Legal

Website Privacy Policy

This policy covers **our websites** — sonomos.ai and every sonomos.ai subdomain we operate. The Locke app and browser extension are covered separately by the Locke Privacy Policy.

Effective: September 15, 2026 · Last Updated: November 10, 2026

Which policy do you need? We publish two privacy policies, because our websites and our software handle data in genuinely different ways.

- **This policy** covers our **websites**: sonomos.ai and every subdomain of sonomos.ai we operate, including support.sonomos.ai and trust.sonomos.ai, plus any subdomain we launch in the future.
- The **Locke Privacy Policy** covers the **Locke product**: the desktop application and the browser extension, which process your content locally on your own device.

Our Terms of Service, by contrast, are shared — one agreement covers all of our websites and all of our products.

This Website Privacy Policy for Sonomos, Inc., doing business as Sonomos, a Delaware corporation with its principal place of business at 9924 Kika Court #2416, San Diego, CA 92129, describes how and why we might access, collect, store, use, and/or share ("process") your personal information when you use our websites (the "Sites"), including when you:

- Visit sonomos.ai, or any subdomain of sonomos.ai, or any other website of ours that links to this Privacy Policy;
- Create a Sonomos account, subscribe, or manage your subscription and billing through our Sites;
- Contact us through a form on our Sites, or open a request through our Support Center;
- Apply to the Locke beta tester program through the form on our Sites; or
- Engage with us in other related ways through our Sites, including any marketing or events.

Questions or concerns? Reading this Privacy Policy will help you understand your privacy rights and choices. If you do not agree with our policies and practices, please do not use our Sites. If you still have any questions or concerns, please contact us at info@sonomos.ai.

1. Which Websites This Policy Covers

In Short: Every website we run on our sonomos.ai domain, including subdomains that do not exist yet. It does not cover the Locke app or browser extension.

1.1 The Sites. "Sites" means the website located at sonomos.ai together with **every subdomain of sonomos.ai that we operate**, whether that subdomain exists as of the Last Updated date above or is launched at any time afterward. As of the Last Updated date, this includes:

- **sonomos.ai** and **www.sonomos.ai** — our main website.
- **support.sonomos.ai** — our Support Center.
- **trust.sonomos.ai** — our Trust Center.

1.2 Future Subdomains. Any additional website we make available at a subdomain of sonomos.ai — for example, and without limitation, an address such as dashboard.sonomos.ai, app.sonomos.ai, status.sonomos.ai, docs.sonomos.ai, or api.sonomos.ai — is covered by this Privacy Policy from the moment it becomes available. This is a single policy for our entire website estate: you do not need to look for a different privacy policy when you move between our subdomains.

1.3 One Consistent Standard. All of our Sites are operated by us on the same infrastructure and to the same standard described in this policy: no cookies, no cross-site tracking, no advertising technology, and anonymous, cookieless analytics only. If we ever launch a Site that departs from that standard — for example, one that necessarily sets a functional cookie in order to work — we will say so on that Site and update this policy before doing so.

1.4 What This Policy Does Not Cover. This policy does not describe how the Locke product handles data. Locke — our desktop application and our browser extension — performs its sensitive-data detection and masking locally on your device and is governed by the separate Locke Privacy Policy at sonomos.ai/locke/privacy. This policy also does not cover third-party websites we link to, which have their own policies.

2. Key Terms

We, us, our — Sonomos, Inc., doing business as Sonomos, a Delaware corporation with its principal place of business at 9924 Kika Court #2416, San Diego, CA 92129.

Personal Information — Any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, as defined in Cal. Civ. Code § 1798.140(v)(1).

Sensitive Personal Information — Personal information revealing a consumer's social security number, driver's license or passport numbers, account log-in credentials, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, contents of mail/email/text messages (where the business is not the intended recipient), genetic data, biometric information, health information, sex life or sexual orientation information, or citizenship/immigration status, as defined in Cal. Civ. Code § 1798.140(ae)(1).

Biometric Information — An individual's physiological, biological, or behavioral characteristics, including DNA, used to establish individual identity, including imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, and keystroke patterns, gait patterns, and sleep, health, or exercise data containing identifying information, as defined in Cal. Civ. Code § 1798.140(c).

Service Provider — A legal entity that processes personal information on our behalf pursuant to a written contract that prohibits the entity from retaining, using, or disclosing the personal information for any purpose other than performing the specified services.

Sale / Sell — Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer's personal information to a third party for monetary or other valuable consideration, as defined in Cal. Civ. Code § 1798.140(ad)(1).

Share / Sharing — Communicating a consumer's personal information to a third party for cross-context behavioral advertising, as defined in Cal. Civ. Code § 1798.140(ah)(1).

Targeted Advertising — Displaying advertisements selected based on personal data obtained from a consumer's activities over time and across nonaffiliated websites or applications.

Profiling — Any form of automated processing of personal data to evaluate, analyze, or predict certain personal aspects of an individual, including economic situation, health, preferences, interests, reliability, behavior, location, or movements.

3. Personal Information We Collect Through Our Sites

In Short: Only what is necessary to run an account, take a payment, and answer your message. We do not collect browsing history, geolocation data, biometric information, or behavioral profiles anywhere on our Sites.

In the preceding 12 months, we have collected the following categories of consumer personal information through the Sites:

- **A. Identifiers** — Real name, email address, account identifiers, unique user ID. *(Collected)*
- **B. Personal information per Cal. Civ. Code § 1798.80(e)** — Name, email address. We do not collect SSN, physical description, address, telephone, insurance, bank account, credit/debit card numbers, or health information. Payment card data is collected directly by Stripe. *(Collected)*
- **C. Protected classification characteristics** — None collected.
- **D. Commercial information** — Subscription purchase records and billing history (maintained by Stripe). *(Collected)*
- **E. Biometric information** — None collected.
- **F. Internet or other electronic network activity** — Limited and transient. *(Collected)* Our edge infrastructure processes your IP address and user agent in order to serve pages and to rate-limit abuse of our forms, and a salted hash of your IP address is held briefly for that rate-limiting purpose only. Our only analytics are aggregate statistics that our host, Cloudflare, derives from the same request data it already processes to serve our pages: for example, counts of requests and page loads, an estimate of unique visitors (which Cloudflare calculates from IP addresses), which pages were requested, and the type of browser or automated agent that requested them. We also use Cloudflare Web Analytics, a script from Cloudflare that runs on our pages and reports that a page was viewed, its address, the referring page, and how quickly it loaded. We look at these totals only. No cookies are set, nothing is stored on or read from your device's storage, and no individual profiles are created. We do not track your browsing history or search history across our Sites, do not build profiles, and do not join any of this to your account.
- **G. Geolocation data** — None collected.
- **H.** Audio/visual information — None collected.
- **I. Professional or employment-related information** — Collected only through the beta tester application: the field you work in, chosen from a short list (for example law, healthcare, finance and accounting, IT and security, or student), and nothing more specific. *(Collected)*
- **J.** Education information — None collected, beyond a "student" option in the field-of-work question above.

- **K. Inferences** — None created. We do not build consumer profiles, infer preferences, or create behavioral models.
- **L. Sensitive personal information** — None collected.

Contact and Support Messages. If you write to us through a form on any of our Sites, including the Support Center at support.sonomos.ai, we process the contents of your message and the contact details you give us, for the sole purpose of answering you. Your message is delivered to us by email, which means it passes through our edge provider and our email providers and is stored in our company inbox. Please do not include sensitive personal information in a support message.

Beta Tester Application. If you apply to test Locke through the form at sonomos.ai/beta/, we collect what you enter there: your name and email address; the field you work in; how comfortable you are with software, on a scale you pick; whether you want to join the beta Slack group or prefer email; which part of Locke matters most to you; and how you heard about us. The form is hosted by Google Forms and your answers are stored in our Google Workspace account; see Section 6. We use them only to run the beta program: to choose a varied group of testers, to contact you about testing, to invite you to the Slack group if you asked for it, and to understand which features testers care about. Applying does not create a Sonomos account, and we do not combine your answers with analytics or with any other source.

Payment Data. All payment data is collected, handled, and stored directly by Stripe, Inc. We do not receive or store your full payment card number, CVV, or bank account details. See: stripe.com/privacy.

Third-Party Authentication. We may in the future offer registration via third-party authentication providers such as Google. If implemented, our use of such data will adhere to applicable API data policies. We will update this Privacy Policy before enabling any such feature.

Server Logs and Abuse Prevention. Our hosting and edge infrastructure processes standard request data (such as IP address and user agent) transiently in order to serve pages and to defend against attacks and abuse. When you submit a form, we compute a salted hash of your IP address and keep it for a short period as a rate-limiting key, so that the same source cannot flood us with submissions; we do not keep the raw address for that purpose and we do not put it in the message. We do not use any of this data to build profiles, and we do not join it to your account.

4. How Your Personal Information Is Collected

In Short: Directly from you, and from our authentication and payment providers. We do not collect from data brokers, advertising networks, or other third-party sources.

- **Directly from you** — registration, subscription, contact and support forms, the beta tester application form, or email communication.
- **From the authentication provider(s)** — Supabase and Resend (email address and authentication tokens, used for passwordless login via one-time passcode).
- **From our payment processor** — Stripe provides subscription status and billing events, not full card numbers.

We do not collect personal information from: data brokers, advertising networks, internet service providers, social media platforms, credit reporting agencies, government entities, publicly accessible sources, or any other third-party sources.

5. How and Why We Process Your Personal Information

In Short: To run your account, take payment, answer you, keep the Sites secure, and comply with law.

- Account creation, authentication, and management — Performance of our contract.
- Delivering the Sites and managing your subscription — Performance of our contract.
- Process payments and billing through Stripe — Performance of our contract.
- Respond to inquiries and provide support — Contract performance; legitimate interest.
- Run the Locke beta tester program: select and contact testers, invite those who asked to the beta Slack group, and learn which features matter to them — Legitimate interest; consent for the Slack invitation.
- Security, fraud prevention, and abuse detection — Legitimate interest.
- Comply with legal obligations — Legal obligation.
- Send marketing communications (only with express opt-in consent) — Consent.

We do not use your personal information for: profiling, automated decision-making, targeted advertising, cross-context behavioral advertising, sale to third parties, building consumer profiles, or training machine learning models.

6. Who We Share Your Personal Information With

In Short: A short list of service providers, used across all of our Sites, only as necessary to operate them.

- **Supabase** — Authentication and database. Receives: email address, user ID. Purpose: account management.
- **Stripe** — Payment processing. Receives: name, email, payment data. Purpose: subscription billing.
- **Resend** — Transactional email. Receives: your email address, and — where you use a contact or support form — your name and the contents of your message. Purpose: one-time-passcode delivery, account notifications, and routing your message to us.
- **Cloudflare** — Hosting, content delivery, edge security, aggregate traffic statistics, and delivery of contact-form messages to our inbox. Processes: standard request metadata (including your IP address and user agent), which Cloudflare logs and retains under its own privacy policy, as any host does, and from which it gives us aggregate traffic statistics; a short-lived salted hash of your IP address for rate limiting; and the contents of a contact-form message in transit. We look only at aggregate totals, except that Cloudflare's security tools show us details of individual requests it blocks or challenges as threats, which we use only to protect the Sites.
- **Google Workspace** — Our company email. Receives: any message you send us, including contact-form and support messages and the address you asked us to reply to. Purpose: receiving and answering your correspondence.
- **Google Forms (Google LLC)** — Hosts the beta tester application form at sonomos.ai/beta/. Receives: everything you enter in that form, together with the standard request data (IP address, user agent) any web page sends when it loads. Your answers are stored in our Google Workspace account. Purpose: collecting beta applications.
- **Slack** — Only if you ask, in the beta form, to join the beta testers' Slack group. Receives: your email address, as an invitation. Purpose: the beta discussion group. If you choose email only, nothing goes to Slack.

The same list applies to every one of our Sites, including support.sonomos.ai and trust.sonomos.ai. We do not share with: advertisers, data brokers, social media platforms, marketing agencies, credit reporting agencies, or any third parties not listed above.

Embedded third-party content. Two of our pages embed content served by Google: the contact page embeds a Google Calendar scheduling widget so that you can book a call with us, and the beta tester page (sonomos.ai/beta/) embeds the Google Form described in Section 3. If you open either page, Google receives your IP address, user agent, and the fact that you visited it, under Google's own privacy policy, and Google may set its own cookies inside the embedded frame; we do not set, read, or receive those cookies. If you would rather not have that happen, email us at info@sonomos.ai instead; for the beta program, an email with the same details is treated exactly like a form submission.

7. Categories of Personal Information Sold or Shared

We do not sell your personal information. We have not sold consumers' personal information in the preceding 12 months and will not do so without notice and an opportunity to opt out.

We do not share your personal information for cross-context behavioral advertising or targeted advertising.

8. Categories of Personal Information Disclosed for a Business Purpose

In the preceding 12 months, we have disclosed the following categories to service providers for business purposes:

- **A. Identifiers** (email address, user ID) → Supabase, Resend — Account management, transactional email.
- **B. Personal information** (name, email) → Stripe — Subscription billing.
- **D. Commercial information** (subscription records) → Stripe — Payment processing.
- **F. Internet or other electronic network activity** (IP address, user agent) → Cloudflare — Serving pages, abuse prevention, aggregate traffic statistics.
- **A. Identifiers and message contents** (name, email, message text) → Resend, Google Workspace — Delivering and answering your correspondence.
- **A and I. Identifiers and professional information** (name, email, field of work, and your other beta-form answers) → Google (Forms and Workspace) — Collecting beta applications; and, only if you asked to join it, your email address → Slack — Inviting you to the beta group.

No other categories (C, E, G, H, J, K, or L) have been disclosed for any purpose in the preceding 12 months. None of these disclosures is a sale or a sharing for cross-context behavioral advertising.

9. How Long Your Personal Information Will Be Kept

In Short: Active account + up to 6 months after termination, except billing records, which tax law requires us to keep for longer.

- **Account information** — Account duration + 6 months.
- **Authentication data** — Deleted upon account termination.
- **Payment and billing records** — We keep the record of what you bought and what you paid for as long as tax, accounting, and audit law requires — generally seven years from the transaction — even after your account is closed. We never hold your card data at any point. Stripe retains its own copy under its policies.
- **Contact and support correspondence** — Retained for 24 months after your request is closed, so that we have a record of the resolution, then deleted.
- **Beta tester applications** — Retained for the life of the Locke beta program and for 12 months after it ends, so that we can follow up with testers about the release, then deleted. You can ask us to delete your application sooner at any time (Section 15).
- **Abuse-prevention IP hashes** — Retained for a matter of minutes and then discarded.
- **Transactional email logs** — Retained by Resend per its retention policies.
- **Marketing opt-in preferences** — Account duration + 6 months.

When no longer needed, we delete or anonymize your information. If not immediately possible, we securely isolate it until deletion is possible.

10. How We Keep Your Information Safe

In Short: Encryption, passwordless authentication, and organizational security measures, applied uniformly across all of our Sites.

- **Encryption in transit** — TLS encryption for all traffic to our Sites and all API communications.
- **Encryption at rest** — AES-256 via infrastructure provider.
- **Authentication security** — We use passwordless authentication (one-time passcode via email). No passwords are collected or stored.
- **Payment security** — Stripe handles all payment data (PCI-DSS Level 1 certified).
- **Privacy-first analytics** — aggregate traffic and page-view statistics from our host, Cloudflare — no cookies, nothing stored on your device, no profiles.
- **Access controls** — User data access restricted to authorized personnel on need-to-know basis.

No transmission or storage technology is 100% secure. You should access the Sites in a secure environment.

11. Do We Collect Information From Minors?

We do not knowingly collect, solicit data from, or market to children under 18 years of age. If we learn personal information from users under 18 has been collected, we will deactivate the account and promptly delete such data. Contact us at info@sonomos.ai if you become aware of any such collection.

12. Analytics, Cookies, and Do-Not-Track

In Short: No cookies, no tracking, on any of our Sites. Privacy-first analytics only.

Cookies and local storage: We set no cookies on any of our Sites. The two Google frames we embed (the scheduling widget on our contact page and the beta tester form at sonomos.ai/beta/) are served by Google, and Google may set its own cookies inside those frames under its own policy; those are not ours, we cannot read them, and both pages tell you so before the frame loads and offer email as an alternative. We do use your browser's local storage for a small number of strictly necessary things: remembering that you dismissed a notice, and keeping you signed in. None of it is used for analytics, advertising, or tracking, and all of it is cleared when you clear your browser data. We mention local storage explicitly because privacy rules in the EU and UK treat anything stored on your device the same way they treat cookies, and "no cookies" on its own would not tell you the whole story.

Analytics: Our only analytics come from our host, Cloudflare, in two forms. First, aggregate traffic statistics that Cloudflare derives from the requests it already processes to deliver our pages: for example, how many requests and page loads we served, an estimate of unique visitors, which pages were requested, and the type of browser or automated agent that requested them. Second, Cloudflare Web Analytics: a script served by Cloudflare runs on our pages and reports to Cloudflare that a page was viewed, the page's address, the referring page, and page-load performance measurements. That script sets no cookies and neither stores anything on your device nor reads anything from its storage, and Cloudflare states that it does not use your IP address or user agent to fingerprint you. We run no advertising or third-party marketing script, pixel, or tag. Cloudflare keeps request logs under its own privacy policy, as any host does; we look only at the totals, never at a record of you as an individual, and we do not count clicks.

Do-Not-Track: We do not track you, so there is no tracking for a Do-Not-Track signal to switch off. Our statistics count every request and page view, including those from browsers that send a Do-Not-Track signal. We state this plainly rather than claiming to act on a signal we have no occasion to act on.

Global Privacy Control (GPC): GPC is a browser signal that tells a site not to sell or share your personal information. We do not sell personal information, do not share it for cross-context behavioral advertising, and do not profile you — so there is no processing here for a GPC signal to switch off, and sending one changes nothing about how we treat you. We state this plainly rather than claiming to act on a signal we have no occasion to act on. If we ever begin any processing that a GPC signal would apply to, we will implement the signal and update this policy before doing so.

Our full commitment on this point, including how you can verify it for yourself, is set out in our No-Tracking Policy.

13. Your Rights Under the CCPA/CPRA (California)

In Short: California residents have specific rights under the CCPA/CPRA as described below.

Right to Know / Right to Access — You have the right to request disclosure of the categories and specific pieces of personal information we have collected, the sources, purposes, and third parties to whom we disclose it. We are not required to provide this information more than twice in a 12-month period.

Right to Opt Out of Sale or Sharing — We do not sell or share your personal information, so no opt-out action is required.

Right to Limit Use of Sensitive Personal Information — We do not collect or process sensitive personal information. No limitation request is necessary.

Right to Deletion — On receipt of a verifiable request, we will delete your personal information and direct our service providers to do the same, subject to lawful exceptions. The principal exception is billing and transaction records, which tax and accounting law requires us to retain for the period described in Section 9; we will tell you what we have retained and why.

Right to Correction — You may request correction of inaccurate personal information.

Right to Non-Discrimination and Non-Retaliation — We will not deny goods or services, charge different prices, or provide different quality for exercising your privacy rights.

14. Your Rights Under Other US State Privacy Laws

In Short: Residents of states with comprehensive privacy laws have specific rights. Because of our minimal data collection and no-sale, no-targeting, no-profiling practices, many of these rights are already satisfied by default.

This section applies to residents of states with comprehensive consumer privacy legislation, including: Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Montana, Texas, Oregon, Delaware, New Hampshire, New Jersey, Nebraska, Kentucky, Maryland, Minnesota, Rhode Island, and Florida.

Common rights across state laws:

- Right to Access / Right to Know
- Right to Correction
- Right to Deletion
- Right to Data Portability
- Right to Opt Out of Sale — We do not sell your personal data. No opt-out action required.
- Right to Opt Out of Targeted Advertising — We do not process data for targeted advertising.
- Right to Opt Out of Profiling — We do not profile consumers.
- Right to Non-Discrimination

Universal Opt-Out Mechanisms: Several of these states require us to act on browser-based opt-out preference signals such as Global Privacy Control. We do not sell personal data, share it for targeted advertising, or profile consumers, so there is no processing for such a signal to stop. If that ever changes, we will implement the signal and update this policy before beginning the processing.

Appeals Process: If we decline your privacy rights request, we will inform you of our reasons and provide instructions for appealing. Email info@sonomos.ai with subject line "Privacy Rights Appeal." We respond within 60 days.

15. How to Exercise Your Rights

To exercise any right described in Sections 13 or 14:

- Visit sonomos.ai/contact
- Email info@sonomos.ai
- Write to: Sonomos, Inc., 9924 Kika Court #2416, San Diego, CA 92129

A single request covers all of our Sites — you do not need to file a separate request for each subdomain. Your Locke desktop account is separate: the app signs in through Clerk and its account and billing are managed from inside the app, not from this website. A request here covers your Site account; to delete a Locke desktop account, say so and we will tell you what that needs, or see the Locke Privacy Policy.

Data access or portability requests are limited to twice per 12-month period. We verify identity using the email address associated with your account. We respond within 45 days, extendable by an additional 45 days with written notice.

Authorized Agent: You may designate an authorized agent with written permission. We may require direct identity verification.

16. Do Other Regions Have Specific Privacy Rights?

EEA, United Kingdom, and Switzerland: GDPR and equivalent rights apply: access, rectification, erasure, restriction, portability, objection, and the right not to be subject to a decision based solely on automated processing. Legal bases: contract performance (running your account, delivering the Sites, taking payment), consent (marketing), legitimate interests (security, fraud prevention, abuse detection), and legal compliance. You may withdraw consent at any time without affecting processing carried out before you withdrew it.

Providing your information. Giving us your email address is a contractual requirement — we cannot create or operate an account without it. Everything else is optional, and declining to provide it affects only the feature it relates to.

Automated decision-making. We do not make decisions about you based solely on automated processing, and we do not profile you.

International data transfers. Sonomos is established in the United States, and the personal information you give us is processed there. That is a direct collection from you rather than an onward transfer, so no Chapter V transfer mechanism applies to it. Where one of the service providers listed in Section 6 moves personal data out of the EEA or the UK on our behalf, that provider does so under the European Commission's Standard Contractual Clauses, the UK International Data Transfer Addendum, or another safeguard permitted by Article 46. A copy of the safeguard relevant to you is available on request at info@sonomos.ai.

Our EU and UK representatives. Under Article 27 of the GDPR and Article 27 of the UK GDPR we have appointed representatives whom you may contact on any matter relating to our processing of your personal data, as an alternative to contacting us directly. Their names and contact details are available on request at info@sonomos.ai.

Complaints. You have the right to lodge a complaint with the supervisory authority in the country where you live or work, or where you believe an infringement occurred — for example, the Irish Data Protection Commission, the UK Information Commissioner's Office, or the Swiss Federal Data Protection and Information Commissioner. We would appreciate the chance to address your concern first, but you are not required to come to us before going to them.

Australia and New Zealand: We process your information under Australia's Privacy Act 1988 and New Zealand's Privacy Act 2020. You may request access or correction. Complaints may be filed with the OAIC or NZ Privacy Commissioner.

Canada: Your PIPEDA rights are addressed throughout this Privacy Policy. We process with express or implied consent. Withdraw anytime.

17. California 'Shine the Light' Law

Cal. Civ. Code § 1798.83 permits California residents to request disclosure of personal information shared for direct marketing. We do not disclose personal information to third parties for their direct marketing purposes.

18. Do We Make Updates to This Policy?

We may update this Privacy Policy from time to time. For any change that materially affects how we handle your personal information, we will give you at least thirty (30) days' notice by email to the address on your account and by a notice on the Sites before it takes effect, and we will keep the previous version available at sonomos.ai/privacy/archive. Other changes take effect when posted, and are reflected in the "Last Updated" date above.

Adding a new sonomos.ai subdomain that follows the practices described here is not a material change and does not require an update to this policy — the new Site is covered automatically under Section 1.2. If a new Site would depart from those practices, we will update this policy first.

19. How Can You Contact Us?

Sonomos, Inc.
9924 Kika Court #2416
San Diego, CA 92129
United States

General: info@sonomos.ai

20. How Can You Review, Update, or Delete Your Data?

To submit a request, visit sonomos.ai/contact or email info@sonomos.ai. We respond to all verified requests within 45 days.