Security & Data Protection

Effective Date: October 28, 2025

Codectopus analyzes codebases and identifies the areas most likely to cause bugs, instability, and maintenance issues. It provides a prioritized refactoring plan for engineering teams while ensuring full control and security of the customer’s source code. Codectopus never stores source code, only lightweight analysis metadata.

1. What We Access

- Repository contents via GitHub API using OAuth authentication
- Code access is strictly limited to generating analysis, reviews, and documentation
- You control exactly which repositories we can access through GitHub's permission system
- We never write, modify, or delete any of your code

2. What We Store

- We never store your source code. Only metadata and analysis summaries are retained.
- Repository names, file paths, commit hashes, and basic file statistics
- Analysis results including metrics, issue flags, and generated documentation
- Dashboard settings, notification preferences, and account information

3. Processing Model

- Your code is never used to train any AI models. All processing is temporary and ephemeral.
- Code is loaded into memory, analyzed, and immediately discarded
- AI models see only the minimum necessary code snippets required for analysis
- All processing occurs in secure, isolated environments that are destroyed after use
- No caching or temporary snippet storage between sessions

4. Infrastructure

- Metadata and analysis results encrypted at rest using AES-256
- Secure authentication through GitHub OAuth
- Encrypted access tokens with automatic rotation
- TLS 1.3 for all data in transit
- Hosted on enterprise-grade cloud infrastructure with SOC 2 compliance
- Processing environments isolated from public networks

5. Data Retention & Deletion

- Source code is deleted from memory immediately after processing
- Metadata and analysis results retained for account lifetime
- Full data deletion within 30 days of account termination
- Immediate deletion available upon request
- Encrypted backups purged according to retention policy

6. Compliance Roadmap

- SOC 2 Type II completion target: Q2 2026
- GDPR compliant for EU customers
- CCPA compliant for US customers
- ISO 27001 certification planned for 2026
- HIPAA readiness for Enterprise plans

7. Data Retention & Deletion

- Only zero-retention AI processing partners
- Built on GitHub’s enterprise-grade security stack
- Stripe handles all payment processing (PCI-compliant)
- Third-party vendors go through security review
- DPAs in place with all data-handling providers

8. Data Retention & Deletion

- NDA signing within 1 business day
- Detailed logging and reporting options available
- Custom security controls available for industry-specific needs

Security Questions?

security@codectopus.com
Response time: within 24 hours.