World Monitor Data Processing Addendum (DPA)

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

Last updated: 20 August 2026

Download: PDF · Markdown

This Data Processing Addendum ("DPA") applies where you use the Service to process personal data and, in doing so, act as a controller and we act as your processor. It forms part of the Terms of Service and the End User License Agreement, and is made between you and **World Monitor FZ LLC, a free zone limited liability company registered in Dubai, United Arab Emirates** ("World Monitor", "we", "us").

You do not need to sign anything for this DPA to apply. It takes effect automatically when the Service processes personal data on your behalf. If your procurement process needs a countersigned copy, write to privacy@worldmonitor.app and we will provide one.

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

1. The short version

The Service is built so that it does not need personal data to do its job. Monitoring runs on **customer-declared static coordinates** — a site, a facility, a route, a region — not on people. It does not require, and is not designed to receive, the names, locations, itineraries, or contact details of the individuals a customer cares about. That is a structural difference from tools that track travellers or staff, and it is worth stating first because it determines how little of what follows applies to most customers.

What we do process on your behalf is narrow: the account details of the people you authorize to use the Service, the technical data any web request carries, and whatever content you choose to submit.

2. Definitions

- **Applicable Data Protection Law** — the EU GDPR, the UK GDPR and Data Protection Act 2018, the Swiss FADP, the California Consumer Privacy Act as amended by the CPRA and comparable US state privacy laws, Canada's PIPEDA, the UAE Federal Decree-Law No. 45 of 2021, and any other data protection law that applies to processing under the Agreement.
- **Personal Data** — personal data, personal information, or equivalent, as defined by Applicable Data Protection Law, that we process on your behalf under the Agreement.
- **Data Subject**, **Controller**, **Processor**, **Subprocessor**, **Processing**, **Personal Data Breach** — as defined in the GDPR, and read to include their equivalents under other Applicable Data Protection Law.

- **SCCs** — the standard contractual clauses approved by the European Commission in Decision 2021/914, Module Two (controller to processor).
- **UK Addendum** — the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018.
- **Agreement** — the Terms of Service, the End User License Agreement, and any order form between us.
- **Restricted Data** — special categories of personal data under Article 9 GDPR, criminal-offence data, government identifiers, financial-account or payment-card numbers, precise geolocation of an identified individual, children's data, and any data whose loss would require breach notification to a regulator on its own.

3. Roles and scope

You are the controller and we are the processor for the personal data described in Annex 1. Where you are yourself a processor for another controller, we act as subprocessor and this DPA applies as if references to you were references to that controller.

We are a controller, not your processor, for the data we process to run our own business: account and subscription records, billing metadata, security and diagnostic logs, and product analytics. That processing is described in the Privacy Policy and is outside this DPA.

This DPA applies for as long as we process personal data on your behalf, and survives the Agreement until that processing ends.

4. Your instructions

We process personal data only on your documented instructions, which are: the Agreement, this DPA, your configuration of the Service, and any further written instruction you give that is consistent with the Agreement.

We will tell you if, in our opinion, an instruction infringes Applicable Data Protection Law, and may suspend that processing until it is resolved.

If we are required by law to process personal data other than on your instructions, we will tell you before doing so unless that law prohibits it.

5. Confidentiality and personnel

Anyone we authorize to process personal data is bound by confidentiality, is granted access on a least-privilege basis, and receives access only for as long as they need it.

6. Security

We implement appropriate technical and organizational measures, described in **Annex 3**, taking into account the state of the art, the cost of implementation, and the risk to data subjects.

Personal Data Breach. If we become aware of a personal data breach affecting personal data we process on your behalf, we will notify you **without undue delay, and in any event within 72 hours**. The notification will describe what we know: the nature of the breach, the categories and approximate volume of data affected, the likely consequences, and the measures we have taken or propose to take. We will provide reasonable assistance with your own notification obligations. Our notice is not an admission of fault.

7. Your responsibilities

- You are responsible for the lawfulness of the personal data you submit and of your instructions, including having a valid legal basis and giving any notices data subjects are owed.
- **Do not submit Restricted Data to the Service** without our prior written agreement. The Service is not designed for it, and the Privacy Policy tells users not to place sensitive personal data into AI prompts.
- You are responsible for the security of your own credentials and API keys, and for the destinations you configure for alerts and webhooks. Content sent to a destination you choose — Telegram, Slack, Discord, an email address, a webhook of yours — is transmitted at your direction and leaves our control on delivery.

8. Subprocessors

You give us general authorization to engage subprocessors. **The current list is the subprocessor table in the Privacy Policy**, which is the single place we maintain it — it is not duplicated here, so it cannot fall out of date relative to what actually runs.

We impose data protection obligations on each subprocessor that are no less protective than those in this DPA, and we remain liable to you for their performance.

Changes. We will give at least 30 days' notice before a new subprocessor starts processing personal data, by updating that table and, where you have asked to be told, by email to your account address. If you have a reasonable objection on data protection grounds, tell us within those 30 days and we will work with you in good faith; if we cannot resolve it, you may terminate the affected subscription and we will refund the pro-rata portion of prepaid fees.

9. Data subject rights

Taking into account the nature of the processing, we will assist you with requests from data subjects — access, rectification, erasure, restriction, portability, and objection — by providing the functionality in the Service and, where that is not enough, reasonable additional assistance.

If a data subject contacts us directly about data we process on your behalf, we will not respond substantively; we will tell them to contact you, and tell you promptly.

We will also give you reasonable assistance with data protection impact assessments and prior consultations with a supervisory authority, so far as they relate to our processing.

10. International transfers

We and our subprocessors process personal data in countries other than yours, including the United States and the European Union.

Where personal data is transferred out of the EEA, the UK, or Switzerland to a country without an adequacy decision, the transfer is governed by the **SCCs**, which are incorporated into this DPA by reference and which the parties are deemed to have signed:

- Module Two applies where you are a controller and we are your processor; Module Three applies where you are a processor and we are your subprocessor.
- Clause 7 (docking) applies. Clause 9 uses **Option 2**, general written authorization, with the 30-day notice period in section 8. Clause 11 does not use the optional independent dispute-resolution body. Clause 17 selects the law of Ireland; Clause 18(b) selects the courts of Ireland.
- Annexes I, II and III of the SCCs are populated by **Annex 1**, **Annex 3**, and the subprocessor table in the Privacy Policy respectively.
- For UK transfers, the **UK Addendum** applies to the SCCs, with Tables 1–3 populated as above and Table 4 selecting "neither party".
- For Swiss transfers, references to the GDPR are read as references to the FADP, and the Swiss Federal Data Protection and Information Commissioner is the competent authority.

11. Audits and evidence

We will make available the information reasonably necessary to show compliance with this DPA, and will respond to a reasonable security questionnaire **no more than once in any 12-month period**, or after a personal data breach affecting your data.

Where an on-site audit is required by Applicable Data Protection Law or by a supervisory authority, we will cooperate on reasonable written notice, during business hours, without disrupting the Service, and subject to confidentiality. You bear the cost unless the audit reveals a material breach of this DPA.

12. Artificial intelligence and automated processing

We do not use personal data processed on your behalf to train, fine-tune, or improve any model — ours or anyone else's — except where that is strictly necessary to provide the Service on your instructions.

We instruct our AI subprocessors not to use data submitted through the Service for their own model training or improvement, and we select providers whose terms support that. Where a routing provider passes requests to downstream model providers, the applicable terms are the ones the routing provider imposes; we do not represent that every downstream provider offers identical terms, which is why the Service is not designed to receive personal data in AI prompts and the Privacy Policy tells users not to submit it.

Automated decision-making. The Service produces scores, forecasts, and classifications about places, organizations, and events. It is not designed to make automated decisions producing legal or similarly significant effects about individuals, and the Terms prohibit using it that way — with an express carve-out for lawful sanctions screening, know-your-customer and other regulatory compliance checks, due diligence, research, and journalism. Where you carry out any of those, you are the controller of that decision and responsible for the safeguards it requires, including human review.

13. Return and deletion

On the end of the Agreement, or earlier at your written request, we will delete or return the personal data we process on your behalf, and delete existing copies, within **30 days** — except where Applicable Data Protection Law requires us to keep it, in which case we keep it only for that purpose and for that period.

Backups are overwritten on their normal cycle; personal data in a backup is not restored to production use after deletion.

14. Liability

Each party's liability under this DPA is subject to the limitations and exclusions in the Terms of Service. Nothing in this DPA limits any liability that cannot be limited under Applicable Data Protection Law, including a data subject's rights under the SCCs.

15. General

If this DPA and the Agreement conflict on the processing of personal data, **this DPA controls**. If this DPA and the SCCs conflict, the SCCs control.

We may update this DPA where a change in Applicable Data Protection Law, a subprocessor, or the Service requires it, in the same way and on the same notice as the Terms. We will not make a change that materially reduces the protections in this DPA.

Questions, signed-copy requests, and data protection contact: privacy@worldmonitor.app.

Annex 1 — Details of processing

Data importer (processor): World Monitor FZ LLC, Dubai, United Arab Emirates. Contact: privacy@worldmonitor.app. Activities: real-time global intelligence aggregation, analysis, alerting, and API access.

Data exporter (controller): the customer that is party to the Agreement. Activities: use and receipt of the Service in accordance with the Agreement.

Categories of data subjects

- the individuals you authorize to use the Service — your personnel, contractors, and named seat holders;
- any individuals whose personal data you choose to submit through the Service, including in queries, prompts, uploads, or alert configuration.

Categories of personal data

- **Account and identity** — name, email address, and the authentication identifiers held by our authentication providers.
- **Authentication** — session tokens, API keys, license keys, and OAuth grants.
- **Technical** — IP address, user agent, device and browser characteristics, request metadata, and the timing and performance data any web request carries.
- **Content you submit** — alert rules, declared site coordinates, saved views, queries and prompts, webhook destinations, and anything else you place into the Service.

Not required by the Service: names, home or current locations, itineraries, travel bookings, or contact details of the individuals a customer monitors. Monitoring operates on customer-declared static coordinates and configuration.

Sensitive data: none. Restricted Data must not be submitted without prior written agreement (section 7).

Frequency: continuous, as initiated by you through your use of the Service.

Nature and purpose: the processing operations necessary to provide the Service and perform our obligations under the Agreement, on your instructions.

Retention: for the duration of the Agreement, then as set out in section 13.

Transfers to subprocessors: as described in the subprocessor table in the Privacy Policy.

Annex 2 — Regional terms

European Economic Area, United Kingdom, Switzerland. Section 10 applies, incorporating the SCCs and, for the UK, the UK Addendum. You are the data exporter; we are the data importer.

United States. Where the CCPA/CPRA or a comparable state privacy law applies, we act as a **service provider** (or processor, where that term is used). We will not sell or share personal data, will not retain, use, or disclose it for any purpose other than performing the Service, and will not combine it with personal data received from another source except as that law permits. We certify that we understand and will comply with these restrictions.

Canada. Where PIPEDA or a provincial private-sector privacy law applies, we process personal data only for the purposes you specify, provide protection comparable to that required of you, and will notify you of any breach of security safeguards as set out in section 6.

United Arab Emirates. Where UAE Federal Decree-Law No. 45 of 2021 applies, we process personal data as your processor on your documented instructions and apply the measures in Annex 3.

Annex 3 — Security measures

The measures below are the ones we run. They are stated at the level we can evidence.

- **Encryption in transit** — TLS for all connections to the Service, its API, and its MCP server. Desktop secrets are held in the operating-system keychain rather than in plaintext files.
- **Encryption at rest** — provided by our infrastructure and database providers as listed in the Privacy Policy.
- **Access control** — authentication through a managed identity provider; least-privilege access to production systems; credentials and API keys scoped per subscriber and revocable; a token-authenticated local sidecar in the desktop application so other local processes cannot reach it.
- **Segregation** — customer configuration and content are separated by account identifier in the application database.
- **Availability and resilience** — managed, redundant hosting and content delivery; automated deployment with rollback.
- **Logging and monitoring** — structured request and application logging, error and crash monitoring, and rate limiting at the edge, each through the providers named in the Privacy Policy.
- **Vulnerability management** — dependency auditing in continuous integration, and a published security policy for reporting.
- **Personnel** — confidentiality obligations and access granted only for as long as required.
- **Subprocessor diligence** — data protection terms no less protective than this DPA, and a published subprocessor list.
- **Deletion** — deletion or return within 30 days of the end of the Agreement, with backups overwritten on their normal cycle.

Annex 4 — Subprocessors

The current list is the **subprocessor table in the Privacy Policy**, maintained in that one place and covering authentication, database, payments, hosting, content delivery, logging, error monitoring, analytics, performance monitoring, rate limiting, container hosting, documentation hosting, AI model

providers, and transactional email.

Notice of changes, and your objection right, are in section 8.

Previous versions

This page carries the date it was last changed. Every earlier version, and the exact change between any two, is in the repository history: github.com/koala73/worldmonitor/commits/main/docs/dpa.mdx.