LEGAL

Blue Privacy Policy

Effective November 9, 2026. Replaces the October 20, 2026 version (which said mailing-list signups were stored only by our email provider; we now keep our own copy), the Blue Voice Assistant privacy notice of July 27, 2025 and the August 25, 2026 draft.

This policy explains what information Blue handles, what we do with it, and what you control. It is written to be read, not skimmed, and every statement in it is meant to be true of how Blue actually works. If something here is unclear, email hello@heyblue.com and we will answer.

"Blue," "we," and "us" mean Effortless Trading, Inc. "Blue" also means the products this policy covers: the Blue Phone (a Google Pixel running BlueOS), BlueOS (our operating system, built on the Android Open Source Project with additional security hardening), the Blue apps that run on it (the Blue assistant, Messages, Phone, Contacts, Photos and Files, Notes, Clock, Vault, Blue Store, and Find Phone), your Blue account and the Blue cloud that syncs and stores your data, the Blue Mac app used to move data from an iPhone, our software update service, and our website at heyblue.com.

Blue is not affiliated with, endorsed by, or sponsored by Google or Apple. Data handling on a Blue Phone is governed by this policy, not by theirs.

The short version

- **Your data is yours.** We store it to make Blue work for you. We do not sell it, we do not use it for advertising, and we do not use it to train AI models, ours or anyone else's.
- **It is encrypted**, in transit and at rest, in the United States.
- **By default, no one at Blue reads it.** People at Blue see your data only when you ask us for help and allow it, when we have to investigate abuse or a security incident, or when the law requires it. Such access is limited and logged.
- **Your passwords, cards, and IDs live in the Vault**, where every secret is encrypted with its own AES-256-GCM key and your account's key is sealed in a hardware security module. The assistant never sees Vault secrets; it can only ask the Vault to use one on your phone, after your fingerprint or face.
- **You can see, edit, and delete everything Blue remembers about you**, and you can delete your account and its data.
- **Blue uses AI providers** (currently OpenAI, Anthropic, and Google) to understand and act on your requests. They process your content for us under contracts that forbid them from training on it or using it for anything else.

The rest of this policy is the detail behind those six sentences.

1. Information Blue handles

> **In short:** Blue is your operating system, so it handles your messages, contacts, photos, notes, calendar, location, notifications, what is on your screen while it operates an app, your voice when you talk to it, and the secrets you keep in the Vault.

Blue is your phone's operating system, and the Blue assistant is a privileged part of it. To do its job, Blue sees more of your data than an ordinary app would. Here is what that includes.

Account information. Your name, email address, phone number, and a password, which we store only as a salted hash. To register your phone number on the Blue network, your device texts a one-time token from its SIM to a number we operate through Twilio, and Twilio reports the sending number to us. We also keep session tokens, device identifiers, device model, the BlueOS build on the device, IP address, and connection times.

Your content, synced to your Blue cloud. Blue keeps a synced copy of your phone's data in your Blue cloud so the assistant can use it, so your Blue apps stay in step, and so you can move to a new Blue Phone or read your data in a browser. This includes:

- your text messages: contents, senders, recipients, timestamps, and attachments, sent and received. Because Blue is your messaging app, this includes verification and two-factor codes texted to you, which the assistant can use on your behalf;
- your contacts and your history with them, and your call log;
- your photos, videos, and files, including location data embedded by the device that captured them;
- your notes, calendar, alarms, lists, voice notes, home screen layout, and automations;
- your conversation history with the assistant, and a record of the actions it took for you.

What Blue remembers about you. From your content and your requests, Blue builds a memory: the people in your life, the places you go, how you write, and your preferences. You can see, edit, and delete all of it in the Blue app.

Audio and voice. "Hey Blue" wake-word detection runs on your device; your microphone is not streamed to us while the phone is idle. When you talk to the assistant, your device opens a direct, encrypted connection to our voice provider (currently OpenAI) using a short-lived credential we mint, so your live audio goes from your phone to that provider and not through our servers; the transcript is saved to your conversation history. Dictation and voice notes are transcribed by our providers (currently Google and OpenAI). An open microphone hears whatever is in the room, including other people. Short clips around a wake-word detection are uploaded only if you turn on the option to help improve "Hey Blue" in Settings; it is off unless you turn it on.

Screen contents. When you ask Blue to operate an app for you, your device captures the current screen and the accessibility description of it and sends them to our servers, which

pass them to our AI provider to decide the next tap or keystroke. Whatever is on screen at that moment is captured, including content inside third-party apps. These captures are stored with the record of that task in your account so you can review what Blue did, and you can delete them. Separately, the assistant runs as an accessibility service so it can read on-screen text in the app you are using.

Notifications and installed apps. Blue reads the notifications your apps post, including their contents, in order to filter, group, and act on them. A list of the apps installed on your phone is sent to our servers when an assistant session starts.

Location. With your permission, Blue uses precise location, including in the background, for location-aware requests, for context, and for Find Phone. Coordinates are sent to a map service (currently OpenStreetMap Nominatim, Google Maps, Google Routes, and Google Weather or Open-Meteo for the specific request) to resolve a place name, and your location may be included in the context sent to our AI providers for a request that needs it.

Blue Vault. The Vault holds passwords, one-time-code seeds, payment cards, government identifiers such as a passport or Social Security number, and secure notes. How it is protected is described in Section 4.

Data from other apps on your phone. BlueOS includes a privileged component that can read another app's private data, for example the message database of WhatsApp. Only a short, non-sensitive default list is readable without your action. Anything else is readable only after you grant it in the Blue Data Access screen, and you can revoke a grant at any time.

Linked accounts. If you connect an account, we store the tokens needed to use it and the data it returns. Today this includes Google, where Blue may ask to read and send Gmail and to use your Google Calendar, Google Drive, and basic profile, and media services such as Spotify. Our use of information from Google APIs follows the Google API Services User Data Policy, including its Limited Use requirements. You can disconnect a linked account in Blue at any time, and from the provider's own settings.

Moving from an iPhone. If you migrate with the Blue Mac app, your Mac makes an encrypted iPhone backup and uploads it to our cloud. The Mac only ever handles ciphertext. Our servers decrypt the backup with the backup password you provide, hold that password only for the duration of the migration, import your photos, videos, messages, contacts, and files into your Blue account, and then delete the uploaded backup.

Usage and diagnostics. Which apps you open and when; a log of actions taken on the device; assistant task records including the tools used and their results; server logs and error reports; and update requests to our software update service, which identify the device model, the requested build, and the device's IP address.

Website and purchases. heyblue.com does not use advertising or analytics cookies. When you join a mailing list or waitlist, we store your email address and the country you give us on our own servers, and share them with our email provider (currently Loops) to send you the updates you asked for. Payments are processed by Stripe, which collects your card details

directly; we never see or store full card numbers, but we do receive order, contact, and shipping information.

Information about other people. Because Blue runs your phone, it necessarily handles information about people who are not Blue users: your contacts, the people who text and call you, people in your photos, people whose voices your microphone hears, and people whose information appears on your screen. See Section 9.

2. How we use your information

> **In short:** To make Blue work for you, keep it secure, and support you when you ask. Never to train AI models, never for advertising, never to sell.

- **To make Blue work for you.** To understand your requests and act on them, to sync your data across your Blue devices, to deliver messages and calls, to install and update apps and the operating system, and to remember what matters to you.
- **To keep Blue secure.** To detect and stop abuse, fraud, and unauthorized access, and to protect you, other users, and Blue.
- **To support you.** When you ask us for help, and only with your permission, a member of our team may look at the specific data needed to solve your problem.
- **To improve Blue.** We use aggregated, de-identified usage information, such as which features are used and how often things fail, to decide what to build and fix. This never involves reading your content.
- **To meet our legal obligations** and to establish, exercise, or defend legal claims.

We do not use your content, your conversations, your screen captures, your audio, or anything else you store on Blue to train AI models, and we do not allow our providers to. We do not use your data for advertising, and we do not sell it. If we ever want to use data from your account for anything beyond the purposes above, we will ask you first, and the answer "no" will cost you nothing.

3. Who else receives your information

> **In short:** The AI providers that power the assistant (OpenAI, Anthropic, Google), under contracts that forbid training on your data, and the infrastructure companies that run Blue for us. No one else, unless you choose a recipient or the law requires it.

AI providers. The assistant runs on models from third-party providers, currently OpenAI (voice and text sessions, transcription, some search), Anthropic (reasoning, screen-operation decisions, image understanding), and Google (transcription, image and video understanding, grounded search). For each request we send only what that request needs. Requests go out under Blue's own accounts with these providers, not yours, so they do not receive your Blue identity, and Vault-class secrets (passwords, codes, card and ID numbers) are redacted from assistant transcripts before they are stored or shared. Our agreements with these providers prohibit them from using your data to train their models or for any purpose other than serving our requests.

Service providers. Companies that run infrastructure for us under contract and only on our instructions: Amazon Web Services (compute, databases, and storage), Google Cloud (the hardware security module that seals Vault keys, and some infrastructure), Firebase (push notifications), Twilio (phone number verification and message routing), the map and weather services named in Section 1 (for the specific requests you make), Stripe (payments), and Loops (email).

Recipients you choose. When you send a message, place a call, share a file, or ask Blue to enter information into an app or website for you, that information goes to the recipient or service you chose.

Legal requirements. We may disclose information when the law requires it, or when we believe in good faith it is necessary to comply with a legal obligation, to protect someone's safety, or to protect Blue's rights. Where the law allows, we will tell you.

Business transfers. If Effortless Trading, Inc. is involved in a merger, acquisition, or sale of assets, your information may be transferred as part of that transaction. This policy will continue to apply to it, and we will tell you before any change.

We do not sell your personal information, and we do not share it for cross-context behavioral advertising, as those terms are defined under California law.

4. The Vault

> **In short:** Every secret is encrypted with its own key and your account key is sealed in a hardware security module. The assistant never sees a Vault secret; it can only ask the Vault to use one on your phone after your fingerprint or face. Vault is not zero-knowledge.

The Vault is where Blue keeps the things that must never leak: passwords, one-time-code seeds, payment cards, government identifiers, and secure notes.

- Every secret is encrypted with AES-256-GCM, and each encrypted value is bound to your account and that item, so it cannot be moved or substituted.
- The key that encrypts your secrets is itself sealed by a key held in a hardware security module in Google Cloud KMS. That key never leaves the module.
- Our main servers hold only ciphertext and have no permission to unseal it. A separate, restricted broker service is the only component that can, and every unseal is tied to your session, rate-limited, and written to an audit log.
- The assistant never receives Vault secrets. It can ask the Vault to use an item on your behalf, such as filling a password or a card into an app, and that happens on your phone after your fingerprint or face. The model behind the assistant only ever learns that the item was used.
- Titles, websites, and username hints are stored unencrypted so your Vault can be searched and displayed. Keep secrets in the secret field, not the title.

Vault is not a zero-knowledge system: because account recovery works through your Blue login rather than a separate passphrase, the broker is technically capable of unsealing your entries within its limits, and that capability is what the rate limits and the audit log exist to constrain. We think that is the right trade for a phone you cannot afford to be locked out of. If you need a store that we are cryptographically unable to open, use a separate password manager alongside Blue.

5. Where your data lives, and how long

> **In short:** In the United States, for as long as your account exists. Deleted items are gone from our active systems within 30 days, and a deleted account is gone from backups within about six weeks.

Your data is stored on infrastructure in the United States. Our AI providers and other service providers may process it in the United States and other countries under the safeguards described in Section 8.

We keep your data for as long as your account exists, so that Blue can keep working for you. Within that:

- **Items you delete** in a Blue app, including memories, conversations, task records, and screen captures, are removed from your view immediately and from our active systems within 30 days.
- **Wake-word clips** you have chosen to share are kept only as long as needed to improve detection and are never linked to your content.
- **iPhone migration uploads** are deleted when the migration completes or is abandoned, and the backup password is discarded with them.
- **Server logs and diagnostics** are kept for a limited period, normally no more than 90 days, and are not used to reconstruct your content.

When you delete your account, in Settings or by emailing hello@heyblue.com, we delete your data from our active systems within 30 days. Our backups are kept for 14 days and are overwritten on that schedule, so a deleted account is gone from backups within about six weeks. We may retain specific information for longer where the law requires it, or where we need it to resolve a dispute or enforce our agreements, and we will keep only what that purpose needs.

6. Security

> **In short:** a security-hardened Android base on the phone, encryption in transit and at rest, limited and logged access to production, and prompt notice if we are ever breached.

BlueOS is built on an open-source, security-hardened version of Android and keeps almost all of its protections, including verified boot, sandboxed Google Play, and per-app permission controls. A few of the strictest settings are off by default for convenience; you can turn them on in Settings. Blue blocks ad tracking by default.

Between your phone and our servers, and between our servers and our providers, data travels over TLS. At rest, your data is encrypted, and Vault secrets are encrypted again under the scheme in Section 4. Access to production systems is limited to the people who operate them, requires strong authentication, and is logged. We test and review our own security, we rotate credentials, and we keep tested backups.

No system is perfect, and we do not promise that Blue cannot be breached. If we learn of a breach that affects your data, we will tell you promptly and as the law requires.

7. What you control

> **In short:** Permissions, app-data access, Vault access, linked accounts, and everything Blue remembers about you. Export or delete your account at any time.

- **Permissions.** Grant or revoke microphone, camera, location, contacts, messages, and file permissions in Settings at any time. Revoking a permission turns off the features that need it.
- **Data Access.** Choose which other apps' private data the assistant may read, and revoke a grant at any time.
- **Memory.** See, edit, and delete everything Blue remembers about you, in the Blue app.
- **Vault.** Decide, item by item, whether the assistant may use a secret on your behalf. Revoking access takes effect immediately.
- **Linked accounts.** Disconnect Google, Spotify, or any other linked service at any time, in Blue or from the provider.
- **Sessions.** End an assistant or screen-operation session at any time to stop capture. You can also turn off "Hey Blue" entirely.
- **Wake-word improvement.** Off unless you turn it on.
- **Export and deletion.** Ask for a machine-readable copy of your account data, or delete your account, in Settings or by emailing hello@heyblue.com.

8. Your privacy rights

> **In short:** Access, correction, deletion, portability, and the right to complain, under California, other U.S. state, UK, and EU law. Email hello@heyblue.com to exercise them.

California. Under the California Consumer Privacy Act as amended, you have the right to know what personal information we collect, use, and disclose, to access it and get a copy, to correct it, to delete it, and not to be treated differently for exercising these rights. We collect the categories of personal information in Section 1, from you and your device, for the purposes in Section 2, and disclose them for business purposes to the categories of recipients in Section 3. Some of it is sensitive personal information: your precise location, the contents of messages where we are not the intended recipient, the account credentials, financial account information, and government identifiers you keep in the Vault, and voice recordings where applicable. We use sensitive personal information only to provide and secure the Service, which the law treats as a use you do not need to limit. We do not sell personal information or share it for cross-context behavioral advertising. We honor Global Privacy Control signals on our website.

Other U.S. states. If you live in a state with a comprehensive privacy law, including Colorado, Connecticut, Virginia, Texas, Oregon, and Montana, you have rights of access, correction, deletion, portability, and appeal, and the right to opt out of targeted advertising, sale, and certain profiling. We do none of those three.

Europe, the United Kingdom, and Switzerland. Where the GDPR or UK GDPR applies, our legal bases are performance of our contract with you, your consent (for the microphone, location, screen capture, linked accounts, and any special-category data), our legitimate interests in securing and improving the Service, and compliance with legal obligations. You have the rights of access, rectification, erasure, restriction, portability, and objection, the right to withdraw consent at any time without affecting earlier processing, and the right to complain to your supervisory authority. Transfers to the United States rely on the European Commission's standard contractual clauses or another lawful mechanism.

To exercise any right, or to appeal a decision we make, email hello@heyblue.com. We will verify the request against your account before acting on it, and we will respond within the time the law allows. An authorized agent may act for you with proof of authorization.

9. Other people's information

> **In short:** Blue handles data about people who have not agreed to this policy. Recording and consent laws are your responsibility.

Blue handles audio, screen contents, and messages that involve people who have not agreed to this policy. Many places, including California, require the consent of everyone in a recorded conversation, and other laws restrict sharing another person's information. You are responsible for following those laws, for telling the people around you when Blue may be listening or capturing the screen, and for not using Blue to capture conversations or records you do not have the right to capture.

10. Children

> **In short:** Blue is for adults, 18 and older.

Blue is for adults. You must be 18 or older to have a Blue account, and we do not knowingly collect personal information from anyone under 18. If we learn that we have, we will delete it.

11. Changes to this policy

> **In short:** At least 30 days' notice before a material change, and changes never say less than this policy does today.

When we change this policy in a way that matters, we will post the new version on heyblue.com, update the effective date, and give you at least 30 days' notice in Blue or by email before it takes effect, unless a shorter period is required for legal or security reasons. Where the law requires your consent to a change, we will ask for it. Changes will never make this policy say less than it does today about what we do with your data.

12. Contact

> **In short:** hello@heyblue.com.

Effortless Trading, Inc.
Santa Clara, California
hello@heyblue.com