

Pictograph Enterprise Self-Hosted Privacy Notice

Version 2026-10-02

This notice explains how Pictograph Enterprise Self-Hosted (the "**Software**") handles data, and what limited information Pictograph LLC ("**Pictograph**", "**we**") itself handles in connection with a self-hosted deployment. The short version: the Software runs entirely inside the customer's own cloud environment, everything it stores and processes stays there under the customer's control, and the Software sends nothing to Pictograph. Capitalized terms not defined here have the meanings given in the Pictograph Enterprise Self-Hosted License Terms.

1. SCOPE.

- (a) This notice applies to each deployment of the Software in a customer's own Cloud Environment. It does not apply to Pictograph's hosted service at pictograph.io and app.pictograph.io, which is covered by the Pictograph Privacy Policy.
- (b) The organization that licenses and operates the Software (the "**Customer**") is the controller of all personal data in its deployment, including any personal data in images and other content, and the account information of its users. Pictograph does not host, store, or process that data, and is not a controller, processor, or subprocessor of it.
- (c) If you use a deployment of the Software as an employee, contractor, or other user of a Customer, that Customer's own privacy notices and policies govern how your information is handled, and requests about your information should go to that Customer.

2. EVERYTHING STAYS IN THE CUSTOMER'S ENVIRONMENT.

- (a) **Storage and processing.** The Software stores its database, images, datasets, annotations, exports, trained models, and other content in services that run in the Customer's own cloud project, and performs all of its processing there, including annotation, AI-assisted annotation, embeddings and similarity search, auto-tagging, depth maps, model training, evaluation, and inference.
- (b) **Generative features.** Image generation and editing features use the AI services of the Customer's own cloud provider, in the Customer's own project and region, under the Customer's own agreement with that provider.
- (c) **Sign-in.** User sign-in uses the identity service in the Customer's project, which the Customer may connect to its own identity provider for single sign-on and multi-factor authentication.
- (d) **No training on Customer content.** Nothing in a Customer's deployment is used to train or improve Pictograph's models or any shared or foundation model. Models trained in the

deployment belong to the Customer.

3. WHAT THE SOFTWARE NEVER DOES.

The Software does not send Pictograph, or any system Pictograph operates:

- any content, images, annotations, models, or other Customer Data;
- usage information, analytics, diagnostics, crash reports, or any other telemetry;
- license checks, activation requests, or update checks.

The Software contains no advertising, no third-party tracking, and no analytics software.

4. DATA THAT LEAVES THE ENVIRONMENT ONLY IF THE CUSTOMER CONFIGURES IT.

Some features connect to services outside the Customer's cloud project. Each works only if the Customer sets it up, and sends data only to destinations the Customer chooses:

- an external identity provider the Customer connects for sign-in;
- an email delivery provider the Customer configures for notifications and invitations;
- outbound webhooks to endpoints the Customer specifies;
- any other integration the Customer builds with the Software's APIs, SDK, or exports.

The Customer is responsible for those destinations and for its agreements with their providers.

5. WHAT PICTOGRAPH ITSELF HANDLES.

(a) **Business contact information.** We handle the names, work email addresses, and other business contact details of Customer and reseller personnel that we receive when contracting, implementing, and communicating about the Software, and the content of those communications. We use them to perform and administer the engagement, and we handle them under the Pictograph Privacy Policy.

(b) **Implementation and support access.** When a Customer, or its Authorized Reseller acting for the Customer, grants Pictograph personnel access to its cloud project to deploy, verify, or support the Software, that access is through the Customer's own access controls, limited to the work requested, and revocable by the Customer at any time. We use it only for that work, we do not copy Customer Data out of the Customer's environment except as the Customer directs in writing, and anything we see is confidential under the License Terms.

(c) **License records.** We keep records of which organizations hold licenses, their designated cloud environments, and the Releases delivered to them, to administer licenses and our agreements with resellers.

(d) **Our websites.** Visits to pictograph.io, including the pages that publish this notice and the License Terms, are covered by the Pictograph Privacy Policy.

6. THE CUSTOMER'S RESPONSIBILITIES AS CONTROLLER.

Because the Customer controls its deployment and the data in it, the Customer is responsible for: giving any notices and obtaining any consents required for the data it processes, including for people depicted in images and under biometric and privacy laws; responding to requests from individuals to access, correct, export, or delete their information, which the Software's delete and export features support; setting retention and deletion for its databases, storage, backups, and logs; configuring security for its deployment and cloud project; and meeting any breach notification and other legal obligations that apply to its environment.

7. SECURITY CAPABILITIES OF THE SOFTWARE.

The Software is built to support a secure deployment, including: encryption in transit using TLS; encryption at rest provided by the Customer's cloud provider, with support for customer-managed encryption keys; application-level authenticated encryption of stored secrets; role-based access control; separation of data between organizations within a deployment; and hashed API keys. The Customer configures and operates these capabilities in its environment, together with the security controls its cloud provider offers. Pictograph does not warrant that any deployment will be free from unauthorized access.

8. SECURITY VULNERABILITIES.

If Pictograph learns of a security vulnerability in a delivered Release, Pictograph will use reasonable efforts to inform the Customer's Authorized Reseller, or the Customer directly, so that it can be addressed.

9. WHEN USE ENDS.

Because Customer Data never leaves the Customer's environment, the Customer deletes its data by deleting it within the Software or by deleting the cloud resources and projects that hold it. Pictograph holds no Customer Data to delete. When implementation or support work ends, Pictograph deletes any credentials and materials it received for that work.

10. VERSIONS AND CHANGES.

This notice is identified by version. This is Version 2026-10-02. Pictograph may publish new versions, and prior versions remain available, including as a downloadable copy at pictograph.io/privacy/self-hosted. A new version will not reduce the protections in the version that applied when a Customer's license began without that Customer's written agreement.

11. CONTACT.

Questions about this notice or the Software's data handling can be sent to support@pictograph.io. Questions about how a particular deployment handles your information should go to the organization that operates it.