SECURITY AND DATA HANDLING

Your code stays yours.

CodePulse turns engineering workflow data into delivery insight through a least-privilege, read-only GitHub connection. We never clone your repository, read your files, or ask for write access. The one place code ever touches CodePulse is documented on the next page.

Read-only GitHub App	Your code stays yours	Encrypted credentials	SOC 2-aligned controls
No write, delete, or administration permissions.	We never clone your repository or read your files.	GitHub tokens and webhook secrets are encrypted with Fernet before storage.	Mapped to the applicable AICPA Trust Services Criteria.

Data flow

01 Selected repositories
An organization owner selects exactly which repositories CodePulse may access.

→

02 Read-only connection
API traffic uses TLS. Inbound GitHub webhooks are signature-verified.

→

03 Scoped processing
CodePulse processes delivery and review context without cloning repositories.

→

04 Tenant-scoped analytics
Workflow data and calculated metrics are partitioned by organization.

Data boundary

CodePulse processes

- ✓ Account, organization, repository, and team identifiers
- ✓ Pull request titles, descriptions, states, labels, and timestamps
- ✓ Commit identifiers, messages, authorship, and change counts
- ✓ Changed file paths and aggregate additions/deletions
- ✓ Review activity, comments, and discussion
- ✓ The short code snippet GitHub attaches to an inline review comment, retained with that comment so review depth and quality can be measured
- ✓ Check and deployment events
- ✓ Connected issue fields when issue analytics is enabled

CodePulse does not ingest

- x Your source files - CodePulse never clones your repository or reads file contents
- x Complete pull request patches or full source-code diffs
- x Secrets, environment variables, or private keys
- x CI/CD logs and build output
- x Write, delete, or repository administration access
- x Keystrokes, screens, browsers, or local machine telemetry

GitHub App permissions

Permission	Level	Purpose
Metadata	**Read**	Repository identity and installation metadata. GitHub grants this automatically.
Contents	**Read**	Commit history, branches, file paths, and change counts. File contents are never requested.
Pull requests	**Read**	Lifecycle events, reviews, comments, requested reviewers, and changed-file metadata.
Checks and statuses	**Read**	Check name, state, conclusion, and timing used for delivery-health metrics.

Permission	Level	Purpose
Issues	**Read**	Optional issue analytics and links between work items and pull requests.
Members	**Read**	Organization membership used for access control and team configuration.

CONTROL ENVIRONMENT

The controls behind the connection.

These controls are in place today and documented, so your reviewer can assess them directly rather than inferring them from a certificate.

Access control

- ✓ Role-based product permissions
- ✓ Organization membership checks
- ✓ Restricted production administration
- ✓ Revocable GitHub installations

Encryption and secrets

- ✓ TLS for data in transit
- ✓ Encrypted external credentials
- ✓ Webhook signature validation
- ✓ Production secret startup checks

Tenant isolation

- ✓ Organization-scoped data models
- ✓ Authenticated membership enforcement
- ✓ Role checks on protected actions
- ✓ Administrative action logging

Application integrity

- ✓ Peer-reviewed changes
- ✓ Automated tests and dependency checks
- ✓ Parameterized database access
- ✓ Input validation and rate limits

Operational resilience

- ✓ EU-hosted production infrastructure
- ✓ Operational backups
- ✓ Error and performance monitoring
- ✓ Documented incident response

Privacy and lifecycle

- ✓ Public Data Processing Agreement
- ✓ Documented sub-processors
- ✓ Organization deletion workflow
- ✓ Data-subject request support

SOC 2 posture

The CodePulse security program is mapped to the applicable AICPA Trust Services Criteria, with security as the core category. Controls are being operated and documented now so an examination can follow as the business scales.

CodePulse has not yet completed an independent SOC 2 examination and does not represent itself as certified or as holding a Type I or Type II report.

Control framework	**Mapped**
Operational evidence	**Ongoing**
Independent report	**Not yet issued**

Incident and data lifecycle commitments

Incident response

- ✓ Central security contact and defined incident ownership
- ✓ Severity-based triage, containment, recovery, and review
- ✓ Customer notification consistent with contractual and legal duties
- ✓ Post-incident corrective actions tracked to completion

Customer control

- ✓ Repository selection controlled by the GitHub organization owner
- ✓ GitHub installation revocable at any time
- ✓ Organization deletion uses a tracked offboarding workflow
- ✓ Data-subject and portability requests supported through the DPA

PROCUREMENT AND RESPONSE

Ready for your security review.

CodePulse publishes the documents and contacts a buyer needs to evaluate data handling, privacy terms, service providers, and incident readiness.

Security and privacy review materials

Trust Center

Live permissions, data-flow, control, and compliance information.

codepulsehq.com/security

Data Processing Agreement

Article 28 terms, technical measures, and sub-processor annex.

codepulsehq.com/dpa

Privacy Policy

Personal-data use, retention, rights, and contact information.

codepulsehq.com/privacy

Service Status

Current and historical availability information.

status.codepulsehq.com

Current customer-data sub-processors

Provider	Purpose	Customer data
Amazon Web Services	**Hosting**	Customer personal data at rest in EU (Ireland)
Stripe	**Billing**	Billing identifiers and contact email
Resend	**Service email**	Administrator email and message content
PostHog	**Product analytics**	Usage events with account or organization identifiers
Self-hosted Sentry	**Error monitoring**	Diagnostic telemetry with secret-bearing values redacted
OpenRouter	**Work classification**	Pull request titles and file paths only

Security review contact

security@codepulsehq.com

Keep Pushing Forward Ltd, trading as CodePulse.
Registered in England and Wales.
codepulsehq.com