

PRIVACY POLICY

Last modified: September 8, 2025

Open Vision Engineering, Inc., a Delaware corporation (the “**Company**”, “**we**”, “**us**”, or “**our**”) respects your privacy and is committed to protecting it. This Privacy Policy (this “**Policy**”) describes the categories of information we collect, the purposes for which we use it, the parties with whom we disclose it, and the choices available to you.

This Policy applies to your use of (i) <https://heypocket.com> (the “**Website**”), (ii) our mobile and desktop software applications (the “**Apps**”), (iii) the Pocket hardware recording device (the “**Pocket Device**”), and (iv) all related content, functionality, and services we provide (collectively with the Website and Apps, the “**Services**”). Capitalized terms not defined herein have the meanings set forth in our Terms of Use and Terms of Sale, which are incorporated by reference.

By accessing or using any part of the Services, you acknowledge that you have read and understand this Policy. If you do not agree, you must not use the Services.

Scope of this Policy

This Policy covers information we collect: (i) on the Website; (ii) through the Apps; (iii) from the Pocket Device and related cloud features (including when data syncs after offline use); (iv) in email, text, in-app messages, and other electronic communications between you and the Company; and (v) when you interact with our content or ads on third-party services that link to this Policy.

It does not apply to offline collection or to third-party services we do not control. We may update this Policy as described in Changes to Our Privacy Policy Section; continued use means you accept the revised Policy.

Children Under the Age of 13

The Services are intended for individuals 13 years of age or older. We do not knowingly collect personal information from children under 13. If we learn that we have collected personal information from a child under 18, we will delete it.

Categories of Personal Information We Collect

We collect several types of information from and about users of the Services, including:

- Identifiers and contact information. Name, email address, mailing/shipping address, phone number, Account credentials, and unique user IDs.
- Account and profile data. Preferences, settings, saved prompts/templates, tags, labels, and other profile details you choose to add.

- Forms and requests. Information provided via forms on the Website or Apps (e.g., product inquiries, waitlists, beta sign-ups, feature requests).
- Commercial information. Order history and purchase details (product, price, date, fulfillment status), return/exchange information, and limited tax/shipping details.
- Payment information. Payment method type and last-four digits, payment tokens, and billing address. We do not store full credit card numbers; our third-party payment processors collect and process that data on our behalf.
- User Content. Audio recordings captured with the Pocket Device or Apps (the “**Recordings**”), related transcripts, summaries, mind maps, widgets, prompts, and other AI-enabled outputs you generate (together, “**User Content**”).
- Device, app, and network data. Log files, IP address, device and browser type, operating system, app version, device identifiers, mobile advertising identifiers, crash/diagnostic data, and in-app events.
- Usage data. Pages viewed, features used, time and date stamps, referral/exit pages, and interaction data across the Services.
- Approximate location. General location derived from IP address (we do not collect precise geolocation unless you explicitly enable a feature that requires it).
- Communications. Messages you send to us (support requests, feedback, email correspondence, surveys) and your marketing preferences.
- Inferences. Inferences we derive from other data (e.g., preferences or feature interests) to improve and personalize the Services.
- Aggregated or de-identified data. We may create or receive aggregated statistics that no longer identify you; we may use such data for lawful purposes.

Note on microphones and background capture. The Apps and the Pocket Device access the microphone only when you start a recording or enable a feature that explicitly requires it. We do not continuously record by default.

How We Collect Information

We collect information:

- Directly from you. For example, when you create an Account, make a purchase, initiate a Recording, generate a User Content, contact support, or participate in surveys or promotions.
- Automatically. As you use the Services, via cookies, SDKs, pixels, log files, and similar technologies. This includes device/app/network data and usage data.
- From the Pocket Device. When you use the Pocket Device, we collect operational data needed to capture, store, and sync your Recordings, User Content, and related metadata and the provided Services. Audio is captured only when you activate recording and can be used offline; data syncs when you reconnect.

- From service providers and partners. For example, payment processors (billing), analytics providers (metrics), cloud/AI vendors (transcription and model processing), fraud prevention, logistics, and customer support tools.

Sensitive Information. If you choose to record or otherwise include sensitive information (for example, health details) in a User Content, you direct us to process that information as part of the Services.

You are responsible for obtaining any consents from third parties whose voices or information are captured (see Consent to Record Others in the Terms of Use). For clarity, “sensitive information” here is used in the everyday sense and not necessarily as defined under any specific privacy statute unless expressly stated.

Information we collect through automatic data collection technologies

As you use the Services (the Website, Apps, and Pocket Device), we and our service providers may automatically collect certain information about your devices and interactions, including:

- Usage details: pages/screens viewed, clicks, feature use, session duration, referring/exit pages, timestamps, and in-app events.
- Device, app, and network data: IP address, browser type, operating system, device model, language, app version, device and advertising identifiers, crash/diagnostic logs, and push notification tokens (if enabled).
- Approximate location: derived from IP address (we do not collect precise geolocation unless you explicitly enable a feature that requires it).
- Pocket Device telemetry: firmware version, device identifiers, basic operational metrics, and sync timestamps needed to capture, store, and transmit Recordings, User Content, and metadata. Audio is captured only when you start a recording.

We may associate or link automatically collected data with other information we hold about you. Where this data identifies you or is reasonably linkable to you, we treat it as personal information.

How We Use Your Information

We use information we collect about you or that you provide to us (including personal information) to:

- Provide and operate the Services, including capturing, storing, syncing, and making available audio recordings you initiate with the Pocket Device, generating transcripts and AI-enabled outputs (e.g., summaries, prompts, mind maps, widgets), and providing customer support.
- Process transactions and manage accounts, including billing, payment processing, order fulfillment, shipping, refunds, fraud monitoring, and authentication.
- Maintain, secure, and debug the Services; detect, prevent, and address security incidents, abuse, and violations of our Terms of Use.
- Personalize and improve the Services, content, and features; remember preferences; measure performance and usage.

- Communicate with you about the Services (e.g., confirmations, technical notices, security alerts, administrative messages), and-where permitted by law-send marketing or promotional communications (you can opt out at any time).
- Conduct research and development to improve and develop new features, models, and offerings (we will not use your personal Recordings to train our models without your consent).
- Comply with legal obligations and enforce our agreements, including our Terms of Use and Terms of Sale.
- Fulfill any other purpose disclosed at the time of collection or with your consent.

Advertising and measurement. Where permitted by law and subject to your choices, we may use information (e.g., device or cookie identifiers, generalized location, usage data) to provide, measure, and improve interest-based advertising and marketing. We do not disclose information that directly identifies you (like your name or email) to advertisers without your consent. If you interact with an ad, the advertiser may infer you fit certain criteria.

Legal bases (EEA/UK where applicable). We process personal information as needed to perform a contract (provide the Services), with your consent (e.g., certain marketing, cookies, or model training), to pursue legitimate interests (e.g., security, improvement, analytics), and to comply with legal obligations.

How we use automatically collected data

We use it to: (i) operate, secure, and debug the Services; (ii) authenticate users and prevent fraud/abuse; (iii) measure performance and usage; (iv) personalize and improve features and content; (v) remember your preferences; and (vi) (with consent where required by law) provide and measure marketing.

The technologies we use for automatic data collection may include:

- Cookies (browser cookies). Small files placed on your device that enable core functionality (e.g., sign-in, security) and, where enabled, preferences, analytics, and advertising. You can set your browser to refuse cookies or alert you when cookies are set. Some parts of the Services may not function properly without certain cookies.
- Local storage. Browser/app storage used to remember settings and improve load times.
- Pixels/Web beacons. Tiny graphics/code used in the Website, Apps, and emails to understand usage (e.g., whether an email was opened) and to measure campaign effectiveness.
- SDKs and mobile identifiers. In-app software components that provide analytics, crash reporting, push notifications, and (if enabled) marketing measurement.
- Log files. Server and application logs that record events and errors for security and diagnostics.

Do Not Track / Global Privacy Control. Your browser may offer “Do Not Track” (DNT) or Global Privacy Control (GPC) signals. Our Services do not respond to DNT signals, and we will honor Global Privacy Control (GPC) signals where required by applicable law.

Choices About How We Use and Disclose Your Information

We provide controls over how your information is used. In addition to the options described in Information We Collect Through Automatic Data Collection Technologies and in the Electronic Communications; Marketing section of our Terms of Use, you can:

- **Cookie/SDK Preferences.** Manage non-essential cookies/SDKs via our cookie banner or settings and your browser/device controls. We honor Global Privacy Control (GPC) where required by law. (We do not currently respond to “Do Not Track” signals.)
- **Interest-Based Advertising.** Adjust cookie/SDK preferences and your mobile ad-identifier settings (e.g., “Limit Ad Tracking”/”Opt out of Ads Personalization”).
- **Marketing Communications.** Opt out of marketing emails via the unsubscribe link or by contacting us; service (transactional/security) messages will continue.
- **Push Notifications & In-App Messages.** Disable in your device or in-app settings.
- **Permissions** (e.g. Bluetooth/Microphone/Location). Control OS-level permissions for the Apps/Pocket Device; revoking permissions may limit functionality.
- **Third-Party Integrations.** Disconnect integrations (e.g., cloud storage) in your Account; future sharing stops, but copies already held by that third party remain subject to their policies.

Disclosure of Your Information

We may disclose aggregated or de-identified information without restriction. We disclose personal information as described below:

- **Service providers/Processors.** To vendors that host, process, or support the Services (e.g., cloud hosting, storage, transcription/AI processing, analytics, crash reporting, communications, customer support, payment processing, shipping/fulfillment). These parties are contractually required to use personal information only to provide services to us and to protect it.
- **Affiliates.** To our subsidiaries and affiliates for purposes consistent with this policy.
- **Professional advisors & insurers.** To auditors, lawyers, accountants, and insurers under confidentiality obligations.
- **Business transfers.** In connection with, or during negotiations of, any merger, sale of company assets, financing, acquisition, reorganization, bankruptcy, or similar event.
- **Legal and safety.** To comply with law, regulation, legal process, or governmental request; to enforce our terms; and to protect the rights, property, or safety of the Company, our users, or others (including fraud prevention and security).
- **Your direction/consent.** To third parties or integrations you choose (e.g., when you share User Content, transcripts, or links; when you connect third-party apps or cloud storage); and for any other purpose disclosed at collection with your consent.
- **Public and other users.** Content you post in public areas of the Website or Apps (User Contributions) may be visible to others as configured by you.

Interest-based advertising. Third parties may set cookies/SDKs to provide analytics and, where enabled, interest-based ads. In some jurisdictions (e.g., California), such practices may be deemed

a “sale” or “sharing” of personal information. You can manage these activities via our cookie or in-app privacy controls and applicable device/browser settings.

If you have questions about a specific disclosure or recipient, contact us at the email listed in Contact Information.

Third-Party Use of Cookies and Other Tracking Technologies

Some content, features, and integrations in the Services are provided by third parties (for example: analytics, crash reporting, payment processing, customer support tools, cloud/AI vendors that process transcription/model outputs, marketing partners, and ad networks). These third parties may set their own cookies, pixels, SDKs, or similar technologies to collect information about your device and usage over time and across different websites and apps. They may use this information to provide services to us (e.g., analytics, security, performance, and support) and, where enabled, to deliver or measure interest-based advertising.

We contractually require service providers to use personal information only to provide services to us and to protect it appropriately. However, we do not control third parties’ independent data practices, which are governed by their own privacy policies.

Accessing and Correcting Your Information

Access/Update. You can review and update certain personal information in your Account settings on the Website or in the Apps. If you cannot find what you need there, email hey@heypocket.com from the email address associated with your Account.

Verification & Authorized Agents. We may require reasonable verification of your identity (and, where applicable, your authorized agent’s authority) before acting on a request. We may ask for limited additional information to confirm your identity and help locate the data.

Timing. We aim to respond within 15–30 days, subject to permitted extensions where reasonably necessary or required by law. We will let you know if we need more time.

Correction. If any personal information we hold about you is inaccurate or incomplete, you may request that we correct or complete it. In some cases, we may provide self-service tools so you can make corrections directly.

Deletion. You may request that we delete personal information. We will delete or de-identify it, subject to lawful exceptions (e.g., security and fraud prevention, exercising or defending legal claims, complying with record-keeping, tax, and other legal obligations). Deleting your Account will remove associated personal information from active systems, but:

- content previously shared with others or with third-party integrations may persist with those recipients subject to their policies;
- residual copies may remain in routine backups and logs and will be purged on scheduled cycles.

Limits on Requests. We may deny or limit a request if we cannot verify it, if fulfilling it would violate the rights of another person, if a legal exception applies, or if the request is excessive or manifestly

unfounded (in which case a reasonable fee may apply where permitted). If we deny your request, we will explain the reason unless prohibited by law.

User Contributions. Deleting your User Contributions from the Services does not guarantee complete removal from caches/archives, and copies made by other users or indexed by search engines may remain outside our control.

How to Contact Us. To make any of the requests above, use the self-service tools in your Account or email hey@heypocket.com

Your California Privacy Rights

If you are a California resident, California law may provide you with additional rights regarding our use of your personal information.

Data Security

We use administrative, technical, and physical safeguards designed to protect the integrity and security of personal information we process. These measures are intended to protect your information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. However, no method of transmission or storage is 100% secure, and we cannot guarantee absolute security. If we learn of a security incident that affects your personal information, we will notify you consistent with applicable law.

Your role in security matters too. If we give you (or you choose) a password or other credentials for any part of the Services (including the Website or Apps), you are responsible for keeping them confidential and for restricting access to your devices and Account. Please do not share your password with anyone.

Although we work to protect your personal information, any transmission over the Internet is at your own risk. We are not responsible for the circumvention of any privacy settings or security measures on the Services.

Retention of Your Information

We retain personal information only for as long as necessary to fulfill the purposes described in this Privacy Policy, including to provide the Services, comply with our legal obligations, resolve disputes, and enforce agreements. When determining retention periods, we consider factors such as:

- the type of Services provided and our relationship with you;
- the nature, sensitivity, and volume of the data;
- the potential risk of harm from unauthorized use or disclosure;
- legal, tax, accounting, and regulatory requirements (including statutes of limitation and legal holds).

When personal information is no longer needed, we will delete, de-identify, or anonymize it. Residual copies may remain in routine backups and system logs for a limited time and will be purged on scheduled cycles.

Changes to Our Privacy Policy

We will post any changes to this Privacy Policy on this page and update the “Last modified” date at the top. If we make material changes to how we treat personal information, we will provide additional notice (e.g., by email to the address in your Account, in-product notice, or on the Website). You are responsible for maintaining an active, deliverable email address in your Account and for reviewing this page periodically.

Contact Information

To ask questions or comment about this Privacy Policy and our privacy practices, contact us at hey@heypocket.com or write to: Open Vision Engineering, Inc., 131 Continental Dr, Suite 305, Newark, DE 19713, United States.