Sealens

// SECURITY ONE-PAGER

Access and data handling

Closed beta · October 2026 · hello@sealens.io

A short, factual description of what Sealens accesses in your environment, what it cannot do, and where your data goes — written to be attached to a vendor security review. It describes the service as operated for closed-beta customers. **Where something is not yet true, or not yet fully resolved, this document says so rather than omitting it.** The contractual version of these commitments is the Data Processing Agreement (sealens.io/dpa.html); where the two differ, the DPA governs.

ACCESS	IN YOUR INFRA	HOSTING	DELETION
Read-only token scopes	**No agent, nothing installed**	**Scaleway, Paris region**	**Within 30 days**

01 What Sealens reads

Sealens analyses the history of the Git repositories you connect — commits, diffs, file paths, authorship metadata, branches and tags — and correlates them with deployment and incident events that **your own tools send to it**.

SCOPE	ACCESS	WHY
`contents:read`	Read-only	Commits, diffs, file paths, branches and tags
`metadata:read`	Read-only	Repository metadata
`deployments:read`	Read-only · **optional**, shown as its own line at installation	Tells which changes were actually running when an incident started, instead of guessing from tags. The product works without it, with a stated loss of precision

Sealens **cannot create commits, branches or pull requests**, and cannot modify any setting in your repository or organisation. This is not a policy applied on top of broader access — **it is the only access we hold.** Connecting is done per repository, by someone who already has rights on it — roughly five minutes, no organisation administrator involved. A future GitHub Marketplace installation would be configured for selected repositories only, never “all repositories”.

02 What Sealens never receives

- **No production data.** Sealens reads code history — not your databases, traffic or logs.
- **No runtime agent.** No daemon, no sidecar, no instrumentation of your services.
- **No polling of your monitoring tools.** Incident and deployment events arrive only because your tools push them to an endpoint you configure. Sealens never queries your observability stack on its own initiative.
- **No secret values.** Sealens flags that a credentials or configuration file appears in a change; it never extracts, stores or displays the value of a secret.

03 Hosting, isolation and credentials

TOPIC	COMMITMENT
Where data lives	Analysis and storage run on **Scaleway, Paris region (France)** — a deliberate choice of a European provider over a US-headquartered cloud, so that infrastructure data is not exposed to US extraterritorial access regimes such as the CLOUD Act.
Your source code	Analysis runs against a **clone held by Sealens**. Your source is not forwarded anywhere else, and no third party receives your code.
Customer isolation	Separated by workspace at two levels: every query is scoped to the workspace at the application layer, and every affected table carries an indexed workspace column filtered on each access.
Credentials	Git provider tokens are held in a **dedicated secrets manager** — never stored in plain text

TOPIC	COMMITMENT
	in the application database, never written to logs.
Encryption	In transit: **TLS 1.3**. At rest: **AES-256**.

04 Sub-processors

The authoritative, maintained list is Annex 1 of the DPA. In summary:

SUB-PROCESSOR	LOCATION	PURPOSE
Scaleway	France	Hosting, storage, transactional email
Anthropic (Claude API)	United States	Turns an already-computed, structured analysis result into readable text
Brevo	France	Closed-beta application and access correspondence
Slack / Microsoft Teams	—	Notifications to a channel you configure, only if you enable it. On Slack, a Sealens app with three permissions: choose that channel at install (incoming-webhook), post and reply in the incident thread (chat:write), find a fix author's Slack account from their commit email to mention them (users:read.email; only the matching ID is kept). It cannot read your messages. On Teams, a workflow you create, no app

THE OPEN POINT, STATED PLAINLY

Our language-model provider is a US company. This is the one place where the European-sovereignty argument above is not end-to-end, and we would rather name it than let you discover it in Annex 1.

Two things bound it: the provider receives **the structured analysis payload only** — never your commits, diffs or source — and it does not train on data submitted through its commercial API. Transfers rely on Standard Contractual Clauses. We are evaluating a European alternative; we have not switched, because we have not yet verified it is as faithful on our task, and **we will not claim a migration we have not made.**

05 Retention and deletion

On termination, or on written request, Sealens deletes or returns your data **within 30 days**. Deletion cascades across every storage engine holding workspace-scoped data. Backups are not purged instantly: they expire with the normal backup rotation cycle, as stated in the DPA.

06 What Sealens deliberately does not do

These are architectural boundaries, not features awaiting prioritisation.

- **No write access to your repositories**, at any stage. Where Sealens suggests an action — including a rollback — it produces text for a person to act on. It never acts on your repository.
- **No approval or deployment gating.** Sealens observes whether your existing review process was followed; it is never the mechanism that enforces it, and it cannot block a deployment.
- **No access-permission auditing.** Sealens reads changes in Git. It does not query your cloud IAM state or assess your live permissions.
- **No agent acting unsupervised.** Every recommendation is proposed to a person. Nothing is applied automatically.

07 Verifying this yourself

Most of the above is checkable without taking our word for it: the scopes appear on the installation screen before you grant anything, the absence of write access is visible in the same place, and the sub-processor list is published rather than supplied on request.

QUESTIONS

If your review needs something this document does not cover, ask — **a question we cannot answer plainly is a problem on our side.**

hello@sealens.io · sealens.io/dpa.html