

Master Data Privacy & Protection Policy

Effective Date: September 2026 | Primary Domain: wimika.ng | Framework: NDPA 2023 & GAID 2025

1. Introduction

Wimika RMS Technologies Ltd ("Wimika," "we," "us," or "our") is committed to maintaining the confidentiality, integrity, and security of personal data entrusted to us.

This Master Data Privacy & Protection Policy (the "Policy") outlines how we collect, process, store, share, and safeguard personal data across all user touchpoints. This includes our primary web portal (wimika.ng), mobile applications (including **MoneyGuard**), API integrations, customer support interactions, and offline operational channels.

We comply fully with applicable statutory privacy laws, including the **Nigeria Data Protection Act (NDPA) 2023** and the **General Application and Implementation Directive (GAID) 2025**, alongside internationally recognized data protection principles (such as the EU General Data Protection Regulation—GDPR).

2. Scope & Applicability

This Policy governs all data processing activities conducted by Wimika and applies to:

- **Website Visitors:** Individuals browsing wimika.ng or accessing online public resources.
- **App End-Users & Retail Customers:** Individual consumers and micro/SME account holders utilizing Wimika products, including the MoneyGuard active loss-control and financial recovery app.
- **Business Partners & Merchants:** Authorized contacts, enterprise representatives, and financial institution personnel interacting with Wimika platforms.
- **Job Applicants & Personnel:** Individuals applying for employment or contracting with Wimika.

This Policy covers data collected digitally (web, mobile app, APIs) and physically (manual claims forms, paper documentation, and customer service phone calls).

3. Categories of Personal Data We Process

To provide active threat detection, device security scoring, and guaranteed financial loss reimbursement, we collect and process the following categories of data:

a. Identity & Contact Information

Names, phone numbers, email addresses, residential addresses, and government-issued identification numbers required for account creation, KYC verification, and claims verification.

b. Mobile Device Telemetry & Technical Signals

Device identifiers (IMEI, IP addresses, OS versions), network connectivity metadata (e.g., detection of unencrypted or unsafe Wi-Fi access points), malware threat logs, phishing URL telemetry, and app vulnerability flags collected directly via mobile platforms (e.g., MoneyGuard).

Note on Accessibility Services: Where explicitly authorized by the user, our mobile software utilizes Android AccessibilityService APIs strictly to evaluate and block malicious phishing links and harmful URLs in real time.

c. Fraud Claims & Financial Telemetry

Incident reports, dispute documentation, bank transfer receipts, dispute communication logs, and transaction timestamps required to validate fraud eligibility and execute financial reimbursements.

d. Commercial & Partner Data

Business contact details, corporate registration records, and due diligence checks for enterprise partners, underwriters, and service vendors.

4. Lawful Basis for Processing

We process personal data only when backed by valid statutory grounds under the NDPA 2023 and GAID 2025:

- **Performance of a Contract:** Processing required to fulfill our service commitments to you, validate claim eligibility, operate MoneyGuard accounts, and process financial loss reimbursements.
- **Legitimate Interests:** Processing necessary for real-time cybersecurity monitoring, threat intelligence gathering, fraud prevention, network integrity maintenance, and protecting user funds against zero-day takeovers—provided these interests do not override fundamental data subject rights.
- **Legal & Regulatory Obligations:** Processing necessary to comply with anti-money laundering (AML) laws, regulatory audit trails, court orders, or statutory NDPC directives.
- **Explicit Consent:** Where you have explicitly opted in (e.g., marketing communications or specific device permission grants). You reserve the right to withdraw consent at any time.

5. Data Sharing & Third-Party Disclosure

Wimika does **not** sell, rent, or trade personal data to third parties. We share data strictly on a confidential, need-to-know basis subject to formal Data Processing Agreements (DPAs) with:

- **Regulated Underwriters & Insurance Partners:** Authorized risk transfer partners responsible for fulfilling contractual fraud loss reimbursements.
- **Technology & Infrastructure Vendors:** Secure cloud hosting, SMS gateway, threat intelligence, and analytics providers bound by confidentiality and security standards.
- **Financial Institutions & Banking Partners:** Partner banks and payment operators involved in investigating claims, executing chargebacks, or processing fund recoveries.
- **Law Enforcement & Regulatory Authorities:** Statutory bodies (such as the Nigeria Data Protection Commission or law enforcement agencies) when legally compelled by court order or binding regulatory mandate.

6. Cross-Border Data Transfers

When personal data must be stored or processed outside Nigeria (e.g., on secure cloud infrastructure located in international data centers), Wimika enforces strict transfer protocols compliant with Section 41 of the NDPA 2023 and GAID 2025 guidelines. This includes verifying adequacy decisions, executing NDPC-approved Standard Contractual Clauses (SCCs), or enforcing binding corporate standards.

7. Data Security & Storage Limitations

- **Security Safeguards:** We implement enterprise-grade technical and organizational controls, including AES-256 encryption for data at rest and in transit, strict role-based access control (RBAC), multi-factor authentication, network firewalls, and alignment with **ISO/IEC 27001** standards.
- **Retention Schedule:** Personal data is retained only for as long as necessary to fulfill the operational purposes outlined in this Policy, manage insurance policy lifecycles, and maintain statutory audit trails (e.g., retaining financial transaction logs for a minimum of 7 years in accordance with regulatory laws). Outdated data is securely deleted or anonymized.

8. Data Subject Rights

In accordance with the NDPA 2023 and GAID 2025 framework, you hold statutory rights regarding your personal data:

- **Right of Access:** Request copies of your personal data held by Wimika.
- **Right to Rectification:** Request correction of inaccurate, out-of-date, or incomplete data.
- **Right to Erasure ("Right to be Forgotten"):** Request deletion of your personal data, subject to legal or audit retention exceptions.
- **Right to Restrict or Object:** Limit or object to data processing based on legitimate interests.
- **Right to Data Portability:** Receive your data in a structured, commonly used, machine-readable format.
- **Right to Withdraw Consent:** Revoke previously granted processing consent at any time without affecting prior lawful processing.
- **Right to Lodge a Complaint:** File a grievance directly with Wimika's Data Protection Officer or directly with the supervisory authority: **Nigeria Data Protection Commission (NDPC)** (ndpc.gov.ng).

9. Cookies & Web Tracking

Our web platform (wimika.ng) uses essential, functional, and analytical cookies to maintain session security, remember user preferences, and analyze website performance. You can manage cookie preferences via our cookie banner or your browser settings.

10. Data Breach Notification Management

Wimika maintains an active Incident Response Plan. In the event of a security compromise or data breach that presents a risk to the rights and freedoms of data subjects, Wimika will:

1. Notify affected individuals without undue delay.
2. Formally report the incident to the Nigeria Data Protection Commission (NDPC) within **72 hours** of becoming aware of the breach, detailing mitigation steps taken.

11. Contact Details & Data Protection Officer (DPO)

To exercise your statutory data subject rights, lodge a privacy query, or request clarification on our data practices, contact our Data Protection Officer:

Data Protection Officer: Wimika RMS Technologies Ltd

Email: privacy@wimika.ng / dpo@wimika.ng

Official Web Portal: <https://wimika.ng>

Physical Address: 4 Olatunbosun Street, Shonibare Estate, Maryland, Lagos, Nigeria

Telephone: +234 813 444 0598

12. Updates to this Policy

We reserve the right to modify this Master Privacy Policy to reflect changing legal mandates, operational updates, or product enhancements. Revisions will be published on wimika.ng with an updated "Effective Date." Continued engagement with Wimika products or websites following updates indicates acknowledgment of the revised policy terms.