

World Monitor privacy policy and data handling

World Monitor · version **2026-08-20** · Authoritative text: <https://www.worldmonitor.app/docs/privacy> · Previous versions: <https://github.com/koala73/worldmonitor/commits/main/docs/privacy.mdx>

Last updated: 20 August 2026

Download: [PDF](#) · [Markdown](#)

This Privacy Policy explains how **World Monitor FZ LLC, a free zone limited liability company registered in Dubai, United Arab Emirates** ("World Monitor", "we", "us"), handles information when you use the World Monitor dashboard, website, API, MCP server, and apps (the "Service").

This page is written in plain language and is not legal advice.

The short version

- The basic dashboard works **without an account and without signup**.
- We do not sell your personal data.
- We use a small set of established subprocessors for authentication, payments, hosting, error monitoring, and AI analysis — listed in full below.
- You can request access to, export of, or deletion of your account data at any time.

Information we collect

Account information. If you create an account or upgrade to Pro, our authentication providers (Clerk and WorkOS) process your email address, name, and login credentials. We store account identifiers and your plan/entitlement state in our database (Convex).

Payment information. Subscriptions are processed by Dodo Payments, which acts as the merchant of record. Your full card details are entered with and held by the payment processor — **World Monitor never receives or stores your full card number**. We receive limited billing metadata (such as plan, status, country, and the last four digits) needed to manage your subscription.

Usage and diagnostics. To keep the Service reliable we collect:

- **Error and crash diagnostics** via Sentry (e.g. error messages, stack traces, browser and device type).
- **Aggregate, privacy-oriented analytics** via Vercel Web Analytics, Cloudflare, and our self-hosted Umami instance (`abacus.worldmonitor.app`) — used to understand traffic patterns. These are designed to avoid cross-site tracking, and where configured are cookieless.
- **Page-performance monitoring (RUM)** via DebugBear on a 10% sample of page loads. It receives the page path, viewport and device pixel ratio, navigation and web-vitals timings, and the user agent, along with the IP address inherent in any web request. **URL query parameters are not collected**

— the dashboard state your address bar carries (map view, time range, selected layers) is not part of what DebugBear stores. It is used to find slow and unstable pages, not to identify or track you.

- **Server and request logs** via Axiom and our hosting/CDN providers (Vercel, Cloudflare), including IP address, user agent, and request metadata, retained for security and debugging.

Content you submit to AI features. When you use AI briefings, analysis, forecasts, or the research assistant, the text of your query and the relevant context are sent to our AI providers (Anthropic and, via OpenRouter, other model providers) to generate a response. Do not submit sensitive personal data into AI prompts.

Preferences and alerts. Settings such as saved locations, alert rules, and layer preferences are stored in your browser (local storage) and, for signed-in users, in our database (Convex).

Cookies and local storage

- **Essential** — authentication sessions (Clerk/WorkOS) and security use cookies or equivalent storage that are required for signed-in features to work.
- **Preferences** — dashboard settings are stored locally in your browser.
- **Analytics** — our analytics are designed to be privacy-friendly and, where configured, do not use tracking cookies.

Data Processing Addendum

If you use the Service to process personal data and need a processor agreement, the [Data Processing Addendum](#) applies automatically — no signature required — and incorporates the EU standard contractual clauses and the UK addendum for international transfers. A countersigned copy is available on request.

Subprocessors

We share personal data only with service providers that process it on our behalf to run the Service. The table also names the one analytics collector we host ourselves, so it can be reconciled against anything you see in a network log:

Provider	Purpose
Clerk	Authentication and account management
WorkOS	Authentication, OAuth, and enterprise/agent sign-in
Convex	Application database (accounts, entitlements, alerts, preferences)
Dodo Payments	Payment processing and subscription billing (merchant of record)
Sentry	Error and crash monitoring
DebugBear	Real-user page-performance monitoring (10% sample)

Provider	Purpose
Umami (self-hosted, <code>abacus.worldmonitor.app</code>)	Product analytics on our own infrastructure — no third party receives this data
Upstash	Rate-limit and cache store; rate-limit keys are derived from your IP address
Railway	Container hosting for our analytics service and for notification delivery
Mintlify	Documentation site hosting (<code>worldmonitor.app/docs</code> , including this page)
Vercel	Application hosting and web analytics
Cloudflare	Content delivery, edge security, bot challenges (Turnstile), and web analytics
Axiom	Application logging and observability
Anthropic	AI model provider for analysis and briefings
OpenRouter	AI model routing for analysis and forecasts
Resend	Transactional email delivery

Where your alerts go

If you connect an alert or digest channel, we transmit the alert content you asked for to the destination **you** chose: Telegram, Slack, Discord, a webhook URL of yours, email, or a browser push endpoint. To do that we store the identifiers that channel needs — a chat or channel id, a webhook URL, or the OAuth token you granted us — and nothing more.

Those destinations are not our subprocessors: they receive your alerts because you directed them to, and what they do with the content is governed by your own relationship with them. Disconnecting a channel deletes the identifiers we hold for it.

How we use information

We use the information above to operate and secure the Service, authenticate users, process subscriptions, generate AI analysis you request, communicate with you about your account, and improve reliability and performance. We rely on legitimate interests, contract performance, and — where applicable — your consent as the legal bases for this processing.

Data retention

We keep account and subscription data for as long as your account is active and as needed to meet legal, tax, and security obligations. Diagnostic and log data is retained on a rolling basis for a limited period. When you delete your account, we delete or anonymize associated personal data, except where we must

retain it by law.

Your rights

Depending on where you live (including under the EU/UK GDPR and the California CCPA/CPRA), you may have the right to access, correct, export, or delete your personal data, and to object to or restrict certain processing. To exercise any of these rights, contact us at support@worldmonitor.app. You also have the right to complain to your local data protection authority.

International transfers

Our subprocessors may process data in countries other than yours, including the United States. Where required, transfers are covered by appropriate safeguards such as standard contractual clauses.

Children

The Service is not directed to children and is not intended for use by anyone under the age required by their local law to consent to data processing. We do not knowingly collect personal data from children.

Changes

We may update this policy as the Service evolves. Material changes will be reflected here with a new "Last updated" date.

Contact

Questions about this policy or your data: support@worldmonitor.app.