

Privacy Policy

Vaethra

Issued 8 September 2026

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

security@vaethra.com · vaethra.com/trust

Privacy Notice

LAST UPDATED 28 AUGUST 2026

The short version. Vaethra Terminal sets **no cookies** and asks 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 Terminal runs no third-party analytics at all — its page counts are first-party and cookieless.

This notice describes what happens to information when you use vaethra.com and terminal.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 Terminal does use 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).

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

The page route (for example /)
The referring website's host (for example news.ycombinator.com)
A two-letter country code
An error message and which panel produced it

NOT RECORDED

Your IP address
Any cookie, identifier or device fingerprint
The query string — so anything you type into the filter or search box is never sent
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.

Request logs and abuse prevention

Our API applies a rate limit of 600 requests per minute per client to keep the public service available. To do that it must look at the requesting IP address. The IP is used for that check **in the moment and is not written to any database by us**. 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.

4. 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
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	Only if you switch the aircraft layer on — it is off by default

5. 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.

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. Webhook URLs must be HTTPS and cannot point at private or internal network addresses.

7. Where data is processed

The Services run on Cloudflare's global network and on Supabase (PostgreSQL, hosted in the United States). Because Cloudflare serves from the location nearest you, requests are usually handled in your own region.

8. 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. In practice we hold almost nothing to which those rights could attach: no account, no cookie, no stored IP address, and no profile. If you have created a webhook alert and want it removed, or you have any question about this notice, contact us at privacy@vaethra.com.

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.

9. Children

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

10. 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.