WW SOFTWARE DEFENDER

Data Processing Agreement (DPA) — Fraud & Risk Intelligence API

Version 2.2 | Effective Date: August 26, 2026 | Replaces v2.1 (August 8, 2026)

This Data Processing Agreement ("DPA") is entered into between:

Processor (Sub-contractor): Kelson Tchisseke Filipe Muiani, doing business as WW Software Defender (hereinafter the "Company," "we," "us," or "our") — kelsonfilipedev@gmail.com

Controller (Data Controller): The Integrator, being the entity that accepts these terms by using the Service.

This DPA is an integral part of the WW Software Defender Terms of Use and Privacy Policy, incorporated by reference into those documents. In the event of conflict between this DPA and the Terms of Use regarding matters of data protection, this DPA prevails. The Integrator accepts this DPA by using the WW Software Defender service (the "Service"). Where an Integrator requires a manually countersigned copy of this DPA — for example, for internal procurement or vendor-review purposes — the Company will provide one upon request; see the Acceptance section at the end of this DPA.

1. Definitions

"Personal Data" — any information relating to an identified or identifiable natural person, including identifiers such as entityId when directly or indirectly associated with a natural person.

"Service" — the WW Software Defender platform, API, and related infrastructure, as defined in the Terms of Use.

"Controller" — the Integrator, who determines the purposes and means of processing of data submitted to the Service.

"Processor" — the Company, which processes personal data on behalf of and under the instruction of the Controller.

"Sub-processor" — any third party engaged by the Company to process personal data of Integrators in the context of service delivery.

"Data Breach" — any security breach leading to destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to personal data.

"TOMs" — Technical and Organizational Measures implemented by the Processor.

2. Subject Matter and Scope

This DPA governs the processing of personal data carried out by the Company (Processor) on behalf of the Integrator (Controller) in the context of providing the Service.

The Company processes, on behalf of the Integrator:

— Entity identifiers (entityId) that may constitute personal data;

— IP addresses and metadata included in payloads;

— Risk scores, states, and decisions generated automatically;

— Audit trail records of decisions executed.

The Company processes data exclusively to:

— Calculate risk scores;

— Determine automatic security states;

— Execute automated response decisions;

— Maintain the audit trail;

— Apply rate limiting;

— Transmit webhook notifications.

Categories of Data Subjects.

The personal data processed under this DPA may relate to the following categories of data subjects, as determined by the Integrator's use of the Service: end-users, customers, employees, contractors, or other individuals whose behavioral events, IP addresses, or identifiers are submitted to the Service by the Integrator.

Duration of Processing.

Processing takes place for the duration of the Integrator's Subscription, as further detailed in Section 8 (Data Retention and Return) and Section 13 (Duration and Termination) of this DPA.

3. Obligations of the Company (Processor)

The Company commits to:

— Process data exclusively based on documented instructions from the Integrator;

— Ensure confidentiality commitments from persons authorized to process data;

— Implement the technical and organizational measures described in Section 6;

— Respect the conditions for sub-processor engagement set out in Section 5;

— Assist the Integrator in fulfilling obligations to respond to data subject requests;

— Assist in fulfilling obligations under Articles 32 to 36 of the GDPR;

— Delete or return all data upon service termination;

— Provide information necessary to demonstrate compliance with this DPA.

4. Obligations of the Integrator (Controller)

The Integrator declares and warrants that:

— It holds an adequate legal basis to submit personal data to the Service;

— It has informed data subjects about the processing carried out;

— Instructions provided to the Company comply with applicable law;

— It is responsible for the accuracy, quality, and lawfulness of submitted data;

— It has assessed the adequacy of the Service for its data protection needs;

— It implements adequate technical and organizational measures in its own systems;

— It will submit only strictly necessary data (data minimization);

— It will not submit Special Categories of Data without express written authorization from the Company.

5. Sub-processors and Operational Providers

Authorized sub-processors (with access to Integrators' personal data):

Sub-processor	Function	Location	Transfer Safeguard
Render (render.com)	API hosting	United States	EU/UK SCCs via Render DPA
Supabase (supabase.com)	PostgreSQL database	EU (Frankfurt)	Not applicable — data remains in EEA

Upstash (upstash.com)	Redis cache / rate limiting	United States	EU SCCs + UK Addendum via Upstash DPA
Vercel (vercel.com)	Frontend dashboard hosting	United States	EU/UK SCCs via Vercel DPA

Copies of the relevant sub-processor Data Processing Addenda and SCC documentation referenced above are available to the Integrator upon written request.

Operational providers (without access to Integrators' personal data): GitHub (github.com) — private code repository and CI/CD.

The Company will notify the Integrator with reasonable advance notice of any planned changes to sub-processors. Absence of objection within 14 days of notification constitutes acceptance.

6. Technical and Organizational Measures (TOMs)

Access control.

Mandatory authentication via JWT or API Key with SHA-256 hashing; per-tenant data isolation via dedicated PostgreSQL schema; production database access restricted to authorized operators.

Encryption.

Data in transit is protected via HTTPS/TLS, including webhook transmissions. Data at rest in the PostgreSQL database (Supabase) is encrypted at rest by the underlying infrastructure provider.

Availability and resilience.

Rate limiting per entity and per IP via Redis; infrastructure managed by Render and Supabase with backup capabilities.

Auditability.

Audit trail with traceability and integrity mechanisms covering all decisions and actions executed.

Current technical limitations (v1.4.0): no automated data deletion mechanisms by defined deadline; no DELETE endpoints for events or audit logs. Deletion requests require manual intervention. These limitations are acknowledged by the Integrator as a condition of the Service in the current version. Resolution is planned for a future version.

7. International Data Transfers

Personal data may be transferred to and processed on servers managed by Render, Upstash, and Vercel, located outside the European Economic Area (EEA). The Supabase PostgreSQL database, where the primary dataset resides, is hosted in Frankfurt (EU) and does not involve an international transfer.

Transfers to Render, Upstash, and Vercel are safeguarded through the Standard Contractual Clauses (SCCs) and, where applicable, the UK Addendum, incorporated into each provider's own Data Processing Addendum, as summarized in the table in Section 5.

Where the Integrator configures webhook endpoints outside the EEA, block notifications transmitted by the Service constitute a further international data transfer for which the Integrator is solely responsible for ensuring compliance with applicable law.

Integrators subject to the GDPR who require additional transfer documentation may request it by contacting kelsonfilipedev@gmail.com.

8. Data Retention and Return

Data is retained while the tenant remains active and the Service is being provided, without automatic deletion deadline in the current version (v1.4.0).

Upon contract termination, the Company will:

— Delete the Integrator's personal data from the cloud instance, upon express request, within a maximum of 30 days after termination;

— Provide a data extract in JSON format before deletion, if requested;

— Certify deletion by email, if requested.

Technical limitation: deletion requires manual intervention. The Integrator must submit an express request to kelsonfilipedev@gmail.com with the subject: "DPA — Data Deletion — WW Software Defender".

9. Audit and Compliance

The Integrator has the right to audit the Company's compliance via:

— Request for information and documentation by email;

— Scheduled audit with a minimum of 30 days prior notice and mutual agreement on scope;

— Use of an independently agreed auditor, subject to a confidentiality agreement.

Audits may not:

— Compromise the security of the cloud instance or other tenants;

— Require direct access to production infrastructure or other Integrators' data;

— Require access to proprietary source code;

— Conduct penetration tests without prior written authorization.

10. Data Breaches

In the event of a personal data breach, the Company will notify the Integrator without undue delay, and in any event within forty-eight (48) hours of becoming aware of the breach, to allow the Integrator sufficient time to meet its own regulatory notification obligations, including the 72-hour deadline under Article 33 GDPR where applicable.

The notification will include:

— Description of the nature of the breach;

— Categories and approximate volume of affected data;

— Measures taken or proposed to remediate the breach;

— Contact point for additional information.

The Integrator is responsible for notifying supervisory authorities and affected data subjects, in accordance with the timelines and requirements of applicable legislation.

11. The Company as Controller

The Company acts as an independent Controller with respect to:

— Tenant contact data and credentials necessary for administrative service management;

— Aggregated and anonymized operational data for service maintenance and improvement;

— Technical system logs that do not contain Integrators' users' personal data.

12. Liability

The Company is liable for damages caused by processing when it has not fulfilled the obligations of this DPA or has acted outside the lawful instructions of the Integrator.

WW Software Defender v1.4.0 — © 2026 Kelson Tchisseke Filipe Muiani — All rights reserved.

The Integrator is liable for damages caused by processing when it has not fulfilled obligations specific to Controllers, including the submission of Special Categories of Data without authorization.

The Company's total aggregate liability under this DPA shall not exceed the amount actually paid by the Integrator (via Paddle) in the twelve (12) months preceding the event giving rise to the claim. For Integrators on the Free Plan, the Company's maximum aggregate liability under this DPA is limited to EUR 500.

Relationship to the Terms of Use liability cap. This cap operates alongside, and does not stack with, the limitation of liability set out in Section 13 of the Terms of Use. For the avoidance of doubt: (i) claims arising under the Terms of Use that do not relate to the processing of personal data remain subject to the limitation of liability in Section 13 of the Terms of Use, including the €0 cap applicable to the Free Plan; and (ii) claims arising specifically from the Company's breach of its obligations as Processor under this DPA are governed exclusively by the cap set out in this Section 12, including the EUR 500 cap applicable to Integrators on the Free Plan. These caps apply to different categories of claims and are not cumulative for the same claim.

13. Duration and Termination

This DPA remains in force while the Company processes personal data on behalf of the Integrator. The DPA terminates automatically upon termination of the underlying service agreement, without prejudice to data deletion obligations and confidentiality obligations, which remain in force for an additional period of 3 years after termination.

14. Amendments to the DPA

The Company reserves the right to update this DPA to reflect legal, regulatory, or operational changes, with prior notification to the Integrator whenever operationally feasible. Material changes will be communicated with a minimum of 30 days' advance notice.

15. Severability

If any provision of this DPA is found to be invalid, illegal, or unenforceable, the remaining provisions shall remain fully valid and effective.

16. Governing Law and Jurisdiction

This DPA is governed by the law of the Republic of Angola, without prejudice to the GDPR of the European Union and other applicable international data protection standards. The courts of the District of Luanda, Republic of Angola, shall have exclusive jurisdiction over any disputes arising from this DPA.

17. Related Policies

This DPA should be read together with the following, which form part of the agreement between the Integrator and the Company:

— Terms of Use — https://ww-software-defender.vercel.app/legal/terms

— Privacy Policy — https://ww-software-defender.vercel.app/legal/privacy

— Refund Policy — https://ww-software-defender.vercel.app/legal/refund

18. Contact

For questions regarding this DPA: Kelson Tchisseke Filipe Muiani, doing business as WW Software Defender | Email: kelsonfilipedev@gmail.com | Subject: "DPA — WW Software Defender"

Acceptance

This DPA is accepted by the Integrator upon accessing or using the WW Software Defender service after its effective date. No separate signature is required for this DPA to take effect.

Optional Countersigned Copy.

Integrators requiring a manually countersigned copy of this DPA for internal procurement or vendor-review purposes may request one by contacting kelsonfilipedev@gmail.com. A dedicated signature block will be provided in that copy.

WW Software Defender v1.4.0 — © 2026 Kelson Tchisseke Filipe Muiani — All rights reserved.