access, rectification, erasure, restriction, objection, data portability, and withdrawal of consent. You may lodge a complaint with your local data protection authority.
- **Representative.** We currently do not have a European representative.

13. Children

The Service is for business use by adults and is not directed to anyone under 18. We do not knowingly collect personal information from children.

14. Cookies and similar technologies

The App uses session cookies to keep you signed in and secure. These cookies can't be read by page scripts, are sent only over HTTPS, and are withheld from most cross-site requests. You can control cookies in your browser, but disabling essential cookies will stop the App from working.

15. Third-party services and links

The Service connects to third-party tools you choose and may link to other websites. Their privacy practices are governed by their own policies.

16. Changes to this policy

We may update this Privacy Policy from time to time. We will revise the "Last Updated" date and, for material changes, notify account holders by email or in the App before the changes take effect.

17. Contact us

- Privacy requests: info@stratiquai.com
- Security reports: info@stratiquai.com
- General questions: info@stratiquai.com
- Mailing address: 1095 Dollar Street, West Linn, OR 97068