REPO REVIEW
ARCHITECTURE & SECURITY

DATA HANDLING STATEMENT

What happens to your repository

For your security reviewer: where your code goes, how long each piece stays, who can read it, and what we do not yet guarantee. Every retention period below is enforced by configuration, not by a person remembering to delete something.

VERSION	LAST REVIEWED	STAGE	REGION
1.0	16 November 2026	Private alpha	AWS Sydney (ap-southeast-2)

In short

- Read-only access through a GitHub App you install and can revoke at any time.
- One copy of one branch, with no history, deleted **one day** after the run.
- Reports deleted **30 days** after the run, or at once when you ask.
- Everything stored in Sydney. Parts of your code are sent to one model provider, Anthropic, and nowhere else.

1 In one table

WHAT	WHERE	KEPT FOR	WHO CAN READ IT
Access to your repository	GitHub, through the Architecture Automation GitHub App you install	until you uninstall it	the service, read-only, one repository per token
The per-run access token	AWS Systems Manager, encrypted, one parameter per run	deleted after the clone; expires within the hour regardless	the clone task only

WHAT	WHERE	KEPT FOR	WHO CAN READ IT
A copy of your code (one branch, depth 1, packed)	S3, private bucket, Sydney	**1 day**, then deleted automatically	the analysis task
The working copy during analysis	the analysis container's own disk	the length of the run (under 3 hours); the container is destroyed after	the analysis task
Parts of your code sent for analysis	Anthropic's Claude model API (section 4)	per Anthropic's terms	Anthropic, as processor
The documents produced	S3, same bucket	**30 days**, then deleted automatically	the reviewer; you, through links once released
Run log and diagnostics	S3 beside the documents; CloudWatch Logs	30 days (S3); 14 days (CloudWatch)	the operator only
The run record: repository URL, branch, commit, status, ratings, finding counts	DynamoDB, encrypted	for the life of your account	the operator; you, through the portal or API with your key
Fixed scores: the seven ratings and the health verdict for each state of your code, so a rerun of unchanged code reports the same scores. Numbers only, never code	S3, same bucket, under a hash of your repository URL	for the life of your account	the analysis task; the operator
Your email address, if you signed up for a free Snapshot	DynamoDB, on your key	for the life of the key's record	the operator; the service, to send you the key and the release
Network log: each HTTPS connection the analysis made or tried, by host name and time, never its content	CloudWatch Logs	30 days	the operator only
Audit trail: who issued, rotated or revoked a key, started, released, withheld or deleted a run, or was handed links to its documents, and when	CloudWatch Logs	1 year	the operator only

2 The path your code takes

1. **Access.** You install the GitHub App on the repositories you choose. Nobody hands us a password or a long-lived token. You can see and revoke the installation in your own GitHub settings at any time, and revocation takes effect at once.

2. **Clone.** When your run's turn comes, the service asks GitHub for a token valid for one hour, read-only, for that one repository. A short-lived task clones the requested branch at depth 1 (no history, no submodules, no git hooks run), packs it, uploads it to the private bucket and stops. The token is deleted.

3. **Analysis.** A second task, in a private subnet with no inbound access whose only way out is an allow-list of hosts (section 3), unpacks the code, builds a structural graph of it and runs the analysis. The analysis reads files and sends the parts it needs to the model API. The documents are written to the bucket; the task and its disk are destroyed.

4. **Review.** By default, a person reads every report before it is released to you, and nothing is sent to you or anyone else until then. A key can be set up with you to release a report automatically when every check passes; a report with any failed check always waits for a person.

5. **Release.** You receive links to the documents. Each link expires after 7 days; the documents themselves are deleted 30 days after the run. Download what you want to keep.

6. **Deletion.** The packed copy of your code is deleted one day after the run, whatever happens to the run. The bucket is versioned, and earlier versions are deleted on the same schedule. You can delete a run's documents yourself at any time from the portal, or ask us to: either removes every version of every file the run left, at once.

3 Storage and transport

Region	Sydney (ap-southeast-2) for every stored item. Code sent to the model provider leaves Australia: see section 4.
Encryption at rest	S3 server-side encryption on the bucket; DynamoDB encryption; access tokens and the GitHub App's private key as SecureString parameters, the key under its own KMS key.
Encryption in transit	TLS everywhere. The bucket refuses any request not made over TLS.

No public access	The bucket blocks all public access. Documents are reached only through expiring signed links or the operator's console, which requires sign-in.
Outbound allow-list	The analysis can connect only to the model API and the AWS services that run it (the container registry, logs, and Parameter Store for the model credential), checked by host name at a filter it cannot bypass, and to our own storage bucket through a private endpoint that refuses every other bucket. Every connection it makes or tries is logged by host name.
Least privilege	Each part of the service has its own role. The clone task reads only run tokens and writes only packed repositories; the analysis task reads packed repositories and writes documents, and the code under analysis runs without those AWS credentials at all.

4 The model provider

The analysis is done by Anthropic's Claude. To analyse your repository, the model reads files from it, so portions of your source code are sent to Anthropic's API and processed in Anthropic's infrastructure, which may be outside Australia.

- **Today (private alpha):** the service runs on a Claude subscription, used only on the operator's own repositories and those of customers who have agreed to that in writing.
- **Before general availability:** the service moves to Anthropic's commercial API, whose terms state that inputs and outputs are not used to train models by default. This statement will be updated with the date.

5 What we do not keep

- ✓ Your code after one day.
- ✓ Any access token after the clone.
- ✓ Your GitHub identity: the App acts as itself and never signs in as you.
- ✓ What a run cost, in or beside your documents.

6 What we do not yet guarantee

Stated plainly, because your reviewer will ask.

Network during analysis	The analysis may run parts of your repository's own code (its test suite, for example). Its HTTPS connections are limited to the allow-list above and it can reach nothing else inside our network, but name lookups are not filtered, and the allowed hosts (the model API, AWS services) are shared services that code holding its own credentials for them could use to send data to its own account. This matters only if your repository's own code is hostile; it never exposes our credentials or your access token, which is already deleted.
The model credential, during the alpha	On commercial API terms the credential is held by a separate process and the analysis only ever has a placeholder for its own run, so code from your repository cannot read it. During the alpha's subscription it would be within reach of that code, so during the alpha **your repository's own code is not run**: its tests are reported as not run.
Free sign-up	Free sign-up is for public repositories only. A private repository is set up with you directly, so nobody who merely names it can request a report on it.
Commercial model terms	See section 4.
Certification	The service holds no SOC 2 or ISO 27001 certification.
Your own AWS account	Running the analysis inside your AWS account, so the code never leaves it, is planned for enterprise customers and not available yet.

7 Your controls

- **Revoke access at any time:** uninstall the GitHub App, or remove a repository from it.

- **Delete a run:** from the portal, or by asking us, which removes every version of its documents at once. The run's record (repository URL, branch, commit, ratings) stays, marked deleted; ask us and we remove that too.
- **Ask what we hold:** we tell you every run, its date, its repository and branch, and what is still stored for it.

Questions, or a security review to complete? Write to support@reporeview.com.au and a person answers.