

PROBE PRIVACY POLICY

Last updated: August 21, 2026 | Effective date: August 21, 2026

Probe, Corp. (“Probe,” “we,” “us,” or “our”) provides Probe Research, a platform that helps AI/ML teams track experiments and organize research knowledge. This Privacy Policy explains how Probe collects, uses, shares, retains, and protects personal data and Customer Data when you use Probe Research, our websites, hosted software, APIs, clients, and support (together, the “Service”).

1. SUMMARY

- We do not sell personal data or use Customer Data for targeted advertising.
- Your organization owns and controls the research content it puts into Probe.
- Probe uses PostHog for product analytics and Resend for account and service email.
- Probe does not use Customer Data to train a general-purpose Probe model.

2. SCOPE AND ROLES

This policy covers Probe Research, our websites, hosted software, APIs, clients, and support. It does not govern a customer's own privacy practices or a self-hosted deployment that Probe does not operate.

Probe is a controller for account, website, support, and business-administration data. For Customer Data submitted to the Service by an organization, that organization is the controller and Probe acts as its processor or service provider. If a signed data processing agreement conflicts with this policy, the data processing agreement controls.

3. DATA WE COLLECT

Account and team data

Name, email, Google profile, team membership, invitations, and workspace names. **Source:** you, your team, and Google Sign-In. **Purpose:** create accounts, authenticate people, administer teams, and provide support.

Customer Data

Projects, experiments, runs, configurations, metrics, logs, traces, prompts, assistant conversations, tool activity, files, artifacts, checkpoints, and linked source-control or experiment data. **Source:** you, your team, Probe clients, and integrations you connect. **Purpose:** provide, secure, search, summarize, and troubleshoot the Service at your direction.

Product and device data

Pages and features used, browser and device details, IP address, API or client surface, client version, service events, and error or crash reports sent by Probe clients, which may include stack traces and related technical context from your environment. **Source:** your browser, Probe clients, our servers, and PostHog. **Purpose:** operate, secure, debug, and improve the Service, and understand feature use.

Integration data

Installation identifiers, repository metadata, imported run data, and tokens or grants needed to keep a connection working. **Source:** GitHub, Weights & Biases, and other integrations you choose. **Purpose:** run the connection you or your team requested.

Communications

Support messages, feedback, invitation delivery, and related email metadata. **Source:** you, your team, and Resend. **Purpose:** answer requests and send account or service messages.

Customer Data can contain personal or sensitive information chosen by a customer. Do not submit data that your organization is not permitted to process or share with Probe.

AI-powered features may process relevant content through third-party service providers.

4. HOW WE USE DATA

We use the data described above to:

- provide, authenticate, maintain, and support the Service;
- process Customer Data under a customer's instructions;
- secure the Service, prevent abuse, and investigate errors;
- measure product use and improve reliability and usability;
- send account, invitation, support, and service messages; and
- meet legal obligations and enforce agreements.

Where applicable law requires a legal basis, we rely on performance of a contract, our legitimate interests in operating and securing the Service, your consent, and compliance with legal obligations.

Aggregated and de-identified data. We may create aggregated or de-identified data by removing information that identifies you or your organization. We do not attempt to re-identify de-identified data, except to test that our de-identification process complies with applicable law. We may use and share aggregated or de-identified data for lawful business purposes, including analyzing and improving the Service.

5. AI FEATURES

Probe may use third-party service providers to support AI-powered features. Some features are initiated by users, while others may operate automatically as part of the Service. To provide these features, Probe may send providers Customer Data and related instructions reasonably necessary for the relevant processing.

Probe does not use Customer Data to train a general-purpose Probe model. Third-party providers process information under Probe's applicable account settings and agreements. AI outputs may contain inaccuracies; you are responsible for evaluating outputs before relying on them.

6. COOKIES AND ANALYTICS

Probe uses cookies for sign-in, session security, and requested settings. Probe also uses PostHog analytics, which sets its own cookies and runs by default, to understand page views, feature use, client versions, and service events, including on publicly shared pages. PostHog may receive account, device, usage, and limited service data. Probe does not use this data for third-party advertising.

Browser or device settings can block or limit cookies, but blocking sign-in and security cookies may prevent you from using the Service.

7. HOW WE SHARE DATA

We disclose data only:

- to the service providers listed in the Subprocessors section below;
- to integrations a customer chooses and directs us to connect;
- to professional advisors, such as lawyers, auditors, and insurers, in the course of their services to us;
- to comply with law and valid legal process, or to protect rights and safety; and
- as part of a financing, acquisition, reorganization, or sale of all or part of our business, subject to law.

We do not sell personal data and do not share it for cross-context behavioral advertising.

8. RETENTION AND DELETION

We retain data as follows:

Data	Retention standard
Account data	For the account term, then deleted within 30 days after closure.

Customer Data	For the service term, then deleted within 30 days after a valid deletion request or contract end.
Server and security logs	For a limited period needed to operate, secure, and debug the Service, or longer to investigate abuse or meet legal requirements.
Identified product analytics	12 months, or earlier when the associated account is deleted.
Database backups	A rolling 7-day recovery window.
Billing and tax records	Up to 7 years after paid billing begins, where law requires it.

Deleting your account removes your account and private account data; it does not delete your team's research. If the sole owner of a team deletes their account, the team and its research are also deleted. Deleted data may persist in encrypted backups for the backup window above and in residual or de-identified records, such as provenance and import history, and copies in storage and search systems are removed as deletion completes. Legal holds, fraud prevention, disputes, and required records may delay deletion.

9. SECURITY

Probe uses technical and organizational safeguards designed for the nature of the data we handle, including encrypted network transport, provider storage encryption, tenant isolation, scoped credentials, and access controls. No system is perfectly secure, and we cannot guarantee that unauthorized access will never occur.

10. OTHER SITES AND SERVICES

The Service may contain links to websites and online services operated by third parties, and content from the Service may be integrated into pages that are not associated with us. These links and integrations are not an endorsement of any third party. We do not control third-party sites and services and are not responsible for their actions. We encourage you to read the privacy policies of the other sites and services you use.

11. INTERNATIONAL TRANSFERS

Probe's hosted Service is operated primarily in the United States. Our providers may process data in the United States and other countries, where privacy laws may differ from those in your jurisdiction. Where required, Probe uses a recognized transfer mechanism, such as the standard contractual clauses, in the applicable data processing agreement.

12. YOUR RIGHTS AND CHOICES

Depending on where you live, you may have rights to access, correct, delete, restrict, object to, or receive a copy of personal data, withdraw consent, or complain to a privacy regulator. If Probe handles the data for your organization, send the request to that organization first; we will help it respond as required by our agreement and law.

To make a request, email founders@prbe.ai. We may need to verify your identity and authority before acting. If we decline a request, you may appeal by replying to our response. You may also use an authorized agent where the law allows; we may verify the agent's authority.

You can review and update account information by signing in to your account, and you can opt out of non-essential emails using the unsubscribe link in the message. Service and account messages will continue while you hold an account.

13. US STATE PRIVACY RIGHTS

This section applies to residents of US states with privacy laws that apply to Probe ("State Privacy Laws"), including California. Section 3 describes the categories of personal information we collect, their sources, and our business purposes. Section 7 and the Subprocessors section describe the categories of recipients.

Probe does not sell personal information, does not share it for cross-context behavioral advertising, does not use it for profiling that produces legal or similarly significant effects, and does not offer financial incentives in exchange

for personal data. Because we do not sell or share personal information within the meaning of the State Privacy Laws, no opt-out is needed.

Subject to the State Privacy Laws, you may request information about our collection and use of your personal information, access a copy of it, correct it, delete it, or receive it in a portable format, and you may appeal a denial. We will not discriminate against you for exercising a privacy right. Submit requests to founders@prbe.ai.

California Shine the Light. Under California Civil Code Section 1798.83, California residents with whom we have a business relationship primarily for personal, family, or household purposes may request the names of third parties to which we disclosed certain personal information for those parties' own direct marketing purposes during the preceding calendar year. Probe does not disclose personal information to third parties for their own direct marketing purposes. California residents may confirm this or make a request by emailing founders@prbe.ai with the subject "Shine the Light Request."

Nevada residents. Nevada residents have the right to opt out of the sale of certain personal information for monetary consideration. Probe does not engage in such sales. Nevada residents who would like to opt out of any potential future sale may email founders@prbe.ai.

14. USERS IN THE EEA AND UK

If you are located in the European Economic Area or the United Kingdom, the legal bases described in Section 4 apply to our processing, and the transfer safeguards in Section 11 apply to transfers outside Europe. You have the rights described in Section 12, including the rights to access, rectify, erase, restrict, and port personal data, to object to processing based on legitimate interests, and to withdraw consent at any time without affecting prior processing. You may also lodge a complaint with your local supervisory authority or, in the UK, the Information Commissioner's Office.

15. CHILDREN

Probe is a business service and is not directed to children under 16. We do not knowingly collect personal data from children under 16. Contact us if you believe a child submitted personal data to Probe, and we will delete it as required by law.

16. CHANGES TO THIS POLICY

We may update this policy as our Service or legal obligations change. We will update the date above and provide additional notice when a change is material. Prior versions are available on request.

17. CONTACT

Privacy questions and requests: founders@prbe.ai

Legal entity: Probe, Corp.

Postal address: 1395 22nd Street, Apt 209, San Francisco, CA 94107

SUBPROCESSORS

A subprocessor is a service provider that may process Customer Data for Probe while Probe provides the hosted Service. Probe remains responsible for selecting and instructing its subprocessors as required by the applicable customer agreement.

Provider	Role and data	Location
DigitalOcean	Cloud computing, networking, Kubernetes, and database infrastructure. May receive account data, Customer Data, and service data.	United States
Vercel	Dashboard hosting and request proxying. Browser requests to the Service pass through Vercel, which may receive session data, Customer Data in transit, and network data.	United States

Cloudflare	Object storage, queues, DNS, content delivery, and network protection. May receive customer files, artifacts, request data, and network data.	US and other Cloudflare locations
Google	Google Sign-In, AI processing, and business productivity services. May receive account data and Customer Data as needed to provide the Service.	US and other Google locations
Cerebras Systems	AI processing. May receive Customer Data as needed to provide AI-powered features.	United States
Fireworks AI	AI processing. May receive Customer Data as needed to provide AI-powered features.	United States
Firecrawl	Web and paper search and page retrieval. May receive search queries, which can include research content, and URLs to retrieve.	United States
PostHog	Product analytics, feature flags, and diagnostics. May receive account, device, usage, and limited service data.	United States
Resend	Account and transactional email. May receive name, email address, message content, and delivery metadata.	United States

Customer-directed integrations. GitHub and Weights & Biases are available only when a customer chooses to connect them. Those providers process data under the customer's own account and instructions and are not used for every Probe customer.

The table above is the current subprocessor list. We will update this policy before a new subprocessor receives Customer Data.