

Peppr Privacy Policy

Last updated: July 15, 2026

This Privacy Policy explains how Peppr AI Inc. (“Peppr,” “we,” “us,” or “our”) collects, uses, discloses, and protects information in connection with the Peppr real-time in-call sales intelligence platform and related applications, the website at usepeppr.ai, and related services (together, the “Service”).

We’ve written this to be read by the people who evaluate us - security, privacy, and procurement teams at the enterprises we serve. Where our practices differ between deployment models, we say so directly rather than describing a single averaged version.

1. Who this policy covers

Peppr provides its Service to businesses (each, a “Customer”). The people who use Peppr - sales representatives, sales engineers, enablement staff, and administrators at a Customer - are “Users.”

- **For Customers and Users:** this policy describes how we handle information processed through the Service.
- **For website visitors:** Sections 3, 8, 9, and 11 describe how we handle information collected through usepeppr.ai.

Where a Customer deploys Peppr and controls the underlying data, that Customer is the controller of the personal data processed in their instance, and Peppr acts as a processor that handles that data on the Customer’s behalf and under their instructions. This policy describes our own practices; it does not override the agreement between Peppr and a Customer, which governs in the event of any conflict.

2. The two deployment models - and why they matter here

How much we can see depends entirely on how a Customer runs Peppr. This is the most important distinction in this policy.

Cloud (hosted) deployment. Peppr operates the Service in our managed environment. In this model, Customer content and operational data pass through infrastructure we operate, and the practices described throughout this policy apply.

In-environment / on-premise deployment (BYOC). Peppr is deployed as a single-tenant instance inside the Customer’s own cloud tenant or on-premise infrastructure. In this model, Customer content and operational data remain inside the Customer’s environment, and Peppr does not have standing access to it. We do not receive, store, or monitor that data by default. If we need specific information - for example, to help diagnose an issue - we request it from the Customer’s designated administrator (the person managing the deployment), who decides what, if anything, to share. Nothing leaves the Customer’s environment unless the Customer affirmatively provides it.

3. Information we process

a. Customer content

To do its job, Peppr processes the content of the sales conversations and knowledge it is connected to. Depending on configuration, this can include:

- Live call audio captured on the User's device and the transcripts derived from it;
- The questions detected during a call and the answers surfaced in response;
- Content drawn from the knowledge sources a Customer connects (for example CRM records, documents, wikis, and messaging tools) for the purpose of grounding answers;
- Post-call analysis, notes, action items, and knowledge-gap records generated by the Service.

Customer content is processed to provide the Service to that Customer. Where a Customer configures call data to be discarded after a call, we honor that configuration.

b. Account and administrative data

Names, business email addresses, role, and authentication and configuration settings for Users and administrators.

c. Usage and operational data

We also process data about how the Service itself is functioning and being used. We want to be direct about this rather than bury it: we collect product-analytics and telemetry data - records of feature usage, events, performance metrics, error and diagnostic logs, and similar operational signals - and our engineering team can access this data to operate, debug, and improve the Service.

Some of this usage data is associated with an identifiable Customer (and, in some cases, with an individual User account) rather than being fully aggregated or anonymized. We access it primarily to diagnose and fix problems, keep the Service reliable, and improve how it works.

Your control over this. A Customer may request that we anonymize or de-identify the usage data associated with their account, and we will do so for that Customer going forward in accordance with their agreement with us. To arrange this, contact support@usepeppr.ai or your Peppr account contact.

In on-premise (BYOC) deployments, the usage and operational data described in this section stays within the Customer's environment and is not available to us unless the Customer's administrator provides it to us on request (see Section 2).

d. Website data

When you visit usepeppr.ai we collect standard web analytics (such as IP address, device and browser information, and pages viewed) and any information you submit through forms. See Section 8 for cookies.

4. How we use information

We use the information described above to:

- Provide, operate, and secure the Service and surface grounded answers and guidance during calls;
- Generate post-call analysis, coaching signals, and knowledge-gap routing;
- **Debug, troubleshoot, and diagnose issues** - the primary purpose for which we access identifiable usage data;

- Monitor performance, reliability, and capacity, and improve the Service;
- Provide customer support and communicate about the Service;
- Meet legal, security, and compliance obligations; and
- Prevent fraud, abuse, and misuse.

We do not sell personal data, and we do not use Customer content or Customer-identifiable usage data to serve third-party advertising.

5. Model processing, and how your content is (and isn't) used

Peppr uses AI models to transcribe conversations, detect questions, and generate answers grounded in a Customer's connected knowledge. What this involves - and where the data goes - depends on the deployment model, so we describe each directly.

- **No cross-customer training.** We do not use one Customer's content, transcripts, or AI outputs to train, tune, or improve any model or instance made available to any other Customer. Each deployment is grounded only on the knowledge that Customer connects, for that Customer's instance alone.
- **In-environment / on-premise (BYOC) deployments.** Customers connect Peppr to their own model endpoints - they bring their own models. Customer content and AI outputs never leave the Customer's environment or reach Peppr-controlled infrastructure, so Peppr has no ability to retain, train on, or improve any model from them. The retention and data-use terms that govern inference are those of the Customer's own agreement with the model provider it chooses to connect.
- **Hosted (cloud) deployments.** Transcription and answer generation are performed by subprocessors Peppr engages to operate the Service (see Section 7), under contractual data-protection terms. Retention and data-use terms depend on the provider and are set out in the applicable order form or data processing addendum. Customers with strict zero-retention requirements can meet them through an in-environment (BYOC) deployment.

6. How long we keep information

- **Customer content:** retained for as long as needed to provide the Service, and per the Customer's configuration and agreement. Live call audio is streamed for transcription and is not stored by our backend; where call data is set to be discarded after a call, it is not retained beyond that.
- **Account data:** retained for the life of the account and for a reasonable period afterward as needed for legal, tax, and security purposes.
- **Usage and operational data:** retained for as long as needed for debugging, security, reliability, and service-improvement purposes, and then deleted or de-identified.

Specific retention periods can be set out in a Customer's agreement or data processing addendum.

7. Who we share information with

We share information only as needed to run the Service:

- **Subprocessors** - vetted vendors that provide infrastructure, transcription, model/inference, analytics, and support services on our behalf, under contractual data-protection obligations. A current list of subprocessors is available on request at support@usepepr.ai.
- **Within a Customer's organization** - the Service surfaces information to Users consistent with the access controls the Customer configures; a User sees only what they are entitled to see.
- **Legal and safety** - where required by law or legal process, or to protect the rights, safety, and security of Peppr, our Customers, or others.
- **Business transfers** - in connection with a merger, acquisition, or sale of assets, subject to this policy.

We do not share Customer content or Customer-identifiable usage data with third parties for their own purposes.

8. Cookies and website analytics

Our website uses cookies and similar technologies for functionality and analytics. You can control cookies through your browser settings.

9. Security

We maintain administrative, technical, and physical safeguards designed to protect information. Peppr has completed a SOC 2 Type I audit and is currently undergoing a SOC 2 Type II audit. In deployments that use a Customer's own environment and access controls, the Service inherits those controls. No method of transmission or storage is completely secure, and we cannot guarantee absolute security.

10. Your rights and choices

Depending on your location and role, you or your organization may have rights to access, correct, delete, export, or restrict the processing of personal data, and to request anonymization of usage data as described in Section 3(c).

- **Users:** because a Customer typically controls the data in their instance, please direct requests to your organization's Peppr administrator. We will support Customers in responding.
- **Customers and others:** contact support@usepepr.ai.

We will not discriminate against you for exercising these rights.

11. International data transfers

Where information is transferred across borders in cloud deployments, we use appropriate safeguards such as standard contractual clauses. In-environment deployments keep data within the Customer's chosen region and infrastructure.

12. Children

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

13. Changes to this policy

We may update this policy from time to time. We will post the updated version with a new effective date and, for material changes, provide notice as required.

14. Contact us

Peppr AI Inc.

Legal: support@usepeppr.ai

Mailing address: 11572 Seven Springs Dr, Cupertino, 95014, CA, United States