

Locke Privacy Policy

This policy covers **the Locke product** — the desktop app and the browser extension. Our websites are covered separately by the [Website Privacy Policy](#).

Last Updated: August 12, 2026

The short version. Locke reads what you are about to send to an AI tool, finds the sensitive parts, and masks them — all of that happens on your own machine. We never receive the content Locke inspects. There is no copy of it on our servers to leak, subpoena, or sell, because it never leaves your device in the first place.

Which policy do you need? This one covers the **Locke product**. Our [Website Privacy Policy](#) covers our websites — sonomos.ai and every sonomos.ai subdomain, including support.sonomos.ai and trust.sonomos.ai. A single set of [Terms of Service](#) covers both.

This Locke 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 ("Sonomos," "we," "us," or "our"), describes how and why we access, collect, store, use, and/or share ("process") personal information in connection with Sonomos Locke.

If you do not agree with our policies and practices, please do not install or use Locke. If you have questions, contact us at info@sonomos.ai.

1. What This Policy Covers

In Short: The Locke software itself, in every form we ship it.

1.1 The Product. "Locke" means the Sonomos Locke product in each of the forms we distribute it:

- **The Locke desktop application** — including its local daemon, graphical application, command-line tools, installers, updates, and documentation, for Windows and Linux, with macOS planned.
- **The Locke browser extension** — including Dagger (detection) and, when available, Cloak (masking), together with related local software components, on every browser we support.

1.2 Why This Policy Is Separate. Our websites and Locke are different kinds of thing, and treating them under one privacy policy would make that policy less accurate about both. A website processes your data on a server. Locke processes your data on your computer, and is specifically engineered so that we cannot see it. Those facts deserve to be stated plainly rather than averaged together, so we publish them separately.

1.3 What This Policy Does Not Cover. This policy does not cover our websites — sonomos.ai and its subdomains — which are governed by the [Website Privacy Policy](https://sonomos.ai/privacy) at sonomos.ai/privacy. It also does not cover the third-party AI tools and services you use Locke with, such as ChatGPT, Claude, Gemini, or a locally hosted model. Once you choose to send a message, the receiving service handles it under its own privacy policy. Locke's role is to determine what is in that message before you send it.

2. What Stays on Your Device

In Short: All of your content. Every part of the detection and masking pipeline runs locally.

The following happen entirely on your device, and the data involved is never transmitted to Sonomos, to any third-party server, or to any external service:

- **The content you type, paste, dictate, or scan.** Locke inspects it in memory on your machine.
- **Files and attachments you scan.** Document parsing and inspection is performed locally.
- **Detection.** Sensitive-data detection uses on-device pattern matching and on-device machine-learning models. No cloud model, inference API, or remote classifier is involved.
- **Masking.** Sensitive values are replaced locally, before the message leaves your device.
- **What was detected.** The categories, counts, positions, and values of anything Locke finds stay on your device. We do not receive detection results, not even in aggregate or anonymized form.
- **Your settings.** Detection preferences, category toggles, allow-lists, and similar configuration are stored in local storage on your device.
- **Your reports.** Compliance and activity reports are generated locally from local data and are yours to export or delete. We do not receive them.

Because this content is never transmitted to us, we cannot produce it in response to a subpoena, disclose it in a breach, sell it, or use it to train a model. That is a property of the architecture, not a promise about our intentions.

3. What Locke Sends to Our Servers

In Short: Enough to confirm you are licensed and to keep the software up to date. Nothing about your content.

Locke makes a small, fixed set of network requests to us:

- **License validation and subscription status.** Locke checks that your subscription is active. This request carries your account email address and subscription tier, and no content, detection data, or usage data.
- **Account authentication.** When you sign in, Locke authenticates through your designated authentication provider, using the passwordless one-time-passcode flow described in the Website Privacy Policy.
- **Update checks and delivery.** The desktop application checks for updates through our designated release channel. The browser extension is updated automatically through the applicable browser marketplace, such as the Chrome Web Store, under that marketplace's own terms.

Certificate checks. Aside from the requests above, the only other connection Locke initiates on its own behalf is a standard TLS certificate-revocation check.

Requests you direct. When you send a prompt to an AI provider, that request goes to the provider you chose, at your direction. We are not the recipient of it and it does not pass through our servers.

4. What Locke Never Does

Locke does not:

- Transmit, log, or store any content you type, paste, or scan.
- Send detected sensitive values, categories, or counts to any server.
- Use cloud-based AI or machine-learning services for content analysis.
- Collect browsing history, page content, keystrokes, or interaction data.
- Use cookies, web beacons, pixels, fingerprinting, or any tracking mechanism.
- Collect telemetry, usage analytics, crash reports, or performance metrics.
- Sell, rent, or share any data for advertising, profiling, or any other purpose.
- Use your data to train our models or anyone else's.

Because Locke collects no telemetry, we genuinely do not know how you use it. That is intentional, and it is why we ask for feedback rather than measuring you.

5. Personal Information We Hold Because of Locke

In Short: Your account and billing record. That is the whole list.

Using Locke requires a Sonomos account, and a paid tier requires a subscription. The personal information behind those — your name, email address, account identifier, and subscription and billing records — is collected and held through our websites and is described in full in the [Website Privacy Policy](#), including which service providers receive it (Supabase, Stripe, Resend), how long it is kept, and how to have it deleted.

Locke itself adds nothing to that record. Installing, running, or using Locke does not cause us to collect any additional personal information beyond the license-validation check described in Section 3, which reuses the account email we already hold.

In the categories used by California law, in the preceding 12 months Locke has caused us to process: **A. Identifiers** (account email address, for license validation). No other category — including **F. Internet or electronic network activity**, **G. Geolocation**, **K. Inferences**, and **L. Sensitive personal information** — is collected by Locke.

6. Permissions Locke Requests

In Short: The access required to read a text box before you hit send, and nothing more.

6.1 Browser extension. The extension requests permission to read and modify text input fields on supported AI interfaces. It uses that access solely to detect and mask sensitive data in what you are about to send. It does not use those permissions to collect, record, or transmit page content, and it does not read pages outside the interfaces it supports.

6.2 Desktop application. The desktop application requires operating-system access sufficient to observe and modify text you are entering into the AI applications you have chosen to protect. That access is used only for detection and masking, on your device, in memory. Which applications Locke is active in is under your control in the app's settings.

6.3 Local storage. Locke stores your settings and locally generated reports on your device. Uninstalling Locke, or clearing its data from within the app, removes them.

7. Retention

Your content — Never retained by us, because it is never transmitted to us. On your own device, content is held only transiently in memory during inspection and is not written to disk by Locke.

Detection results, settings, and reports — Retained on your device, under your control, for as long as you keep them. Deleted when you delete them or uninstall Locke.

Account and billing records — Retained for the duration of your account plus 6 months, as set out in the [Website Privacy Policy](#).

License-validation requests — Not retained as a usage history. We hold your current subscription status, not a log of when you used Locke.

8. Security

- **Local-first architecture** — The strongest control here is structural: content that never leaves your device cannot be intercepted, breached, or compelled from us.
- **Encryption in transit** — TLS for license validation, authentication, and update delivery.
- **Signed releases** — Desktop releases are signed, and browser-extension updates are distributed through the applicable browser marketplace.
- **Least privilege** — Locke requests only the access it needs to inspect the text you are about to send.

What local processing does not protect against. Running on your device means Locke's protection is bounded by your device's own security. It cannot defend against malware, keyloggers, screen capture, unauthorized physical access, or a compromised operating system. It also cannot recover data you have already sent to a third party. More detail on our threat model is on the [Locke security page](#).

Detection is not perfect. Locke uses pattern matching and on-device machine learning, and can produce both false positives and false negatives. It is a tool to support your judgment, not a substitute for it, and using it does not by itself constitute compliance with HIPAA, GDPR, GLBA, or any other framework.

9. Children

Locke is not directed to, and may not be used by, anyone under 18. We do not knowingly collect personal information from children under 18. If we learn that we have, we will deactivate the account and delete the data. Contact info@sonomos.ai if you become aware of any such collection.

10. Your Privacy Rights

The rights described in the [Website Privacy Policy](#) — including the CCPA/CPRA rights of California residents, the rights available under other US state privacy laws, and GDPR, UK GDPR, PIPEDA, and Australian and New Zealand equivalents — apply in full to the personal information we hold in connection with Locke.

Because that information is a single account record, you do not need to submit separate requests for our websites and for Locke. One request covers both. To exercise a right, visit sonomos.ai/contact, email info@sonomos.ai, or write to Sonomos, Inc., 9924 Kika Court #2416, San Diego, CA 92129. We respond to verified requests within 45 days.

We cannot act on a request concerning the content Locke processed on your device, because we never held it. That data is under your control: you can delete it yourself from within Locke or by uninstalling it.

11. International Users

Our account, licensing, and billing infrastructure is hosted in the United States. If you use Locke from outside the United States, the account information described in Section 5 will be transferred to and processed in the United States, under Standard Contractual Clauses and other appropriate safeguards where required.

The content Locke inspects is not transferred anywhere. It is processed on your device, in your own jurisdiction, and never crosses a border on our account.

12. Verifying These Claims

A privacy product should not ask for faith. Our [Trust & Transparency page](#) sets out what actually leaves your device in checkable terms, along with an honest account of what is not yet true, and our [Locke security page](#) describes the architecture in more detail. If you find a discrepancy between this policy and Locke's behavior, tell us at info@sonomos.ai — we would rather fix it than defend it.

13. Changes to This Policy

We may update this policy from time to time. Material changes will be indicated by an updated "Last Updated" date above and may include direct notification. If a future release of Locke changes what it sends to our servers, we will update this policy before that release ships, not after.

14. Contact Us

Sonomos, Inc.

9924 Kika Court #2416

San Diego, CA 92129

United States

General: info@sonomos.ai

Online: sonomos.ai/contact

