FAQ: Compliance and contracts

From the SourceLace manual: Certifications, agreements, security questionnaires, subprocessors and incident notice. Every answer says plainly what is not in place yet.

SourceLace version 0.1.0 · Made November 22, 2026
The latest version is at https://sourcelace.ai/docs

Compliance and contracts

Certifications, agreements, security questionnaires, subprocessors and incident notice. Every answer says plainly what is not in place yet.

Is SourceLace SOC 2 certified? Do you sign a DPA?

Not yet. SourceLace does not yet hold any security certification or attestation: no SOC 2 report, no ISO 27001 certificate and no HIPAA attestation. A GDPR data processing agreement is not yet available either. Please do not record SourceLace as holding a certification in your vendor register. A SOC 2 Type 2 examination is in progress: SourceLace has engaged an independent CPA firm for a SOC 2 Type 2 examination covering Security and Privacy. The observation period began on 1 November 2026, and we expect the report in 2027. SourceLace does not hold a SOC 2 report yet. Email security@sourcelace.com for a security review.

Details: Organization and certifications.

Do you have written security policies and staff checks?

Partly. These are written down and approved by SourceLace's owner, each reviewed yearly: information security (including how information is classified), access control, change management and secure development, risk management, business continuity and recovery, incident response, requests about people's own data, security and privacy training, and vendor management. Not yet in place: staff background checks and a penetration test by an outside firm.

Details: Do you have written security policies, staff background checks or security training?.

What can we request for a security review?

The security questions page in the manual, the subprocessor list, a summary of how incidents are handled, your own questionnaire filled in by SourceLace or a review call, and a security review pack with more technical detail under NDA. There is no SOC 2 report or penetration test report yet. Email security@sourcelace.com.

Details: What can we request for a security review?.

We have a security questionnaire to fill in. Where do we start?

Security questions answers the questions vendor reviews ask (hosting, encryption, keys, access, retention, AI providers, subprocessors, audit, incident response, backups), one by one, and says plainly what is not in place yet. Deeper detail is in a security review pack we share under NDA. For anything else, email security@sourcelace.com.

Details: Security questions.

Has SourceLace had a penetration test? Is there a bug bounty?

Not yet. No independent penetration test report is available, and there is no bug bounty programme. Report vulnerabilities to security@sourcelace.com.

Details: Vulnerability management and secure development.

Can we use SourceLace with patient data?

No, not yet. There is no HIPAA Business Associate Agreement yet, so do not connect systems holding protected health information. Health record connectors are for test data only until a business associate agreement is signed.

Details: Healthcare and HIPAA.

Who are your subprocessors?

The companies that host SourceLace, provide the included AI for the assistant, sign people in, and handle billing. The manual names each one, what it is for and what it receives. Your connected systems receive only the calls each person makes with their own login.

Details: Hosting and subprocessors.

Will you tell us before adding a subprocessor?

The subprocessor list is updated before a new provider handles customer data. A contractual notice period is not yet formalised.

Details: Will you tell us before adding one?.

Will you tell us about a breach?

Yes. If your data may have been reached, SourceLace tells your admins without undue delay, and as the law requires. A contractual notification time, such as 72 hours, is not yet formalised. To report a suspected incident, email security@sourcelace.com.

Details: Incident response and breach notification.

Do you have an incident response plan?

Yes, a written process in use since October 2026: four severity levels, one person leading each incident, harm stopped first, your admins told by email as soon as possible when your organization is affected, a written summary within 5 working days after a serious incident, and yearly practice. A public status page is not in place yet.

Details: Do you have an incident response plan?.

Is there an uptime SLA or a status page?

Not yet. No uptime commitment or public status page is published. The app's **My connections** page shows, for your organization, whether the assistant is ready and how each source's calls went in the last 24 hours, and admins also have a **Health** page: connections, AI agents, the audit trail, usage and sign-in, with the problems first. Your data stays in your own systems, so nothing you rely on lives only in SourceLace except saved chats, skills, projects and agent settings.

Details: Business continuity and backups.

Can our contract differ from the standard terms?

A signed order form or pilot agreement with SourceLace takes priority over the standard terms where they differ. Ask your SourceLace contact. Your organization's own plan, prices and agreed discounts are shown on the **Billing** page.

Details: Plans and limits.