

# Security and privacy

From the SourceLace manual: What SourceLace stores, what it never stores, how it protects what it keeps, and where your data goes. Written for your security reviewer: every statement here describes how SourceLace works today. Questions: [security@sourcelace.com](mailto:security@sourcelace.com).

SourceLace version 0.1.0 · Made October 4, 2026

The latest version is at <https://sourcelace.onrender.com/docs>

# Security and privacy

What SourceLace stores, what it never stores, how it protects what it keeps, and where your data goes. Written for your security reviewer: every statement here describes how SourceLace works today. Questions: [security@sourcelace.com](mailto:security@sourcelace.com).

## The short version

- **Each person uses their own login** to each system. SourceLace never uses a shared admin account for your systems (the exceptions, Amazon S3 and Gong, are explained below), so people only ever see and change what they already could.
- **Read-only by default.** Changes are off for every source until an admin turns them on for named objects, and even then every change is previewed and only sent after the person confirms it.
- **Your records are not stored.** Query results live in memory for at most 30 minutes and are never written to a database. The one exception is saved chats in the SourceLace app, which are encrypted and deleted after your retention period.
- **Secrets are encrypted with a key for your organization alone**, and never shown, returned or logged.
- **Everything is audited:** every call, by every person and every client, in a tamper-evident trail that holds metadata, not your data.

## What SourceLace stores

| What                                                                                                                                                                                                         | Where and how                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Your organization, its people and their roles, groups, sources and their options, skills and projects                                                                                                        | SourceLace's database.                                                                                                                                                                                                           |
| Each person's sign-ins to your systems (access and refresh tokens), database passwords, Oracle and Workday client secrets, custom connectors' shared secrets, single sign-on client secrets, your own AI key | SourceLace's database, <b>encrypted with your organization's own key</b> (see <a href="#">Encryption</a> ). Never shown again after saving, never returned by any API, never logged.                                             |
| Saved chats in the SourceLace app: messages, the tables, charts and tool results in them, and files made in them                                                                                             | SourceLace's database, encrypted with your organization's key, and <b>deleted after your retention period</b> (30 days after last use by default; admins choose 1 to 3,650 days). People can delete their own chats at any time. |
| The audit trail                                                                                                                                                                                              | SourceLace's database. Metadata only (see <a href="#">The audit trail</a> ).                                                                                                                                                     |
| AI usage                                                                                                                                                                                                     | One row per question: who, when, which model and token counts. Never the question or the answer.                                                                                                                                 |
| Sign-in codes, one-time links and tokens SourceLace issues to MCP clients                                                                                                                                    | Stored only as SHA-256 hashes, so a copy of the database cannot be replayed as tokens.                                                                                                                                           |

## What SourceLace does not store

- **Rows from your systems.** Query results are held in memory, for the person who asked, for at most 30 minutes (up to 2,000 rows a query), then forgotten. They are never written to a database, a file or a log, outside saved chats.
- **Files from your file stores.** SourceLace reads a file only when someone asks, pulls its text out in memory, and does not copy, crawl or index files.
- **Passwords to SourceLace.** People sign in to SourceLace with Google, Microsoft or your single sign-on provider.

## Encryption

- **In transit:** SourceLace is served over HTTPS. Connections from SourceLace to your systems use TLS, and SourceLace checks the certificate; for databases it also checks the certificate was issued for the host name your admin entered, and TLS cannot be turned off for any database other than one on the same computer as SourceLace.
- **At rest:** each organization has its **own random data key**. Secrets and saved chats are encrypted with it using Fernet (AES-128 in CBC mode with an HMAC-SHA256 integrity check). Your data key is itself stored only in encrypted ("wrapped") form, under a master key held by the hosting provider as a secret and never stored in the database. Without your data key, nothing encrypted for your organization can be read.

## Access control

- **Signing in to SourceLace:** with Google, Microsoft, or your own single sign-on (OIDC, such as Okta or Microsoft Entra ID; see [Single sign-on](#)). Only people your admins add, or people from your organization's allowed email domains, can sign in. A session in the SourceLace app lasts 7 days.
- **MCP clients** sign in through SourceLace with standard OAuth. Their access tokens last 1 hour and are refreshed for up to 30 days, after which the person signs in again.
- **Roles:** admins manage people, sources, groups, single sign-on and AI settings; members use the sources they may use. See the [Admin guide](#).
- **Groups:** admins can limit each source to named groups of people, and sync groups from your identity provider. See [Access by group](#).
- **Your systems' own permissions** apply to every call, because each person signs in with their own login. SourceLace adds its own limits on top, never removes any.

## Shared access: Amazon S3 and Gong

Two sources cannot use per-person logins, so their access is **per source**: Amazon S3 (one set of read-only AWS credentials or a role per source) and Gong (Gong only lets a technical admin authorize an app, for the whole company). Everyone who may use such a source reads with the same access. Add them only where that is acceptable, and narrow who can use them with groups.

## Reads, changes and query checks

- Every query is checked **before** it is sent: one read-only statement in the system's own language, with anything that writes, deletes, locks, calls out or runs code refused. Databases are also queried inside read-only (or always rolled-back) transactions with a time limit. See [How queries stay read-only](#).
- **Changes** are off for every source until an admin turns them on for named objects. Then `propose_change` shows the current and new values, and nothing is sent until the person confirms: in SourceLace's own confirmation prompt where their app can show one, or by typing the confirmation code from the preview. Three wrong codes discard the preview, and previews expire after 10 minutes. Where the system supports it, the change is refused if the record changed after the preview.
- SourceLace never sends email: mail sources only make drafts, which the person sends themselves.

## The audit trail

Every tool call is recorded, whether it succeeded, was refused or failed, from the SourceLace app, from every MCP client and from admins. So are sign-ins and every change to people, sources, groups and single sign-on.

Each entry holds: when, who, the tool, the source, the person's id in that system, the query text, the object, the record id, the **names** of changed fields, how many rows came back, the outcome, the error type, and how long it took. It **never** holds row values, field values, passwords, keys or tokens. Note that the query text is kept as written, so a filter value typed into a query (such as a customer name) appears in the trail.

Entries are chained by SHA-256 hashes per organization: editing, removing or reordering an entry breaks the chain, which SourceLace detects. If an entry cannot be written, the call fails rather than returning data that was not recorded. Admins read the trail on the **Audit Log** page. It is kept, and not deleted automatically today.

## AI and your data

### **From your own AI app (MCP clients such as Claude, ChatGPT, Cursor or VS Code):**

SourceLace sends nothing to any AI model. It returns results to your AI app, which sends them to its own AI provider under your agreement with that provider.

**From the assistant in the SourceLace app:** to answer, SourceLace sends the conversation to Anthropic's API: the person's questions, the assistant's earlier replies, your project instructions and skills used, and the results of the tools the assistant called, which can include rows from your systems. Your admin chooses whether this goes through SourceLace's Anthropic account (the default), your organization's own Anthropic key, or your organization's own OpenAI key. With your own key it is under your own agreement with that provider. Requests to OpenAI are sent with OpenAI's store option off, so OpenAI does not keep the conversation for later retrieval.

SourceLace does not train AI models on your data, and does not send it to any AI provider other than the one your admin chose.

## Hosting and subprocessors

- **Hosting:** SourceLace runs on **Render**, in its **Oregon (United States)** region: the application and its database. A move to **AWS is planned**, not yet done.
- **Subprocessors:**

| Company                                                | What for                                                                  | What it receives                                                                      |
|--------------------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Render                                                 | Hosting the application and database                                      | Everything SourceLace stores (encrypted as described above) and processes.            |
| Anthropic                                              | The assistant in the SourceLace app (only when people use it)             | The conversation and tool results, as described in <a href="#">AI and your data</a> . |
| OpenAI (only if your admin enters your own OpenAI key) | The assistant in the SourceLace app, under your own agreement with OpenAI | The conversation and tool results, as described in <a href="#">AI and your data</a> . |
| Google, Microsoft, or your single sign-on provider     | Signing people in to SourceLace                                           | The sign-in itself, under your own account with them.                                 |

Your connected systems (Salesforce, SAP and so on) receive only the calls each person makes with their own login.

## Certifications and agreements

SourceLace does not yet hold any security certification or attestation. **SOC 2, ISO 27001 and HIPAA are not yet available**, so neither is a HIPAA Business Associate Agreement. **A GDPR data processing agreement (DPA) is not yet available** either. Data is hosted in the United States only today.

For a security questionnaire, a review call, or to report a vulnerability, email [security@sourcelace.com](mailto:security@sourcelace.com).

## Removing access and data

- **A person** can disconnect any source at any time, which deletes their stored sign-in for it, and delete their own chats.
- **An admin** can remove a person, remove a source, or turn changes off at any time.
- To close your organization's account and have its data deleted, email [support@sourcelace.com](mailto:support@sourcelace.com).