Privacy Policy

Last updated: November 25, 2025

1. Introduction

This Privacy Policy explains how **Vidoc Security Lab, Inc.** ("**Vidoc**", "**we**", "**us**", or "**our**") collects, uses, and protects personal data in connection with the Vidoc Security Lab platform and related services (the "**Service**").

This Privacy Policy forms part of our **Terms of Service**. If you do not agree with this Policy, you should not use the Service.

2. Data Controller and Contact

The data controller for personal data processed in connection with the Service is:

> *Vidoc Security Lab, Inc.*
> *1111B S Governors Ave STE 21466, Dover, DE 19904*
> *Email: contact@vidocsecurity.com*

If you have any questions about this Policy or our data practices, you can contact us at the email address above.

3. What Data We Collect

We collect the following categories of data when you use the Service:

3.1. Account and Identity Data

- Name (if provided by your identity provider)
- Email address
- WorkOS user identifier
- Organization identifier and membership information
- Onboarding information you choose to provide (e.g. role, company size, experience)

3.2. Organization and Workspace Data

- Organization name and internal identifier
- Relationship between users and organizations (membership and roles)
- Settings and configuration associated with your organization

3.3. Codebase and Repository Data

When you connect repositories and run scans, we process:

- Repository metadata (e.g. name, owner, size, branches)
- Source code files and file paths from your repositories
- Pull request metadata (e.g. title, branch, commit SHA, PR identifier)

- Security issues identified in your code (including file path, location, severity, and category)
- Scan configuration (e.g. which branches and files are scanned)

3.4. Usage and Analytics Data

- Actions taken in the product (e.g. scans started, issues triaged)
- Number of scans and files scanned per organization
- Technical logs and telemetry (timestamps, request metadata, performance metrics)
- Limited product analytics to understand feature usage and improve the Service

3.5. Billing and Subscription Data

When you subscribe to a paid plan, we process:

- Subscription plan and status
- Basic billing metadata (e.g. organization ID, plan type, usage limits)
- Stripe customer identifier

We do **not** store full payment card numbers; these are handled by our payment processor (Stripe).

4. How We Use Your Data

We use the data described above for the following purposes:

- **To provide and operate the Service**
  - Authenticate users and organizations
  - Connect to your GitHub repositories and run code scans
  - Detect, validate, and display security issues in your codebase
  - Store and display scan history and issue states per branch and organization
- **To secure the Service**
  - Monitor for abuse, unauthorized access, and security incidents
  - Maintain audit logs where appropriate
- **To improve the Service**
  - Understand which features are used and how they perform
  - Debug issues, optimize performance, and improve user experience
- **To manage subscriptions and billing**
  - Create and manage subscriptions
  - Enforce usage limits (e.g. files scanned, number of scans)
  - Coordinate with Stripe for invoicing and payments
- **To communicate with you**
  - Send transactional messages (e.g. onboarding emails, subscription notifications, security-related updates)
  - Respond to support requests and feedback

5. AI and Model Training

- We use Artificial Intelligence (AI) and Large Language Models (LLMs) to assist with code analysis and security issue validation.
- **We do not use your Codebase, scan results, or other User Data to train or fine-tune our own or third-party AI models**, other than transient processing strictly necessary to provide the Service.
- We may log prompts and responses in a limited, access-controlled manner for debugging, safety, and abuse-prevention, but not for training standalone models on your proprietary data.

6. Legal Bases for Processing (EEA/UK)

Where applicable law (such as the GDPR or UK GDPR) requires a legal basis, we rely on:

- **Contract** – to provide the Service under our Terms of Service.
- **Legitimate interests** – to secure, maintain, and improve the Service, prevent abuse, and understand usage patterns, provided these interests are not overridden by your rights.
- **Legal obligations** – to comply with applicable laws, regulations, and lawful requests.

7. Third-Party Service Providers

We use trusted third-party providers to help us deliver the Service. These providers may process limited personal data on our behalf, subject to data protection agreements:

- **WorkOS** – authentication and single sign-on.
- **Stripe** – subscription management and payment processing.
- **GitHub** – repository integration and pull request data.
- **AI Providers** (e.g. OpenAI, Google Gemini, Azure OpenAI, VoyageAI) – code analysis and embeddings strictly for providing the Service.
- **AWS** – cloud infrastructure and storage (e.g. storing code files and scan data).
- **PlanetScale** – database hosting.
- **PostHog** – product analytics.
- **Sentry** – error and performance monitoring.

Each provider is only given the minimum data necessary to perform its function, and they are not permitted to use your data for their own independent purposes inconsistent with this Policy.

8. Data Retention

We retain personal data only for as long as necessary to:

- Provide the Service to you and your organization.
- Comply with legal, accounting, or reporting obligations.
- Resolve disputes and enforce our agreements.

In general:

- Account and organization data are retained while your organization maintains an active account and for a reasonable period thereafter.
- Code and scan data may be retained for the duration of the subscription and a limited period after termination (for backups and legal compliance), after which it may be deleted or anonymized.

You may contact us if you require more detail on specific retention periods for your organization.

9. Data Security

We implement technical and organizational measures designed to protect your data, including:

- Encryption of data in transit and at rest where appropriate (e.g. storage of code files and database records).
- Access controls and authentication to limit access to authorized personnel.
- Audit logging and monitoring for anomalous activity.

No method of transmission or storage is completely secure, and we cannot guarantee absolute security, but we aim to apply industry-standard safeguards.

10. International Data Transfers

Because we and some of our service providers are located outside the European Economic Area (EEA) and the United Kingdom, your data may be processed in countries that may not have the same level of data protection as your home jurisdiction.

Where required, we use appropriate safeguards for international transfers, such as:

- Standard Contractual Clauses approved by the European Commission, and/or
- Other lawful transfer mechanisms recognized under applicable data protection laws.

11. Your Rights

Depending on your jurisdiction and subject to certain conditions and exceptions, you may have the right to:

- Access the personal data we hold about you.
- Request correction of inaccurate or incomplete data.
- Request deletion of your personal data.
- Object to or restrict certain types of processing.
- Request a copy of your data in a portable format.
- Withdraw consent where we rely on consent (without affecting prior processing).

Requests can be made by contacting us at **contact@vidocsecurity.com**. We may need to verify your identity before fulfilling your request.

If you are located in the EEA or UK, you also have the right to lodge a complaint with your local data protection authority.

12. Children’s Privacy

The Service is not intended for use by children under the age of 16, and we do not knowingly collect personal data from children under 16. If you believe that a child has provided us with personal data, please contact us so we can take appropriate action.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. When we do, we will revise the “Last updated” date at the top of this page. If changes are material, we may provide additional notice (for example, by email or in-product notice).

Your continued use of the Service after any changes become effective will constitute your acceptance of the updated Policy.

14. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, you can contact us at:

Email: contact@vidocsecurity.com
Vidoc Security Lab, Inc.