WW SOFTWARE DEFENDER

Privacy Policy — Fraud & Risk Intelligence API

Version 2.1 | Effective Date: August 26, 2026 | Replaces v2.0 (August 8, 2026)

This Privacy Policy describes how the Company collects, processes, stores, and transfers personal data in connection with: the WW Software Defender public website; the creation and management of Accounts and Subscriptions; and the WW Software Defender cloud API and dashboard (the "Service"). The product source code is proprietary and not publicly available.

1. Data Controller

The data controller responsible for personal data processed in connection with WW Software Defender is: Kelson Tchisseke Filipe Muiani, doing business as WW Software Defender (hereinafter the "Company," "we," "us," or "our") — kelsonfilipedev@gmail.com.

For privacy and data protection inquiries, contact the above email with the subject line: "Privacy — WW Software Defender".

2. Scope of Application

This Policy applies to:

— Visitors — individuals browsing the public WW Software Defender website;

— Account Holders — individuals who create an Account (Free or paid) via the website's sign-up form;

— Integrators and Tenants — business entities, and their authorized representatives, with configured access to the Service;

— End-users of Integrators — individuals whose behavioral events, identifiers, or related data may be submitted to the Service by an Integrator via the API. The Company does not collect this data directly from these individuals; it processes it on the Integrator's documented instructions, as described in the Data Processing Agreement (DPA).

3. Data Processed

3.1 Account and Billing Data (the Company as Controller).

When you create an Account, we collect: your name, company name, email address, and password. Passwords are never stored in plain text; they are hashed using bcrypt before storage.

When you upgrade to a paid Subscription Plan, we receive limited billing-related data from Paddle (our payment processor and Merchant of Record) — such as your subscription status, plan tier, and billing email — necessary to provision and manage your Subscription. We do not collect or store your payment card details; these are collected and processed directly by Paddle. See Section 6.

3.2 Data Submitted by Integrators via the API (the Company as Processor).

(a) Event type (e.g., LoginFailed, SuspiciousIp, PasswordReset); (b) Entity identifier (entityId) — if directly or indirectly associated with a natural person, this constitutes personal data; (c) Free-format JSON payload — may contain IP addresses, session metadata, or other data; (d) Event creation timestamp.

3.3 Data Automatically Generated by the Service.

(a) Risk score (0–100) per entityId; (b) Entity state — NORMAL, SUSPICIOUS, ALERT, CRITICAL, BLOCKED; (c) Automatic decision — ALLOW, THROTTLE, CHALLENGE, BLOCK; (d) Audit trail of all decisions and actions executed.

3.4 What the Service Does Not Do.

The Service does not itself perform active geolocation derived from IP addresses, device or browser fingerprinting, or direct collection of personal data from Integrators' end-users. However, as described in Section 3.2, payloads submitted by Integrators via the API may contain personal data such as IP addresses or session metadata. The Company does not use data for advertising or marketing purposes, and does not sell personal data to third parties.

4. Purpose of Processing

Data is processed to:

— create and manage Accounts, and authenticate Account Holders;

— process and administer Subscriptions and billing, in conjunction with Paddle;

— calculate behavioral risk scores per entity;

— determine security states and execute automated response decisions;

— produce and maintain the audit trail;

— apply rate limiting per entity and per IP;

— authenticate tenants and integrators via JWT and API Keys;

— respond to support and privacy-related inquiries.

The Company does not use data for advertising, marketing, or sharing with third parties for commercial purposes.

5. Legal Basis for Processing

Where the GDPR applies, the legal bases are:

— Performance of a contract (Art. 6(1)(b)) — processing is necessary to create and administer your Account, provide the Subscription, and deliver the contracted Service;

— Legitimate interests (Art. 6(1)(f)) — detection and prevention of fraud and abusive behavior;

— Compliance with a legal obligation (Art. 6(1)(c)) — for example, retaining billing records as required by applicable tax and accounting legislation;

— For data submitted by an Integrator via the API — the Integrator represents that it holds an adequate legal basis (which may include consent obtained from its own end-users) for submitting that data. The Company relies on this representation, as further described in the DPA.

6. Payment Processing via Paddle

Paid Subscriptions are processed through Paddle.com Market Limited ("Paddle"), which acts as the Merchant of Record and, with respect to payment data, as an independent data controller. When you subscribe to a paid plan, Paddle collects and processes your billing name, address, email, and payment method directly, governed by Paddle's own Privacy Notice, available at paddle.com/legal.

Paddle's checkout may set its own cookies or use similar technologies for fraud prevention and payment processing purposes; these are governed by Paddle's Privacy Notice, not this Policy.

The Company receives limited data back from Paddle — such as subscription status and plan tier — necessary to provision your access to the Service.

7. Data Transfers to Third Parties

Data is stored and processed by the following sub-processors:

— Render (render.com) — API hosting — United States — safeguarded by EU/UK Standard Contractual Clauses (SCCs) under Render's Data Processing Addendum;

— Supabase (supabase.com) — PostgreSQL database hosting — European Union (Frankfurt) — data remains within the EEA;

— Upstash (upstash.com) — Redis cache and rate limiting — United States — safeguarded by EU SCCs and the UK Addendum under Upstash's Data Processing Addendum;

— Vercel (vercel.com) — frontend and dashboard hosting — United States — safeguarded by EU/UK SCCs under Vercel's Data Processing Addendum.

Copies of the relevant sub-processor Data Processing Addenda are available upon written request. The Company does not transmit data to analytics, error tracking, advertising, or third-party monitoring services.

When an entity reaches the BLOCKED state, the Service may send webhook notifications to URLs registered by the Integrator, containing: event type, entityId, risk score, and timestamp. The Integrator is solely responsible for the security and legal compliance of data received via webhook.

8. Automated Decision-Making

The Service performs automated processing of behavioral event data to calculate risk scores and execute automatic decisions (ALLOW, THROTTLE, CHALLENGE, BLOCK) without human review at the point of decision, as described in the Terms of Use. Where these decisions are applied to data that identifies or relates to a natural person, this may constitute automated decision-making within the meaning of Article 22 GDPR.

The Integrator, as data controller for its own end-users, is responsible for informing those end-users of this automated processing and for providing an appropriate mechanism to contest automated decisions or request human review, where required by applicable law. The Company, as Processor, will provide reasonable assistance to Integrators in fulfilling these obligations upon request.

9. Data Retention

Account and billing data is retained while your Account remains active. Following Account or Subscription termination, the Company may retain limited billing-related records for the period

required by applicable tax and accounting legislation.

Event data, risk scores, entity states, automatic decisions, and audit trails are not subject to automatic deletion by a defined deadline in the current version (v1.4.0). This data persists while the tenant remains active, unless an explicit deletion request is made.

Current technical limitation: There are no automated data deletion mechanisms or DELETE endpoints for events or audit logs. Deletion requests require manual intervention. Submit requests to kelsonfilipedev@gmail.com with the subject: "Data Deletion — WW Software Defender".

10. Rights of Data Subjects

To the extent that data processed contains personal data of identifiable natural persons, data subjects hold the following rights:

— Access;

— Rectification;

— Erasure;

— Restriction of processing;

— Objection;

— Data portability;

— The right to lodge a complaint with a competent supervisory authority.

Current technical limitation: The system does not provide automated mechanisms for exercising these rights (v1.4.0). Requests must be submitted by email with the subject: "GDPR — Exercise of Rights — WW Software Defender". For data submitted by an Integrator via the API, the Integrator is the primary point of contact for rights requests from its own end-users.

11. Data Security

The Service implements:

— Dual authentication (JWT + API Keys with SHA-256 hashing);

— Bcrypt password hashing for Account credentials;

— Per-tenant data isolation via dedicated PostgreSQL schema;

— Data transmission via HTTPS/TLS;

— Rate limiting per entity and per IP via Redis;

— Audit trail with full traceability and integrity.

In the event of a data breach impacting personal data, the Company will notify affected Integrators and Account Holders without undue delay, and in any event within forty-eight (48) hours of becoming aware of the breach.

12. Cookies and Tracking Technologies

The public website currently does not use cookies, analytics tools, tracking pixels, or any third-party tracking technologies. If this changes in the future, this Policy will be updated accordingly, and cookie consent will be requested where required by applicable law.

The web dashboard (Next.js) may use local session storage for authentication management, with no data shared with third parties. The WW Software Defender cloud API itself is a REST API and does not use cookies, tracking pixels, or browser fingerprinting.

As noted in Section 6, Paddle's checkout may independently set cookies for payment processing and fraud prevention purposes.

13. EU Representative

The Company does not currently have an establishment in the European Union. For the personal data the Company processes as an independent Controller — namely, Account Holder contact and billing data described in Section 3.1 — the Company relies on the derogation under Article 27(2)(a) GDPR, on the basis that this processing is occasional, does not involve large-scale processing of special categories of data, and is unlikely to result in a risk to the rights and freedoms of data subjects, given the Company's current scale of operations.

The Company will reassess this position, and appoint an EU representative if required, as its customer base and data volumes grow. For data submitted by Integrators via the API, where the Company acts as Processor, any obligation to appoint an EU representative rests with the relevant Integrator as data controller for that data.

14. Changes to This Policy

The Company reserves the right to update this Privacy Policy, with prior notice published on the platform whenever operationally feasible. Continued use of the Service after publication of a new version constitutes acceptance of the changes.

15. Severability

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

16. Governing Law and Jurisdiction

This Privacy Policy 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 Policy.

17. Related Policies

This Privacy Policy should be read together with the following, which form part of the agreement between you and the Company:

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

— Data Processing Agreement (DPA) — https://ww-software-defender.vercel.app/legal/dpa

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

18. Contact

For questions regarding this Privacy Policy or the processing of personal data: Kelson Tchisseke Filipe Muiani, doing business as WW Software Defender | Email: kelsonfilipedev@gmail.com | Subject: "Privacy — WW Software Defender"