

VERO360 LIMITED

Privacy Policy — Data Protection & User Rights

Document Version	1.0 — Full Regulatory Edition
Effective Date	01 April 2026
Company	Vero360 Limited
MBRS Registration	Registered — Malawi Business Registry Services
Registered Office	Accurate House, Shop 6, First Floor, Zomba, Malawi
Contact	info@vero360.mw
Platform	Vero360 Super App (Android & iOS)
Document Status	OFFICIAL PRIVACY POLICY — LEGALLY BINDING

Legal Basis: This Privacy Policy is issued in compliance with Section 21 of the Malawi Constitution (Right to Privacy), the Electronic Transactions & Cyber Security Act 2016, MACRA Data Protection Guidelines, and GDPR-inspired best practices voluntarily adopted by Vero360 Limited. By using the platform, you consent to the data practices described herein.

PART A — WHO WE ARE & WHAT THIS POLICY COVERS

Section 1 — About Vero360 & This Policy

Vero360 Limited ('**Vero360**', '**we**', '**us**', '**our**') is a technology company incorporated under the **Companies Act 2013 of Malawi** and registered with **MBRS**. We operate the Vero360 Super App — a mobile platform connecting customers with verified service providers, merchants, and courier partners across Malawi.

This Privacy Policy explains what personal data we collect, why we collect it, how we use it, who we share it with, and what your rights are. It applies to all users of the Vero360 Super App platform, website, and related services.

Section 2 — Regulatory Framework

This Privacy Policy is governed by the following laws and regulations:

Law / Regulation	Regulator / Authority	Key Privacy Provision
Malawi Constitution — Section 21	Republic of Malawi	Fundamental right to privacy of person, home, and communications
Electronic Transactions & Cyber Security Act 2016	MACRA	Data protection, cybersecurity, electronic records, breach reporting
MACRA Data Protection Guidelines	MACRA	Standards for handling personal data of digital platform users

Law / Regulation	Regulator / Authority	Key Privacy Provision
Financial Services Act 2010	RBM	Protection of financial and payment data of platform users
Financial Crimes Act 2017 / AML	RBM / FIU	KYC data obligations and Anti-Money Laundering record-keeping
Companies Act 2013	MBRS	Company records, director data, and shareholder information
Taxation Act (Cap. 41:01)	MRA	Retention of financial transaction records for 7 years
Consumer Protection Act 2003	Government of Malawi	Consumer right to know how their data is used and to seek redress
GDPR — Best Practice (voluntary)	EU — Adopted voluntarily	Lawful basis, data minimisation, subject rights, consent framework

PART B — DATA WE COLLECT

Section 3 — What Personal Data We Collect

Data Category	Specific Data Collected	Who It Applies To	Legal Basis
Identity Data	Full name, phone number, email address, date of birth	All users	Contract performance; Legal obligation
KYC / ID Data	National ID number, NID photo, selfie for liveness check	Providers only	Legal obligation (RBM AML); Contract
Payment Data	Mobile money number, transaction history, escrow records	All users	Contract; Legal obligation (MRA)
Location Data	GPS coordinates during active rides and deliveries only	Customers & drivers	Contract; Legitimate interest
Device Data	Device model, OS version, app version, IP address	All users	Legitimate interest (security)
Usage Data	Pages visited, features used, session duration (anonymised)	All users	Legitimate interest (improvement)
Communications	In-app chat messages, support tickets, dispute evidence	All users	Contract; Legal obligation
Ratings & Reviews	Star ratings and written reviews submitted by users	All users	Legitimate interest; Consent

Data Minimisation: Vero360 collects only the minimum personal data necessary to provide platform services. We do not collect sensitive personal data such as racial origin, religious beliefs, political opinions, or health information unless strictly required by law.

Section 4 — How We Collect Your Data

- **Direct collection** — data you provide when registering, booking, or contacting support

- **Firebase OTP verification** — phone number confirmed at registration and login
- **KYC submission** — NID photo and documents submitted by providers during onboarding
- **Paychangu gateway** — payment transaction data processed through the payment gateway
- **Google Maps Platform** — GPS location data during active rides and deliveries only
- **App usage analytics** — anonymised usage data collected through the Flutter app
- **In-app chat** — messages exchanged between customers and providers on the platform

PART C — HOW WE USE YOUR DATA

Section 5 — Purposes of Data Processing

Purpose	Data Used	Legal Basis
Account creation & management	Identity data, phone number	Contract performance
Identity verification (KYC)	NID data, Firebase OTP	Legal obligation — RBM AML
Payment processing & escrow	Payment data, transaction records	Contract; Legal obligation
Service delivery coordination	Location, booking, identity data	Contract performance
AI-powered service discovery	Usage data, search history (anonymised)	Legitimate interest; Consent
Fraud detection & prevention	Transaction patterns, device data, location	Legitimate interest; Legal obligation
Dispute resolution	Communications, transaction records, evidence	Contract; Legal obligation
Regulatory compliance	KYC, transaction, identity data	Legal obligation — MACRA, RBM, MRA
Platform improvement	Anonymised usage analytics	Legitimate interest
Marketing & promotions	Name, contact details (opted-in users only)	Consent — can be withdrawn anytime
Tax reporting to MRA	Transaction records, provider earnings	Legal obligation — Taxation Act

No Data Selling: Vero360 will NEVER sell, rent, or trade your personal data to any third party for commercial purposes. This is an absolute and unconditional commitment.

Section 6 — Data Sharing

We share personal data only in the following limited circumstances:

Recipient	Data Shared	Reason	Safeguard
Paychangu	Payment data, mobile number	Payment processing	Contractual data processing agreement
Google Firebase	Phone number, device data	OTP, push notifications, authentication	Google Privacy Policy & security standards
OpenAI (GPT-5)	Anonymised query data only	AI assistant responses	No personal identifiers shared with OpenAI

Recipient	Data Shared	Reason	Safeguard
Google Maps	GPS location during active trips	Route & fare calculation	Location shared only during active service
Courier Partners	Delivery address, contact number	Order fulfilment	Signed data sharing agreement required
RBM / FIU	KYC and suspicious transaction data	AML legal obligation	Only when legally required
MRA	Provider earnings, transaction records	Tax compliance	Only when legally required
Malawi Police Service	Account and transaction data	Court order or fraud investigation	Only with valid legal authority

PART D — DATA RETENTION, SECURITY & YOUR RIGHTS

Section 7 — Data Retention Periods

Data Type	Retention Period	Legal Basis for Retention
Transaction & payment records	7 years	Taxation Act (Cap. 41:01) — MRA requirement
KYC / NID verification data	7 years after account closure	Financial Crimes Act 2017 — AML requirement
Account & identity data	Duration of account + 3 years	Contract & Consumer Protection Act 2003
In-app chat messages	2 years	Dispute resolution — Consumer Protection Act
Dispute records	5 years	Legal proceedings protection
GPS / location data	90 days after trip completion	Operational need — minimised retention
Device & usage analytics	12 months (anonymised)	Legitimate interest — platform improvement
Marketing consent records	Until consent withdrawn + 1 year	MACRA data guidelines; GDPR best practice

Section 8 — Data Security Measures

- **End-to-end encryption** on all payment data via Paychangu secure infrastructure
- **Firebase Authentication** with SMS OTP — no passwords stored in plain text
- **Encrypted database** on InterServer cloud with daily automated backups
- **AI fraud detection** — GPT-5 monitors transaction patterns for suspicious activity in real time
- **Access controls** — only authorised Vero360 staff can access personal data
- **Bug bounty programme** — responsible disclosure policy for security vulnerabilities
- **Breach notification** — MACRA notified within 72 hours of any confirmed data breach
- **Staff training** — all Vero360 employees complete data protection training at onboarding

Section 9 — Your Data Rights

Under **Section 21 of the Malawi Constitution**, the **Electronic Transactions & Cyber Security Act 2016**, and GDPR best practices adopted by Vero360, you have the following data rights:

Right	What It Means	How to Exercise
Right of Access	Request a copy of all personal data we hold about you	Email info@vero360.mw — Subject: DATA ACCESS
Right to Rectification	Request correction of inaccurate or incomplete data	Update in-app or email info@vero360.mw
Right to Erasure	Request deletion of personal data (subject to legal obligations)	Email info@vero360.mw — Subject: DATA DELETE

Right	What It Means	How to Exercise
Right to Restriction	Request limitation of how we process your data	Email info@vero360.mw — Subject: RESTRICT
Right to Object	Object to processing based on legitimate interests or marketing	Email info@vero360.mw — Subject: OBJECT
Right to Portability	Receive your data in a structured, machine-readable format	Email info@vero360.mw — Subject: DATA PORT
Right to Withdraw Consent	Withdraw consent for marketing at any time	In-app settings or email info@vero360.mw

Response Time: Vero360 will respond to all data rights requests within 30 days of receipt. Complex requests may take up to 60 days with prior notification to the requester. Data rights requests are free of charge.

Section 10 — Cookies & Tracking

- The Vero360 app uses **Firebase Analytics** for anonymised app performance monitoring
- No third-party advertising cookies are used on the Vero360 platform
- Location tracking is **active only during live rides and deliveries** — not continuously
- Push notifications via **Firebase FCM** can be disabled in your device settings at any time

Section 11 — Children's Privacy

The Vero360 platform is intended for users aged **18 and above**. We do not knowingly collect personal data from children under 18. If we become aware that a child has registered on the platform, the account will be **immediately suspended** and data deleted in accordance with child protection principles under Malawian law.

Section 12 — Governing Law & Contact

This Privacy Policy is governed by the laws of the **Republic of Malawi**. For all privacy-related enquiries, requests, or complaints, contact us at:

Contact Type	Details
Privacy Enquiries	info@vero360.mw — Subject: PRIVACY
Data Access Requests	info@vero360.mw — Subject: DATA ACCESS
Data Deletion	info@vero360.mw — Subject: DATA DELETE
Complaints / MACRA	info@vero360.mw — or escalate to MACRA, P.O. Box 2175, Blantyre, Malawi

Vero360 Limited Accurate House, Shop 6, First Floor, Zomba, Malawi info@vero360.mw vero360.mw	Privacy Policy v1.0 Effective: 01 April 2026 Governed by the Laws of the Republic of Malawi	Regulators MACRA · RBM · MRA · MBRS Consumer Protection Act 2003
---	--	---