Privacy Policy

MIDNIGHT BRONCO
Effective: November 20, 2026 | Last updated: November 20, 2026

Veilora · TrackHarbor · Stillstory · NopeRope · Midnight Bronco

Who we are and what this policy covers

Codin Pangell, operating as Midnight Bronco in Oregon, United States ("Midnight Bronco," "we," "us," or "our"), is responsible for the personal information described in this policy.

This policy covers our websites, applications, digital products, support, and related services, including Veilora, TrackHarbor, Stillstory, NopeRope, and the Midnight Bronco website and brand, including references to "midnightbronco" (together, the "Services"). It also covers future Services that link to this policy.

A feature-specific notice may provide more detail about a particular product, integration, or optional feature. Read that notice together with this policy. A new product or feature does not automatically collect every category of information listed here.

When we process information solely on behalf of a business customer under that customer's instructions, the customer determines the purposes of that processing. The customer's privacy notice and our agreement with that customer govern that processing. Third-party products that we merely support, but do not operate, have their own privacy policies.

Privacy at a glance

We do not run advertisements, sell personal information, or share personal information for cross-context behavioral advertising or targeted advertising. We do disclose information to service providers when needed to deliver the Services; those operational disclosures are explained below.

We use Firebase and Google Cloud for applicable cloud, account, analytics, diagnostics, and infrastructure functions, and OpenAI for applicable AI features. The providers and data involved depend on the product and feature.

We ask for your explicit approval within the relevant AI feature before sending photos or recordings. Import permissions, general settings, and reading this policy do not provide that approval.

Our Services are intended for adults, not minors. You can contact us about access, correction, deletion, or other privacy concerns at midnight.bronco.studio@gmail.com.

Information we process and where it comes from

Information you provide. Depending on the Service, this includes your name, email address, account and profile details, authentication information, preferences, messages to support, collaboration inquiries, and information you choose to include in feedback. If you send us a support attachment, we receive that attachment and any personal information it contains.

Content and files. Depending on the feature you use, a product may process photos, recordings, documents, text, associated metadata, or other files you import, create, store, sync, export, or submit. Content may remain on your device or be transmitted for an enabled cloud or AI function. The feature's controls and notices identify the relevant processing.

Account, purchase, and subscription records. We may receive account identifiers, sign-in-provider information, plan and entitlement status, transaction references, billing contact information, and payment or renewal status from authentication providers, payment processors, or app stores. Payment details entered into a processor's hosted checkout are handled by that processor; the records we receive depend on the payment method and integration.

Technical and diagnostic information. Our Services and providers may process IP addresses, browser and device information, operating system and app versions, timestamps, requests, approximate location inferred from an IP address, feature-usage events, error reports, crash details, and security logs. Crash reports or logs can contain incidental content or identifiers depending on the event and configuration.

Permissions and integrations. When you authorize a device permission or connect another service, we process the information available through the permission or integration that is needed for the requested feature. Sources include your device, selected files, authentication providers, connected services, payment platforms, and our infrastructure providers. Do not grant access or submit other people's information unless you have an appropriate right or permission to do so. Your submitted content may contain sensitive information, such as health details, private communications, or information about other people. We process it only for the relevant disclosed purposes and obtain additional consent where applicable law requires it.

How we use information

We use information to provide the features you request; create and manage accounts; authenticate users; store, sync, or retrieve content when applicable; perform user-authorized AI processing; administer trials, purchases, and subscriptions; and respond to support or business inquiries.

We also use relevant information to understand product usage, diagnose errors, improve reliability and usability, prevent fraud or abuse, protect accounts and infrastructure, enforce our agreements, maintain business records, and comply with legal obligations.

We use contact information for service and account communications. If we offer optional marketing updates, you may unsubscribe using the instructions in those messages or by contacting us. Opting out of marketing does not stop necessary security, transaction, or service notices.

On-device processing, cloud storage, and backups

On-device processing is different from sending information to Midnight Bronco or a provider. If a feature processes content only on your device, we do not receive that content merely because you use that feature. Other parts of the same product, such as sign-in, entitlement checks, diagnostics, or support, may still communicate with our providers.

Where cloud features are enabled, Firebase or Google Cloud may process account information, stored content, usage records, diagnostics, and related metadata as needed for that feature. Cloud-stored copies, local copies, exported copies, and device or operating-system backups are separate. Deleting one does not necessarily delete the others.

If you export, share, or back up content to a destination you choose, the destination may receive the content under its own terms and settings. A decrypted export is no longer protected by the original vault's encryption. We cannot retrieve or delete copies held solely on your device or in an independently controlled third-party destination.

Optional AI features and user authorization

Before sending photos or recordings to an AI provider, the feature tells you which provider will receive them, why, which content is included, and what related information will be sent. The transfer requires an affirmative choice for that action. You can decline and continue without an AI upload.

Stillstory's optional photo grouping sends OpenAI resized previews of photos in the album, including newly imported photos, with app-assigned photo IDs, filenames, photo dates, and image dimensions. OpenAI returns suggested page groupings, labels, and descriptions. If you decline, Stillstory continues the import using its standard layouts.

Stillstory's optional featured-photo selection sends OpenAI resized previews from the current import review with app-assigned photo IDs, filenames, and image dimensions. OpenAI returns suggested picks and rankings. Stillstory leaves your review as it is if you decline. Both features require approval each time you use them and send previews rather than full-resolution originals.

Stillstory uses the OpenAI Responses API with response storage disabled. OpenAI does not use API inputs or outputs to train its models by default. Its abuse-monitoring and other retention rules may still apply.

Websites, cookies, analytics, and diagnostics

We use analytics and crash reporting to understand how the Services work and investigate problems. Depending on the product and configuration, these functions may use cookies, local storage, installation identifiers, account-linked events, or similar technologies. Necessary storage may support authentication, security, and your preferences.

We do not use these technologies to serve advertisements or to sell or share personal information for targeted advertising. Where consent is legally required for nonessential analytics or similar technologies, we will request it before activating those technologies. You may use available consent controls, browser settings, and device or app privacy settings to manage them. Blocking necessary storage may affect sign-in or other features.

Some website pages may load fonts or other assets from an external provider, including Google Fonts. Loading an external asset can disclose your IP address, request details, and browser information to that provider even if you do not have an account with us.

Browser "Do Not Track" signals do not have a single universally implemented standard. We honor legally required opt-out preference signals, including Global Privacy Control, for processing to which they apply. Because we do not sell personal information or use it for targeted advertising, there is no such activity to opt out of under our current practices. A signal does not, by itself, delete account information or disable necessary service processing.

When we disclose information

Service providers. We disclose relevant information to providers that help us operate the Services, subject to applicable agreements and restrictions. These include Firebase and Google Cloud for cloud infrastructure, authentication, storage, analytics, and diagnostics where used; OpenAI for approved AI processing; and payment providers, email/support providers, hosting providers, and professional advisers as needed. Stripe is used in TrackHarbor’s configured hosted-checkout flow where that billing feature is available.

At your direction. We disclose content or account information when you request an export, sharing action, integration, sign-in, purchase, or another function involving a third party. Your chosen recipient may process the information independently.

Legal and safety needs. We may disclose information when reasonably necessary to comply with law or valid legal process, protect rights or safety, investigate fraud or abuse, or enforce agreements, consistent with applicable law.

Business changes. If a merger, acquisition, financing, reorganization, or transfer of assets involves personal information, it may be disclosed to relevant parties with appropriate protections. We will provide notice and choices required by law if the responsible entity or applicable privacy practices materially change.

We do not sell personal information or disclose it for cross-context behavioral advertising or targeted advertising. Providing necessary information to an operational service provider is different from stating that we never disclose information to anyone.

How long we retain information

We retain personal information for as long as reasonably necessary for the purposes described in this policy, unless a longer period is required or permitted by law. Relevant criteria include whether your account is active; whether information is needed to provide a feature, complete a transaction, resolve a dispute, maintain security, or satisfy accounting and legal obligations; the sensitivity of the information; and available deletion controls.

Different records have different lifecycles. Account and cloud content may remain until you delete them or request deletion, subject to necessary exceptions. Diagnostic and security records are retained according to operational needs and provider settings. Billing and tax records may need to be retained after account closure. Provider-side AI retention depends on the feature and configuration described above.

Deletion may not immediately remove information from every backup or log. Retained backup copies remain subject to safeguards and are removed through the applicable backup lifecycle, unless needed for a lawful exception. If you request deletion, we can explain any material retention exception that applies. Files stored only on your own devices remain under your control.

Security

We use reasonable technical and organizational safeguards appropriate to the information and processing involved, including access controls and security measures available through our infrastructure providers. No product, network, storage system, or transmission method can be guaranteed completely secure.

Protect your devices, passwords, authentication factors, and recovery information. A product’s encryption or vault features apply only within their stated scope; they do not automatically protect exported copies, email attachments, device backups, or content you authorize a cloud or AI provider to process. Contact us if you believe your account or our Services have been compromised.

Your choices and privacy requests

You may use available product controls to manage profile information, permissions, cloud functions, content, subscriptions, and optional AI features. You can revoke device permissions through operating-system settings and disconnect an integration using the relevant product or provider controls. Revocation generally affects future access; it does not automatically delete information already lawfully processed.

You may request access to, correction of, or deletion of personal information we hold by emailing midnight.bronco.studio@gmail.com. Use a subject such as "Privacy request" and identify the product, the email associated with your account if applicable, and what you would like us to do. Do not send passwords, payment-card numbers, or unnecessary sensitive documents.

We may need to verify your identity and, where applicable, an authorized agent’s authority before responding. We use verification information for that purpose and security. We respond within the periods required by applicable law, explain permitted extensions or refusals, and do not discriminate against you for exercising

applicable privacy rights. Some features cannot operate without information necessary to provide them.

Deleting an account may not cancel a subscription purchased through an app store or another independently operated payment platform. Use the relevant subscription controls as well. Deletion of cloud records does not erase local or exported copies under your control.

Additional U.S. state privacy rights

Depending on where you live, whether a particular law applies to our activities, and applicable exceptions, you may have rights to confirm processing; access or obtain a portable copy of personal information; correct inaccuracies; request deletion; and opt out of sale, targeted advertising, or certain profiling. Some laws also provide rights concerning sensitive information or disclosures to third parties.

Oregon. If the Oregon Consumer Privacy Act applies to the relevant processing, Oregon residents may exercise the rights it provides, including requesting a list of specific third parties to which personal data has been disclosed where the law requires. We respond to covered requests within 45 days, subject to a permitted extension with notice. If we deny a request, email us with the subject "Privacy appeal." We will review the appeal and respond within the legally required period, generally 45 days for an Oregon appeal. You may also contact the Oregon Department of Justice.

California. If the California Consumer Privacy Act applies, California residents may have rights to know the categories and specific pieces of personal information collected, sources, purposes, and disclosures; request deletion or correction; and exercise applicable rights concerning sale/sharing and sensitive personal information. The categories, purposes, sources, and recipient categories are described in this policy. We do not sell or share personal information for cross-context behavioral advertising. Where applicable, you may request that we limit uses of sensitive personal information beyond permitted purposes.

Where your state provides a right to appeal a privacy decision, send "Privacy appeal" to our contact address. We will explain our decision and any further complaint rights required by law. Applicable rights and deadlines depend on your jurisdiction; this section does not claim that every state privacy statute applies to Midnight Bronco.

EEA, UK, and other international users

Midnight Bronco operates in the United States. Our providers may process information in the United States and other countries where they or their service providers operate. Privacy protections and government-access rules may differ from those in your country. Where applicable law requires safeguards for an international transfer, we use the appropriate lawful mechanism, such as an adequacy decision or applicable standard contractual clauses and related safeguards.

Where the GDPR, UK GDPR, or a similar law applies, our legal bases depend on the activity: performing a contract for requested Services and account functions; legitimate interests in security, support, and proportionate service improvement after considering your rights; legal obligations for required records and compliance; and consent for processing that requires it, including applicable optional AI or nonessential

tracking activities. Where required, a separate condition applies to processing special-category information.

Where applicable, you may have rights of access, rectification, erasure, restriction, portability, objection, and withdrawal of consent. Withdrawing consent does not affect processing that was lawful before withdrawal. You may object to processing based on legitimate interests and to direct marketing. Contact us to exercise these rights; we generally respond within one month where the GDPR or UK GDPR requires, subject to lawful extensions.

You may complain to a competent data protection authority, including the authority in the EEA country where you live or work, or the UK Information Commissioner's Office if applicable. You do not need to contact us first. If an authorized regional representative is required for a particular offering, its contact details will be supplied with that offering.

Adults only

Our Services are not intended for anyone under 18. We do not knowingly collect personal information from minors through the Services. Do not create an account or submit personal information if you are under 18.

If you believe a minor has provided personal information to us, contact midnight.bronco.studio@gmail.com with the product and relevant details. We will investigate and take appropriate steps to delete the information or otherwise address it as required by law. An adult's authorization to submit a file does not remove privacy obligations concerning other people, including minors, depicted or recorded in that file.

Product-specific context

Veilora. Your vault password stays on your device. Firebase Authentication manages sign-in. If you enable end-to-end encrypted sync, linked devices sync encrypted copies of files, collections, and notes. Firestore stores sync enrollment and device preferences. Veilora does not send vault photos or recordings to an AI provider.

TrackHarbor. TrackHarbor captures system audio to local files and reads supported player metadata locally. System audio can include other apps, notifications, or calls. TrackHarbor does not capture microphone audio or send recordings to an AI provider. Firebase handles sign-in and account and entitlement records, including trial or usage counters and completion-event identifiers. Stripe handles applicable billing.

Stillstory. For signed-in projects, Stillstory can upload original photos and thumbnails to cloud storage for your project. That storage is separate from the optional OpenAI photo features, which send previews only after you approve the specific action.

NopeRope. The macOS app keeps recent activity records in memory and lets you export a report locally. It does not send app telemetry. If you approve a macOS restore download, the app connects to Apple. If you enable networking in a guest and use a third-party service there, that service handles data under its own terms.

Midnight Bronco. When you submit the studio contact form, it sends your name, email address, and message to the studio inbox through Gmail so we can respond. The form uses your IP address to limit repeated submissions. Earlier messages may have been submitted through Google Forms.

Third-party services

The Services may contain links to or interact with app stores, payment platforms, connected applications, and other services operated by third parties. Those parties may act independently for their own account, transaction, security, or legal purposes. Their privacy notices govern that independent processing. Our use of a provider does not mean every provider receives every category of information.

For more information, see the privacy and data-protection notices for Google/Firebase/Google Cloud, OpenAI, and, where applicable, Stripe and your app store. Contact us if you need information about the providers involved in a particular product or request.

Changes to this policy

We may update this policy as our Services or legal requirements change. We will change the date shown at the top and provide additional notice when required for a material change. Where consent is required for a new purpose, we will obtain it rather than treating publication of an updated policy as consent. A change does not retroactively authorize an incompatible use of information collected under an earlier commitment.

Contact Midnight Bronco

Privacy contact: Codin Pangell, operating as Midnight Bronco. Location: Oregon, United States. Email: midnight.bronco.studio@gmail.com.

Please identify the relevant product and your request so we can route it correctly. If you need an accessible copy of this policy or information about applicable complaint procedures, contact the same address.