

PerfCopilot Privacy Policy

• Last updated: 2026-06-08

1. Overview & who we are

This Privacy Policy explains how **NSD LLC, operating as “PerfCopilot”** (“PerfCopilot,” “we,” “us”), handles personal data in connection with our website, application, and services (the “Service”).

Our role depends on the data:

- **As a processor.** For the work signals and employee information a customer connects to run performance reviews, the customer (your employer or organization) is the controller and decides why and how that data is used. We process it on the customer's behalf under our Terms and Data Processing Addendum.
- **As a controller.** For account registration data, billing, support, and website/marketing analytics, we determine the purposes and are the controller.

2. Information we collect

- **Account data.** Name, work email, organization, role, and authentication data for users we provision.
- **Work-signal metadata.** From the integrations a customer connects: pull-request titles and review participation, ticket and goal statuses, channel activity counts, email and call *metadata* (sender/recipient/timestamps), attendance events, and similar productivity signals.
- **Review content.** Peer feedback, manager notes, ratings, and the AI-generated and edited review drafts produced for the organization.
- **Billing data.** Handled by our payment processor (Stripe); we receive plan, seat count, and status, not full card numbers.
- **Usage & device data.** Log data, IP address, and product analytics needed to operate, secure, and improve the Service.

3. What we don't collect

We never read message bodies, email contents, subject lines, or document text.

Email and chat are processed as metadata only. We do not fingerprint users, we do not sell personal data, and we do not use customer data to train AI models.

4. How we use information

- Provide, operate, secure, and support the Service, including generating and delivering review drafts.
- Process payments and manage subscriptions.
- Communicate with you about your account, security, and changes to the Service.
- Improve the Service using aggregated, de-identified usage data that does not identify any individual or organization.
- Comply with law and enforce our Terms.

5. AI processing

Review drafts are generated using third-party model providers (currently Anthropic's Claude, OpenAI's GPT, or Google's Gemini APIs; we may route to any of them). Each request sends only the signals relevant to the active review: no historical context and no cross-organization data. **We do not permit our model providers to use your data, in any form, to train or improve their models.** AI output is decision support that a manager reviews and edits before use.

6. OAuth tokens & security

Integration credentials and OAuth tokens are encrypted at rest (Fernet symmetric encryption); the key resides only on the application server, tokens are decrypted in memory at request time, and they are never logged. We maintain administrative, technical, and organizational security measures appropriate to the Service; see our [Security](#) page for details.

7. Customer-facing call analysis (opt-in)

For roles where the conversation is the work (for example sales, customer success, advisory, or property management), an organization can optionally enable analysis of customer-facing call transcripts. **We never record calls.** We only consume transcripts your phone or meeting provider already produced. Supported providers: Aircall, Microsoft Teams, Zoom, and Gong.

Internal team meetings are never analyzed. For Teams and Zoom we automatically skip any meeting where every attendee shares your organization's email domain; only meetings with at least one external participant are eligible. Enabling requires an explicit admin consent attestation, can be turned off at any time, and per-call data can be deleted from the admin console.

8. Sub-processors

We use a small set of vetted sub-processors to deliver the Service:

- **Anthropic:** AI review generation (Claude API).
- **OpenAI:** AI review generation (GPT API), used as an alternative model provider.
- **Google:** AI review generation (Gemini API), used as an alternative model provider.
- **Stripe:** billing and payments.
- **Resend:** transactional email delivery.
- **Sentry:** error monitoring, with PII scrubbing enabled.
- **PostHog:** first-party product and website analytics.
- **European cloud hosting provider:** application and database hosting.

We require each sub-processor to protect personal data consistent with this policy. An up-to-date list is available on request, and customers under a DPA receive notice of material changes.

9. Where data lives & international transfers

Application servers and databases are hosted in Europe, and backups are encrypted and rotated on a 30-day schedule. Some sub-processors (for example email delivery) operate in the United States. Where personal data is transferred internationally, we rely on appropriate safeguards such as the European Commission's Standard Contractual Clauses.

10. Legal bases (EEA/UK)

Where the GDPR or UK GDPR applies and we act as a controller, we process personal data on the bases of: performance of a contract (providing the Service you requested), our legitimate interests (operating, securing, and improving the Service), compliance with legal obligations, and consent where required (for example certain analytics). Where we act as a processor, we process on the documented instructions of the customer (controller).

11. Data retention

We retain personal data for as long as needed to provide the Service and for legitimate business or legal purposes. On account closure or request, we delete or de-identify Customer Content within 30 days, after which residual copies expire on the normal encrypted-backup rotation. We may retain limited records (for example billing) where required by law.

12. Your privacy rights

Depending on where you live, you may have the right to access, correct, delete, port, or restrict the processing of your personal data, to object to certain processing, and to withdraw consent. California residents have rights under the CCPA/CPRA, including to know, delete, correct, and opt out of “sale” or “sharing” (we do not sell or share personal data as those terms are defined). We will not discriminate against you for exercising these rights.

To exercise a right, email privacy@perfcopilot.com from your account address. We verify requests before acting and respond within the timeframes required by law. If we process your data on behalf of your employer, we will route your request to them.

13. Employee & end-user data

Much of the data in PerfCopilot is about a customer's employees, processed on the customer's instructions. If you are an employee of an organization that uses PerfCopilot and want to access, correct, or delete your data, please contact your employer (the controller); we will support them in responding.

14. Cookies & analytics

The marketing site uses PostHog for first-party analytics (page views and CTA clicks) and a small number of cookies needed for the site to function and for these analytics. We do not use cross-site advertising trackers, and we respect your browser's Do Not Track / Global Privacy Control signal.

15. Children

The Service is a workplace tool intended for business use and is not directed to children. We do not knowingly collect personal data from anyone under 16.

16. Changes to this policy

We may update this policy from time to time. For material changes we will provide notice (for example in-app or by email) and update the “Last updated” date above. Continued use of the Service after a change takes effect constitutes acceptance.

Contact

Privacy questions or requests: privacy@perfcopilot.com. Legal notices: legal@perfcopilot.com. Or [get in touch](#).