

Privacy Policy

Vaethra

Issued 11 October 2026

The current version of this document is always at vaethra.com

security@vaethra.com · vaethra.com/trust

Privacy Notice

LAST UPDATED 11 OCTOBER 2026

The short version. The Vaethra Terminal and Atropos set **no cookies** and ask for no account. We do not build a profile of you, and we do not sell, rent or share your data with advertisers. There is no advertising script anywhere. The public products — this site, the Terminal and Atropos — carry Cloudflare Web Analytics, which is cookieless and sets nothing (see §5); the Terminal keeps its own first-party page counts, and the launch-case pages count a few named actions with no identifier (§3). The customer workspace and the operator console carry no third-party script at all. The one place a person signs in is the customer workspace (§7).

This notice describes what happens to information when you use vaethra.com, terminal.vaethra.com, atropos.vaethra.com, api.vaethra.com and workspace.vaethra.com (together, the “Services”). It is written to be checked against the software rather than to be taken on trust.

1. Who we are

The controller of any personal data described in this notice is **Vaethra Technologies LLC**, a limited liability company organised under the laws of the State of Wyoming, United States, with its mailing address at 30 N Gould St Ste N, Sheridan, Wyoming 82801, United States.

Data protection enquiries: privacy@vaethra.com. Where we process personal data on a customer's behalf rather than our own, that customer is the controller and we are the processor; the terms of that processing are in the [Data Processing Agreement](#).

2. No cookies, and no consent banner

The Services set no cookies of any kind — not for analytics, not for advertising, not for sessions. That is why you are not asked to accept anything when you arrive. The workspace keeps its sign-in session in your browser's local storage rather than in a cookie.

The Terminal also uses your browser's **local storage**, which stays on your device and is never transmitted to us. It holds only the choices you make while using the app:

- your panel layout and whether you are in simple or full view;
- your watchlist, and which items you have already seen;

- your daily-brief preference and reading-density setting;
- a random token that owns any webhook alert rules you create (see §6).

On [vaethra.com](#), the launch-case pages keep a note in your browser's **session storage**, for the life of the tab, of which actions they have already counted, so that reloading the page does not count it twice. It is never sent to us and it is gone when the tab closes.

Clearing your browser storage erases all of it. Nothing there identifies you.

3. What our servers record

Page and error counts

To know whether the Services are working and being used, the Terminal sends a small first-party message to our own API when a page loads, and if a part of the interface fails to render. We built this instead of installing a hosted analytics tag precisely so that this data never leaves our infrastructure.

RECORDED	NOT RECORDED
The page route (for example <code>/</code>)	Your IP address
The referring website's host (for example <code>news.ycombinator.com</code>)	Any cookie, identifier or device fingerprint
A two-letter country code	The query string — so anything you type into the filter or search box is never sent
An error message and which panel produced it	Your browser's user-agent string
	Anything from your local storage

These are stored only as **aggregate counts**. There is no record that ties one page view to another, so we cannot reconstruct an individual's session even if we wanted to. Daily counts are kept for 90 days.

Launch-page action counts

The live case pages ([/live](#) and the case page it links to), the home page's route form and the research form on [/access](#) send a short first-party message to our own API when one of a fixed list of actions happens: the page loads, the case is opened, an evidence drawer is opened, a link to the Terminal or Atropos is followed, a form is started, or a form is accepted by our server.

The name of the action	Your IP address
The day, in UTC	Any cookie, identifier or device fingerprint
A campaign code from the link you arrived by, only if it is a short lower-case code	Anything you typed into a form, and the reference you were given
Phone, tablet or desktop, from the window width	The rest of the link's query string
The case and snapshot version, and for an evidence drawer its evidence class	Your browser's user-agent string

They are stored only as **aggregate counts** per day. Nothing ties one action to another or to a form submission, so we cannot tell whether two counts came from one person or from two, and we cannot count returning visitors. The counts are kept for 120 days.

Rate limiting and abuse handling

Our API applies a rate limit of 600 requests per minute per client address to keyless callers, and per key at the key's rate to keyed ones, to keep the public service available. To do that it must look at the requesting IP address, which the rate limiter uses in the moment and does not store. When the API **refuses** a request — no key, a wrong key, a rate limit — it records the path, the status and a **salted, truncated digest** of the requesting address, deduplicated, so that abuse can be recognised without keeping the address itself. That digest cannot be turned back into an address without the secret it was salted with, and it is deleted after 12 months. Cloudflare, our hosting provider, processes IP addresses on our behalf as part of delivering and protecting the Services, under its own terms as our processor.

Requests made with an API key

Every request made with an issued key is recorded against that key — path, query, status, row count, bytes and timing — for billing, abuse handling and incident reconstruction, and kept for 12 months. That record is about an integration, not a person; the key's owner is the customer organisation.

4. The forms

If you write to us through the enquiry form on [/access](#), we store what you typed — your name, email address, organisation if given, what the enquiry is about, and your message — with the page it was sent from, the site that referred you if any, and the same salted digest of your address described above. We keep an enquiry until it is answered and closed, and delete it on request at any time.

If you **send a route or asset** (on [/live](#), the case page or the home page), we store the five things the form asks for — your email address, origin, load point, destination and latest acceptable arrival — with the page it was sent from, a campaign code if the link carried one,

whether the challenge was passed, and the salted digest of your address. A person reads it and replies to you.

If you **request research access** on [/access](#), we store your name, work email, affiliation, purpose, the capability and API areas you ask for, the volume and any deadline you give, and that you acknowledged the licence terms, with the same provenance fields. If access is granted, the grant, its scopes and its expiry are recorded against the account you then sign in with (§7).

All three go into our own database, not a third-party form service, and each sends one notification to our own mailbox (§5). None of what you type is sent to any analytics. A route request or a declined research request is deleted twelve months after it is closed; a granted one is kept for as long as its grant record is, because the grant has to be explainable. Any of them is deleted on request at any time.

The forms carry a Cloudflare Turnstile challenge (§5), verified on our side and never stored, which limits automated submissions: a submission that could not complete the challenge is accepted a few times an hour per sender and marked for a person to check.

5. Third parties that can see your IP address

Some parts of the Services load resources directly from other providers. When your browser fetches those, that provider necessarily sees your IP address. We send them nothing about you beyond the request itself.

PROVIDER	WHAT FOR	WHEN
Cloudflare	Hosting, delivery, rate limiting	Always
Cloudflare Web Analytics	Cookieless page counts. No cookie, no cross-site identifier, no profile, and nothing that identifies you as an individual. Placed on the page by us, not injected by the platform, so it runs exactly where this row says.	Every page of this site, the Terminal and Atropos. Not the customer workspace, not the operator console.
Cloudflare Turnstile	The anti-spam challenge on the enquiry form. It inspects the browser to decide whether you are automated.	Only on pages with a form. On /access it loads with the page; on /live , the case page and the home page it loads only once you start filling in the route form.
Vaethra Terminal and Atropos	The home page embeds the two live products as framed panels rather than screenshots, so your browser loads them from their own subdomains. Same operator, same policy as this site.	Home page only, and lazily — not until the frame scrolls near
CARTO	Base map tiles	When the map is shown
Esri / ArcGIS	Satellite map tiles	When the satellite layer is shown
OpenMapTiles	Map label fonts	When the map is shown
airplanes.live	Live aircraft positions	Not contacted: the aircraft layer has been in maintenance since 15 September 2026

Two more parties process data on our behalf without ever seeing a visitor's browser: **Supabase** (on Amazon Web Services, United States) hosts our database, and **Proton AG** (Switzerland) hosts every @vaethra.com mailbox, so anything you email us, and any enquiry once it is forwarded to us, is held there. The full list, with each party's attestations, is at </security/subprocessors>.

6. Webhook alerts

If you create an alert that posts to a webhook, we store the rule, the webhook URL you supplied, and a **SHA-256 hash** of a random token your browser generated to own it. We never store the token itself, so a copy of our database could not be used to read or edit anyone's rules. There is no email address and no account. If you lose your browser storage, the rule is orphaned rather than exposed, and an orphaned rule is deleted 120 days after its last delivery attempt. Webhook URLs must be HTTPS and may not name a literal private or internal network address.

7. The workspace

The customer workspace is the one part of the Services with accounts. It is for the staff of an organisation that licenses the API, and it holds their **sign-in email address**, the sign-in session and second-factor records the sign-in provider keeps, their role in the organisation, and a record of the administrative actions they take — issuing or revoking a key, inviting a member — with the actor, the time and the reason. That record is append-only. The organisation is the controller of what its staff do there; we process it on its behalf under the [Data Processing Agreement](#), and a membership is deleted when the organisation removes it.

8. What we publish is about the world, not about you

The events, indicators and forecasts in the Terminal are drawn from public data sources — official advisories, coded conflict datasets, satellite and vessel data, market prices and press reporting. Each record carries its source and timestamp. This material describes places, organisations and infrastructure. It is not derived from, and has nothing to do with, the people who visit the site.

9. Where data is processed

The Services run on Cloudflare's global network and on Supabase (PostgreSQL, hosted on Amazon Web Services in the United States). Because Cloudflare serves from the location nearest you, requests are usually handled in your own region. Mail is held by Proton in Switzerland. Transfers from the EEA and the UK rely on the 2021 Standard Contractual Clauses and the UK Addendum, incorporated in the [DPA](#).

10. Your rights

Depending on where you live, you may have rights to access, correct, delete or port personal data, or to object to its processing. What we hold about a visitor is very little: no account, no cookie, no stored address, and no profile. What we hold about an enquirer is the enquiry; about a workspace member, the sign-in address and the administrative record. To exercise a right, or to have a webhook alert or an enquiry removed, write to privacy@vaethra.com. We answer within one month.

You may also complain to a data protection authority. We are established in the United States and have no lead authority of our own, so the competent authority is the one where you live or work — your own national supervisory authority in the EEA, or the Information Commissioner's Office in the UK.

We have not appointed a representative in the Union or in the United Kingdom under Article 27. We rely on the exemption in Article 27(2): the personal data we process as a controller —

an enquiry, a webhook destination, the salted digest of a refused request — is processed occasionally, includes no special-category data, and is unlikely to result in a risk to you. If that changes, a representative's name and address will appear here.

11. Children

The Services are not directed at children and we do not knowingly collect information from them.

12. Changes

If this notice changes materially we will update the date at the top. The Services are open about their own behaviour: what is described here is implemented in the code that runs them.