

Privacy Policy

Version 1.2.3 · Effective September 1, 2026

1. Who we are, and how to read this

Tero is estate-management software for private households, operated by **Tero Household Operations LLC**, a New York limited liability company at 57 Harbor View Avenue, East Hampton, NY 11937, USA ("Tero", "we", "us"). For any question about this policy or your data, write to **andrew@tero.live**.

Two words carry this whole policy. The **Customer** is the person or legal entity that subscribes to Tero under an Order Form or subscription agreement — typically the household's principal, a family office, or a management company. **Authorized Users** are the individual people the Customer gives accounts to: principals, estate managers, and household staff. If you are reading this as someone with a Tero login, you are an Authorized User.

2. Two kinds of data, two different roles

Customer Data is everything a household puts into its Tero workspace: tasks and their history, procedures, expenses, maintenance records, inventory, wines, wardrobe, vendor details, guest information, staff activity within the workspace, and the rest of the household's operational content. For Customer Data, **Tero processes only on documented instructions** — in legal terms, the Customer acts as controller or, where the Customer itself serves another controller (a management company or family office administering a principal's household, for example), as processor; Tero acts as processor or subprocessor respectively. The Data Processing Addendum that forms part of every subscription governs this in detail, automatically — it is not an optional extra.

Account and operational data is the narrower set of information Tero uses for its own limited purposes: the name, email address, phone number, and language of each Authorized User account; authentication and account administration; the records of which document versions were presented to and acknowledged or accepted by each person; billing and subscription records for the Customer; support correspondence; the security and technical data described in section 7; and what the law requires us to keep. For these, Tero is the controller.

Some data serves both purposes — an Authorized User's email address is account data to Tero and workspace content to the household that lists its staff. Where that happens, Tero uses the element for its own purposes only within the narrow list above, and in every other respect treats it as Customer Data.

3. What the workspace typically contains

Households record operational details about people who never touch the app: **guests** (names, visit preferences, stay dates, contact details, and — importantly — allergies and dietary restrictions), **vendors** (business contact details and work performed), and household members.

Allergy and similar health-related information can be special-category or sensitive data under some laws. The Customer decides to record it and is responsible for having the lawful basis — and, where applicable, the explicit-consent or other condition such data requires — along with any notices or permissions owed to the people concerned. Tero stores and displays it on the Customer's instructions and applies the safeguards in the Security Exhibit. Tero does not independently use allergy or other sensitive information for advertising, model training, profiling, or any unrelated purpose. When an Authorized User invokes a feature that processes relevant workspace data — asking the search bar a question, or importing documents — that data may be transmitted to the applicable subprocessor solely to provide the requested feature, under the Customer's instructions and the DPA; the no-generalized-AI-training promise applies throughout.

Keep high-risk data out. Tero is not designed to hold Social Security or other government identification numbers, passport numbers, complete medical records, financial account numbers or credentials, or alarm and access codes. Do not enter them unless a Tero feature expressly supports and says it is authorized for that information. (For subscription accounts, Tero deliberately stores only *where* a password is kept — never the password.)

4. Why Tero processes data

- **To provide the service** — processing Customer Data on the Customer's

instructions under the subscription contract.

- **To run Authorized User accounts** — authentication and administration

(performance of a contract), and the records of which document versions were presented to and acknowledged or accepted by each person — kept in our legitimate interests in documenting agreements and compliance and in establishing, exercising, or defending legal claims. Acknowledging this policy is how we show it to you; it is a notice, not a consent — where processing needs a lawful basis, that basis is the one named in this policy, never the acknowledgment itself.

- **To send reminders a person chose** — email, text, or push, each

individually opted into and revocable (consent).

- **To bill the Customer and keep legally required records** (contract;

legal obligation).

- **To secure and support the service** — the technical data in section 7,

rate limiting, abuse prevention, and answering support requests (legitimate interest in running a safe service).

Tero does not sell personal data, does not use Customer Data for advertising, and does not use Customer Data to train generalized AI models.

5. AI features, named precisely

Currently, the following features transmit content to Anthropic, PBC's Claude API when an Authorized User invokes them: (1) reading a photographed receipt to draft an expense entry; (2) answering a question typed into the search bar using the estate's own data; (3) reading uploaded spreadsheets and document photos during onboarding to propose records, none of which become real until a person approves them; (4) assistance with household procedure documents; and (5) translating entered content between staff languages.

Anthropic processes this content as Tero's subprocessor, solely to return the feature's result. Under Anthropic's commercial API terms, inputs and outputs are not used to train Anthropic's generalized models. Anthropic retains API inputs and outputs for a limited operational period under those terms; Tero has not entered a zero-retention arrangement and therefore does not promise one.

6. Text messages (SMS)

If an Authorized User opts in to reminders by text message: mobile phone numbers and SMS opt-in data are **not shared with or sold to third parties or affiliates for marketing or promotional purposes**; text-messaging originator opt-in data and consent are not shared with any third party except our SMS delivery provider (Twilio), solely to deliver the messages. Message frequency varies. Message and data rates may apply. Reply **STOP** at any time to opt out and **HELP** for help. Opt-in happens through a form inside the app, each opt-in and opt-out is recorded, and consent can be withdrawn at any time in account settings or by replying STOP.

7. Technical and security data

Like any online service, Tero's infrastructure keeps technical records: IP addresses, browser and device information, timestamps, request and server logs, sign-in attempts, and error logs. Tero has no analytics or advertising trackers — but "no trackers" does not mean "no logs": these records exist, are used only for security, abuse prevention, troubleshooting, and service delivery, and are kept for the short operational periods described in section 11.

8. Who helps us run Tero

Tero uses a small set of subprocessors — currently Supabase (database and authentication, on AWS), Vercel (application hosting), Resend (email, operated by Plus Five Five, Inc.), Twilio (SMS), and Anthropic (the AI features above). Vercel's own data-processing terms restrict sensitive and special-category data; until that restriction is resolved for Tero's request path, Tero does not represent Vercel as approved for special-category Customer Data. Push notifications travel through the push service built into the user's own browser platform (operated by Apple, Google, or Mozilla); notification payloads are encrypted end-to-end to the user's device, and those platforms also handle the device registration identifiers routing requires. Tero currently treats them as platform transmission services rather than subprocessors; their role is described in the Subprocessor List. The current **Subprocessor List**, with purposes and locations, is available to every Customer and forms part of the Data Processing Addendum, which also governs notice of changes and the Customer's right to object.

These providers process Customer Data to deliver their service to Tero. Each may also process limited data as needed for its own security, abuse prevention, support, and legal compliance, as permitted by its agreement with Tero — but none may use Customer Data for advertising, sell it, or use it to train generalized AI models.

9. Where data lives, and international transfers

Tero's primary database storage is in the United States (AWS us-east-1, Northern Virginia, via Supabase). Processing by Tero's subprocessors may occur in other locations — for example, content delivery through Vercel's edge network and push delivery through the platform of the user's browser vendor — as described in the Subprocessor List.

For Customers in the EEA, the transfer of Customer Data to Tero in the United States is safeguarded through the mechanisms in the Data Processing Addendum, which incorporates the European Commission's 2021 Standard Contractual Clauses (controller-to-processor module). For UK Customers, the EU clauses alone are not sufficient: the DPA additionally incorporates the UK International Data Transfer Addendum for UK restricted transfers, and addresses Swiss requirements where applicable. Onward transfers to subprocessors are covered by equivalent safeguards in Tero's agreements with them.

10. Security incidents — who tells whom

For **Customer Data**, where Tero acts as processor: Tero will notify the affected Customer without undue delay after becoming aware of a personal data breach affecting their Customer Data, and will reasonably assist the Customer with the Customer's own notification duties to regulators and individuals. Whether and when regulators or individuals must be told is the controller's determination under applicable law.

For **account and operational data**, where Tero is the controller: Tero will make the notifications applicable law requires of it, to regulators and affected people, within the timeframes that law sets.

11. How long data is kept

- **Customer Data:** for the life of the subscription. After termination,

the Customer may export its data for **30 days**; Tero then deletes it from primary systems within **30 days** of the export window closing, except where law requires retention.

- **Backups:** deleted information is removed from active systems;

backup copies remain outside ordinary operational use until they expire under the documented lifecycle — the database provider's rolling daily backups, and Tero's independent weekly backups on a rolling 365-day automated lifecycle. Backups are used only for disaster recovery, and if one containing deleted data is ever restored, deletion is re-applied before normal use where technically and operationally appropriate.

- **Erase requests during a subscription:** an erased person's profile

is pseudonymised (name, email, phone removed), unlinking them from every record at once; their push registrations are deleted outright.

- **Audit log and task history:** retained as append-only accountability

records for the life of the Customer's workspace, unlinked from erased people.

- **Presentation and acceptance records:** which document versions a

person was shown and acknowledged or accepted, retained for as long as needed to evidence the agreement and defend legal claims.

- **Expense records in the workspace:** these are Customer Data — their

retention follows the Customer's instructions and the termination/export/deletion provisions like the rest of the workspace. An erasure request for a person unlinks them from expense entries rather than deleting the entries, because the household's financial history belongs to the Customer; whether tax or accounting law requires the Customer to keep those records is the Customer's own obligation.

- **Tero's own business records:** Tero's invoices to the Customer,

payment, accounting, and tax records are Tero's corporate records, retained for the periods law and legitimate business needs require — independent of workspace content.

- **Technical logs** (section 7): short operational periods set by the

relevant provider, typically days to weeks, not years.

- **Support correspondence:** kept while relevant to the relationship.

12. Your rights

Tero provides these controls to every Authorized User regardless of where they live, for the data Tero controls (your account identity and contact details, reminder preferences, document presentation and acceptance records, and support correspondence): access to and a machine-readable export of that data; correction of inaccurate account details; erasure with the narrow, explained exceptions in section 11; and withdrawal of each reminder channel's consent at any time in account settings. Workspace content connected to you — tasks, expenses, activity history — is Customer Data, and Tero does not disclose it independently: requests that reach into the workspace are answered together with the Customer, as below. Requests reach us at andrew@tero.live; we may verify identity first, and we respond within the timeframe applicable law sets (and within one month where the GDPR applies).

Because most workspace data belongs to the Customer, requests from guests, vendors, or household members about Customer Data are answered together with the Customer: as processor, Tero refers the request to the Customer and assists them, or acts on the Customer's documented instructions — dedicated erasure flows exist for guests and vendors.

Depending on where you live, you may have additional rights under applicable local law — including under EU or UK data protection law where it applies to a given household's processing — and the right to complain to your local supervisory authority. Nothing about Tero's voluntary worldwide controls waives or replaces those laws where they apply.

13. Children

Tero is a workplace tool. It is not directed to children, and children should not create Tero accounts. A Customer may, however, record information about minors in its workspace — a visiting child's allergy is exactly the kind of thing a careful household writes down. Such information is Customer Data: the Customer is responsible for the lawful basis and any parental notices or permissions required, and Tero processes it solely as the Customer's processor under the safeguards in this policy and the DPA.

14. Changes to this policy

Every version of this policy is kept with its dates in force. If we change its meaning, every Authorized User is presented with the new version and asked to acknowledge it before continuing to use Tero; typo-level fixes do not re-prompt. Where a change affects the Customer relationship, notice is given as the subscription agreement provides.

15. Contact

Tero Household Operations LLC 57 Harbor View Avenue, East Hampton, NY 11937, USA
andrew@tero.live

© 2026 Tero Household Operations LLC. All rights reserved.