



AFRIQ GLOBAL MARKET LIMITED

Privacy Policy

Version 3.0 (Final) | **PUBLIC**

Effective: 1 September 2026 | www.afriqglobal.org

Document Title	Privacy Policy
Version	3.0 (Final)
Previous Version	2.1 (Amendment — 5 August 2026) — Superseded and Replaced in Full
Effective Date	1 September 2026
Classification	PUBLIC
Jurisdiction	Multi-Jurisdictional (United States of America, Federal Republic of Nigeria, United Kingdom, European Union, Canada, and other applicable African jurisdictions)
Website	www.afriqglobal.org
Related Documents	Service Agreement v4.0; Vendor Onboarding and KYC Policy v2.0

Confidentiality Notice

This Privacy Policy is a legally binding document of Afriq Global Market Limited. It governs the collection, use, processing, storage, sharing, and protection of personal data on the Afriq Global Market platform. All users of the Platform are bound by the terms set forth herein. This document supersedes all prior privacy notices and disclosures issued by Afriq Global Market Limited.

Amendment Notice — Version 3.0 — Effective 1 September 2026

This Privacy Policy Version 3.0 supersedes and replaces Privacy Policy Version 2.1 (dated 5 August 2026) in its entirety. Key changes from v2.1 to v3.0:

1. **(a)** All references to the Republic of South Africa, POPIA (Protection of Personal Information Act 4 of 2013), and any South African supervisory authority (including the Information Regulator) have been removed in their entirety. The Platform does not currently operate under a South African regulatory mandate. This aligns the Privacy Policy with the Vendor Onboarding and KYC Policy v2.0, which already removed all South Africa references in v1.1 (5 August 2026).
2. **(b)** Section 4.4 (Applicable Legislation) updated — POPIA removed.
3. **(c)** Section 5 (Legal Basis for Processing) — South Africa/POPIA row removed from all tables.
4. **(d)** Section 8 (International Data Transfers) — South Africa/POPIA paragraph removed.
5. **(e)** Section 11 (User Rights) — South Africa row removed from rights table; South Africa row removed from supervisory authorities table; POPIA Notice box (formerly Section 11.3) removed entirely.
6. **(f)** Section 14 (Data Breach Notification) — POPIA notification reference removed.
7. **(g)** Section 16 (Governing Law) — South Africa paragraph removed.
8. **(h)** Cross-references updated: Service Agreement v4.0; KYC Policy v2.0.
9. **(i)** Effective date updated to 1 September 2026.

TABLE OF CONTENTS

Section 1	— Introduction
Section 2	— Data Controller
Section 3	— Categories of Personal Data Collected
Section 4	— How We Collect Data
Section 5	— Legal Basis for Processing
Section 6	— How We Use Your Data
Section 7	— Data Sharing and Third Parties
Section 8	— International Data Transfers
Section 9	— Data Retention
Section 10	— Data Security
Section 11	— Your Rights
Section 12	— Cookies and Tracking Technologies
Section 13	— Children's Privacy
Section 14	— Data Breach Notification
Section 15	— Changes to This Privacy Policy
Section 16	— Governing Law
Section 17	— Contact Information
Section 18	— Third-Party Privacy Policies

SECTION 1 — INTRODUCTION

1.1 Afriq Global Market Limited ("Company", "we", "us", "our") operates a multi-vendor business-to-consumer (B2C) e-commerce marketplace platform ("Platform") connecting African vendors with buyers across the world. The Platform is accessible at www.afriqglobal.org and through associated mobile applications.

1.2 We are committed to protecting the personal data of all individuals who interact with our Platform, including vendors, buyers, influencers, and website visitors. This Privacy Policy explains

what personal data we collect, why we collect it, how we use it, who we share it with, how long we retain it, and what rights you have in relation to your data.

1.3 This Privacy Policy applies to all users of the Platform regardless of their location, to the extent permitted by applicable data protection laws. Where different legal requirements apply in different jurisdictions, we comply with the most protective standard applicable.

1.4 By accessing or using the Platform, registering an account, or completing a transaction, you acknowledge that you have read, understood, and agreed to this Privacy Policy. If you do not agree with this Privacy Policy, you must not access or use the Platform.

1.5 This Privacy Policy should be read together with our Service Agreement v4.0, Vendor Onboarding and KYC Policy v2.0, and Acceptable Use Policy, which are available at www.afriqglobal.org.

SECTION 2 — DATA CONTROLLER

2.1 For the purposes of applicable data protection legislation (including GDPR, the UK GDPR, the Nigerian Data Protection Act 2023 (NDPA), and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)), the data controller is:

Afriq Global Market Limited

Registered Office: Michigan, United States of America

Website: www.afriqglobal.org

Contact: davidsopekan@afriqglobal.org

2.2 We have entered into Data Processing Agreements with the following third-party data processors in relation to the processing activities described in this Privacy Policy:

- Paystack (payment processing — within Africa)
- Flutterwave (payment processing — within Africa and international)
- Stripe (payment processing — international, non-NGN)
- Terminal Africa (logistics and delivery services)

- Dojah (KYC identity verification — Nigerian and African vendors)
- Smile Identity (KYC identity verification — international and diaspora vendors)

2.3 Where our payment processors and KYC partners act as independent data controllers in their own right (for example, in relation to identity verification checks and financial regulatory obligations), their own privacy policies apply in addition to this Privacy Policy.

SECTION 3 — CATEGORIES OF PERSONAL DATA COLLECTED

We collect the following categories of personal data from users of the Platform:

(a) Identity Data: Full legal name; date of birth; gender; nationality; photograph; government-issued identification documents (including national identity card, passport, and driver's licence details).

(b) Contact Data: Email address; telephone number(s); physical address; billing address; delivery address(es).

(c) Financial Data: Bank account details; mobile money account details; Paystack, Flutterwave, or Stripe account references; transaction history; payout records; VAT or tax identification numbers.

(d) Business Data (Vendors only): Business name; certificate of incorporation or registration number; registered business address; business licence details; director and beneficial owner information; tax identification number.

(e) Technical Data: IP address; device identifier; device type; browser type and version; operating system; login timestamps; session data.

(f) Usage Data: Pages visited; search queries on the Platform; product views; click patterns; time spent on pages; cart and checkout behaviour; interaction history.

(g) Delivery Data: Shipping addresses; package tracking information; delivery preferences; Terminal Africa consignment records.

(h) Communication Data: Messages exchanged through the Platform's messaging system; support ticket content; feedback and reviews submitted by users; complaint records.

(i) KYC and Verification Data: Copies of government-issued identification documents; liveness check and selfie images; business registration documents; sanctions screening results; Politically Exposed Person (PEP) status records.

(j) Marketing and Preference Data (where consent given): Notification preferences; communication preferences; marketing opt-in records.

SECTION 4 — HOW WE COLLECT DATA

4.1 Data You Provide to Us Directly. We collect personal data that you voluntarily provide when you: register for an account on the Platform; complete identity verification (KYC); list products (vendors); place an order (buyers); apply to the Influencer Program; contact our customer support team; submit feedback, reviews, or disputes; or subscribe to marketing communications.

4.2 Data We Collect Automatically. When you access or use the Platform, we automatically collect Technical Data and Usage Data through cookies, web beacons, analytics tools, server logs, and similar technologies. This data is collected to ensure the Platform functions correctly, to maintain security, and to improve the user experience. See Section 12 for more information on cookies.

4.3 Data We Collect from Third Parties. We receive personal data from the following third-party sources:

- **Identity verification providers (Dojah and Smile Identity)** — verification status, identity match results, and risk signals arising from KYC checks;
- **Payment processors (Paystack, Flutterwave, Stripe)** — transaction status, payment confirmation, and fraud signals;
- **Logistics partner (Terminal Africa)** — delivery status, tracking events, and shipment records;
- **Publicly available sources** — business registration databases and regulatory watchlists used for sanctions and PEP screening.

4.4 Applicable Data Protection Legislation. This Privacy Policy is designed to comply with the following data protection laws, as applicable to our users and operations:

1. Nigerian Data Protection Act 2023 (NDPA) and NDPC regulations — applicable to Nigerian users and vendors;
2. General Data Protection Regulation (EU) 2016/679 (GDPR) — applicable to users located in the European Union;

3. UK GDPR and Data Protection Act 2018 — applicable to users located in the United Kingdom;
4. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) — applicable to California residents;
5. Personal Information Protection and Electronic Documents Act (PIPEDA) — applicable to Canadian users;
6. Other applicable data protection and privacy laws in African jurisdictions in which we operate.

Note — South Africa / POPIA

We do not currently operate under a South African regulatory mandate, and the Protection of Personal Information Act (POPIA) does not apply to our operations. All prior references to POPIA and any South African supervisory authority have been removed effective this version (v3.0).

SECTION 5 — LEGAL BASIS FOR PROCESSING

The table below sets out the lawful basis under which we process personal data for each primary processing activity. Where multiple legal bases apply, we have identified the primary basis.

Processing Activity	Legal Basis	Applicable Law
Account registration and management	Performance of a contract	GDPR Art. 6(1)(b); NDPA; PIPEDA
Identity verification (KYC)	Legal obligation; Legitimate interest	GDPR Art. 6(1)(c)/(f); NDPA; BSA
Transaction processing and escrow	Performance of a contract	GDPR Art. 6(1)(b); NDPA; PIPEDA
Auto-confirmation (48–72h Africa / 14d international)	Performance of a contract	GDPR Art. 6(1)(b); NDPA
Payment processing via Paystack, Flutterwave, Stripe	Performance of a contract; Legal obligation	GDPR Art. 6(1)(b)/(c); NDPA

Processing Activity	Legal Basis	Applicable Law
Delivery and logistics coordination (Terminal Africa)	Performance of a contract	GDPR Art. 6(1)(b); NDPA
Customer support and dispute resolution	Legitimate interest; Performance of a contract	GDPR Art. 6(1)(b)/(f); NDPA
Analytics and platform improvement	Legitimate interest	GDPR Art. 6(1)(f); NDPA
Marketing communications (where opted in)	Consent	GDPR Art. 6(1)(a); NDPA; CASL
Fraud detection and platform security	Legitimate interest; Legal obligation	GDPR Art. 6(1)(c)/(f); NDPA
AML and sanctions screening	Legal obligation	GDPR Art. 6(1)(c); NDPA; BSA; MLPA 2011
Influencer program management	Performance of a contract	GDPR Art. 6(1)(b); NDPA
Legal compliance and regulatory reporting	Legal obligation	GDPR Art. 6(1)(c); NDPA

Where processing is based on consent, you have the right to withdraw your consent at any time without affecting the lawfulness of processing carried out prior to withdrawal.

SECTION 6 — HOW WE USE YOUR DATA

6.1 Account Management. We use your Identity Data and Contact Data to create and manage your account, verify your identity, authenticate your login, and maintain your account in good standing.

6.2 Transaction Processing. We use your Financial Data, Identity Data, and Delivery Data to process transactions, hold funds in escrow pending delivery confirmation, and release payouts to vendors. Delivery is confirmed either by a buyer's manual confirmation or, if no confirmation or dispute is raised, by auto-confirmation after the applicable Auto-Confirmation Period (48–72 hours for within-Africa orders; 14 calendar days for international orders).

6.3 Delivery Coordination. We share relevant Delivery Data with Terminal Africa to facilitate the booking, tracking, and completion of shipments.

6.4 Customer Support and Dispute Resolution. We use Communication Data and transaction records to provide customer support, facilitate dispute resolution, and maintain records of complaints and resolutions.

6.5 Platform Improvement and Analytics. We use Technical Data and Usage Data in aggregated and anonymised form to improve the Platform's functionality, user interface, and product recommendations.

6.6 Marketing and Communications. Where you have opted in, we use your Contact Data and Marketing Preference Data to send promotional communications about new features, offers, and platform updates. You may opt out at any time by clicking the unsubscribe link in any marketing email or by updating your account preferences.

6.7 Fraud Prevention and Security. We use Technical Data, Usage Data, and KYC and Verification Data to detect and prevent fraud, unauthorised access, money laundering, and other unlawful activities.

6.8 Legal Compliance. We process your data as required to comply with applicable legal obligations, regulatory requirements, court orders, and requests from competent authorities.

6.9 Influencer Program Administration. We use Contact Data, Financial Data, and Usage Data to manage influencer accounts, track referrals, and calculate and process revenue share payments.

SECTION 7 — DATA SHARING AND THIRD PARTIES

7.1 Vendors. We share limited buyer data (name, delivery address, and order details) with the relevant vendor solely for the purpose of order fulfilment. Vendors are prohibited from using buyer data for any purpose other than fulfilment of the relevant order.

7.2 Payment Partners. We share transaction data (including payment amount, currency, and payer references) with our payment processing partners (Paystack, Flutterwave, and Stripe) to facilitate checkout, payment verification, escrow management, and vendor payouts. Each payment partner processes data in accordance with their own privacy policy and applicable financial regulations.

7.3 Logistics Partner. We share delivery data (name, delivery address, contact number, and package details) with Terminal Africa to facilitate shipment booking, tracking, and delivery.

7.4 Identity Verification Partners. We share Identity Data and KYC and Verification Data with Dojah (for Nigerian and African vendor verification) and Smile Identity (for international and diaspora vendor verification) to fulfil our KYC obligations. These partners act as data processors under our instruction and under binding Data Processing Agreements.

7.5 Legal and Regulatory Authorities. We may disclose personal data to regulatory bodies, law enforcement agencies, courts, or other government authorities where required by applicable law, court order, or regulatory directive. We will notify affected users of such disclosures where legally permitted.

7.6 Business Transfers. In the event of a merger, acquisition, restructuring, or sale of all or substantially all of our assets, user data may be transferred to the acquiring entity subject to equivalent privacy protections.

7.7 No Sale of Data. We do not sell, rent, trade, or otherwise transfer your personal data to any third party for that party's own commercial purposes.

7.8 Service Providers. We may engage other carefully selected third-party service providers (for example, cloud hosting, email delivery, and security services) who process data on our behalf under binding confidentiality and data processing agreements. These providers process data only on our instructions and do not use your data for their own purposes.

SECTION 8 — INTERNATIONAL DATA TRANSFERS

8.1 Our Platform serves users in multiple jurisdictions, and your personal data may be transferred to and processed in countries other than the country in which you reside. In particular, data may be transferred to the United States (where our Company is incorporated), Nigeria, the United Kingdom, and other countries where our service providers operate.

8.2 Where personal data is transferred from the European Economic Area (EEA) or the United Kingdom to a country that does not benefit from an adequacy decision, we rely on Standard Contractual Clauses (SCCs) approved by the European Commission or the UK Information Commissioner's Office (ICO), together with appropriate supplementary measures where required, to ensure that your data receives an adequate level of protection.

8.3 For data transfers involving Nigerian users, we comply with the transfer provisions of the Nigerian Data Protection Act 2023 (NDPA) and any applicable NDPC guidelines, including ensuring that the receiving jurisdiction provides an adequate level of data protection or that appropriate safeguards are in place.

8.4 For data transfers involving Canadian users, we comply with PIPEDA and applicable provincial privacy legislation.

8.5 Where our payment processors and KYC partners transfer data internationally in the course of providing their services, those transfers are governed by the data transfer provisions of those partners' own data processing agreements, applicable regulatory approvals, and their commitments under GDPR, UK GDPR, and other applicable laws.

Server Jurisdiction — Pending Confirmation

8.6 The primary infrastructure supporting the Platform is hosted on servers located in [server jurisdiction to be specified upon go-live, prior to 1 September 2026]. We will publish the confirmed server jurisdiction on our website at www.afriqglobal.org.

SECTION 9 — DATA RETENTION

We retain personal data only for as long as is necessary for the purposes set out in this Privacy Policy and for the period required by applicable law. The following retention periods apply:

Category of Data	Retention Period
Account and Identity Data	Duration of account + 7 years after account closure
Financial and Transactional Data	7 years from transaction date
KYC and Verification Data	Duration of account + 7 years after account closure
Delivery and Logistics Data	3 years from delivery date
Communication and Support Data	3 years from the date of the relevant communication
Technical and Log Data	12 months from collection
Marketing Preference Data	Until opt-out, then 2 years

9.1 After the applicable retention period, data is securely deleted or anonymised in accordance with our data destruction procedures.

9.2 We may retain personal data for longer than the periods above where required by: (a) an ongoing legal dispute or regulatory investigation; (b) a court order or regulatory directive; or (c) a contractual obligation with a payment processor or regulatory body.

SECTION 10 — DATA SECURITY

10.1 We implement appropriate technical and organisational security measures to protect personal data against unauthorised access, accidental loss, destruction, alteration, or disclosure. These measures include:

7. Encryption of personal data in transit (TLS/SSL) and at rest (AES-256 or equivalent);
8. Access controls ensuring that personal data is accessible only to authorised personnel on a need-to-know basis;
9. Multi-factor authentication for Platform administrative access;
10. Regular security assessments, penetration testing, and vulnerability management;
11. Employee data protection training and confidentiality obligations;
12. Incident detection and response procedures as described in Section 14.

10.2 Payment Security. Payment data processed through our payment partners (Paystack, Flutterwave, and Stripe) is handled in accordance with those partners' PCI DSS (Payment Card Industry Data Security Standard) compliance obligations. We do not store full card numbers, CVV codes, or payment card magnetic stripe data on our own systems.

10.3 KYC Data Security. Identity verification documents and biometric data submitted for KYC purposes are processed by Dojah and Smile Identity in accordance with their security standards and our Data Processing Agreements. Access to KYC records within our systems is restricted to authorised compliance personnel only.

10.4 Vendor Responsibility. Vendors are responsible for maintaining the security of their Vendor Dashboard login credentials and for ensuring that any buyer data shared with them for order fulfilment purposes is kept secure and used only for the purpose of fulfilling the relevant order.

SECTION 11 — YOUR RIGHTS

11.1 Summary of Rights. The rights available to you depend on your jurisdiction and the legal basis under which we process your data. The table below summarises the rights available by jurisdiction.

Right	GDPR (EU/UK)	NDPA (Nigeria)	CCPA/CPRA (California)	PIPEDA (Canada)
Right to access / know	Yes	Yes	Yes	Yes
Right to rectification / correction	Yes	Yes	Yes	Yes
Right to erasure / deletion	Yes	Yes	Yes	Yes
Right to restrict processing	Yes	Yes	No	Limited
Right to data portability	Yes	Yes	Yes (categories)	Limited
Right to object to processing	Yes	Yes	Yes (opt-out of sale)	Yes
Right to withdraw consent	Yes	Yes	Yes	Yes
Right to non-discrimination	N/A	N/A	Yes	Yes

11.2 How to Exercise Your Rights. To exercise any of the rights described in this Section, please submit a written request to our Data Protection Officer using the contact details in Section 17. We will respond to all rights requests within:

13. Thirty (30) days for GDPR and UK GDPR requests (extendable by a further sixty (60) days for complex requests with prior notice);

14. Thirty (30) days for NDPA requests;

15. Forty-five (45) days for CCPA/CPRA requests (extendable by a further forty-five (45) days with prior notice);

16. Thirty (30) days for PIPEDA requests.

11.3 Identity Verification for Rights Requests. We will verify the identity of any person submitting a rights request before disclosing or modifying personal data. We may request appropriate identification documents as part of this process.

11.4 Limitations on Rights. Certain rights may be subject to limitations under applicable law. For example, we may refuse an erasure request where retention is required by law (such as for

financial reporting or AML compliance) or where your data is necessary for the establishment, exercise, or defence of legal claims.

11.5 Supervisory Authorities. You have the right to lodge a complaint with the relevant supervisory authority in your jurisdiction if you believe we have processed your data unlawfully. Key supervisory authorities include:

Jurisdiction	Supervisory Authority	Contact
European Union	Relevant national Data Protection Authority (DPA)	edpb.europa.eu
United Kingdom	Information Commissioner's Office (ICO)	ico.org.uk
Nigeria	Nigeria Data Protection Commission (NDPC)	ndpc.gov.ng
United States (California)	California Privacy Protection Agency (CPPA)	cppa.ca.gov
Canada	Office of the Privacy Commissioner (OPC)	priv.gc.ca

SECTION 12 — COOKIES AND TRACKING TECHNOLOGIES

12.1 We use cookies and similar tracking technologies (including web beacons, pixels, and local storage) on our Platform to provide core platform functionality, remember your preferences, and analyse how users interact with the Platform.

12.2 Categories of Cookies:

Category	Purpose	Basis
Strictly Necessary	Essential for login, cart, checkout, and security	No consent required
Functional	Remembers language, currency, and display preferences	Consent
Analytics	Collects anonymised usage data for platform improvement	Consent
Marketing	Tracks interactions for personalised advertising	Consent

12.3 You can manage your cookie preferences through our cookie consent banner displayed when you first access the Platform, or at any time through your browser settings or our Cookie Preference Centre available at www.afriqglobal.org.

12.4 Please note that disabling strictly necessary cookies may prevent the Platform from functioning correctly.

SECTION 13 — CHILDREN'S PRIVACY

13.1 The Platform is not directed at or intended for use by individuals under the age of eighteen (18) years. We do not knowingly collect, process, or retain personal data relating to minors under the age of 18.

13.2 If we become aware that we have inadvertently collected personal data from an individual under the age of 18, we will take immediate steps to delete such data from our records.

13.3 If you believe that we may have collected personal data from a minor, please contact us immediately using the contact details in Section 17.

SECTION 14 — DATA BREACH NOTIFICATION

14.1 We maintain an incident response procedure designed to detect, contain, assess, and respond to personal data breaches promptly and effectively.

14.2 In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, we will:

17. Under GDPR and UK GDPR: notify the relevant supervisory authority within seventy-two (72) hours of becoming aware of the breach, and notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights;

18. Under NDPA (Nigeria): notify the Nigeria Data Protection Commission (NDPC) as soon as reasonably possible after becoming aware of a significant breach, and notify affected individuals where there is a risk of harm;

19. Under CCPA/CPRA (California): notify affected California residents of a breach of their unencrypted personal information in the most expedient manner possible;

20. Under PIPEDA (Canada): notify the Office of the Privacy Commissioner and affected individuals of a breach that poses a real risk of significant harm.

14.3 Breach notifications to affected users will include: a description of the nature of the breach; the categories and approximate number of individuals and records affected; the name and contact details of our Data Protection Officer; the likely consequences of the breach; and the measures we have taken or propose to take to address the breach.

SECTION 15 — CHANGES TO THIS PRIVACY POLICY

15.1 We reserve the right to amend this Privacy Policy from time to time to reflect changes in our business practices, legal obligations, or technological developments.

15.2 Where we make material changes, we will notify users via email to their registered email address, a prominent notice on the Platform, and/or notification through the mobile application, no less than thirty (30) calendar days before the effective date of the change.

15.3 Your continued use of the Platform after the effective date of a revised Privacy Policy constitutes your acceptance of the changes. If you do not accept the revised Privacy Policy, you must cease using the Platform and may request the deletion of your account.

SECTION 16 — GOVERNING LAW

16.1 This Privacy Policy is governed by and shall be construed in accordance with the laws of the State of Michigan, United States of America, without prejudice to any mandatory data protection rights afforded to you under the laws of the jurisdiction in which you are located.

16.2 Specifically:

21. The processing of personal data of users located in the European Union and European Economic Area is subject to the GDPR;

22. The processing of personal data of users located in the United Kingdom is subject to the UK GDPR and the Data Protection Act 2018;

23. The processing of personal data of users located in Nigeria is subject to the Nigerian Data Protection Act 2023 (NDPA);

24. The processing of personal data of California residents is subject to the CCPA and CPRA;

25. The processing of personal data of Canadian users is subject to PIPEDA and applicable provincial privacy legislation.

16.3 Where there is a conflict between Michigan law and any of the mandatory data protection rights listed in Section 16.2, the applicable mandatory law of the user's jurisdiction shall prevail in respect of those rights.

SECTION 17 — CONTACT INFORMATION

17.1 Data Protection Officer / Privacy Enquiries. For any questions, concerns, or requests relating to this Privacy Policy or your personal data, please contact:

Data Protection Officer

Afriq Global Market Limited

Email: davidsopekan@afriqglobal.org

Website: www.afriqglobal.org

17.2 We are committed to resolving all privacy-related concerns promptly and in good faith. If you are not satisfied with our response, you have the right to escalate your concern to the relevant supervisory authority for your jurisdiction as listed in Section 11.5.

SECTION 18 — THIRD-PARTY PRIVACY POLICIES

18.1 The Platform may contain links to third-party websites and services. This Privacy Policy applies only to the Platform and does not cover the privacy practices of any third-party sites or services. We encourage you to review the privacy policies of any third-party sites you visit.

18.2 Payment Partner Policies. The following payment partners process personal data in connection with transactions made on the Platform. Please review their privacy policies for details of their data practices:

1. Paystack — paystack.com/privacy
2. Flutterwave — flutterwave.com/us/en/privacy-policy
3. Stripe — stripe.com/privacy

18.3 KYC Partner Policies. Our identity verification partners process personal data in connection with vendor KYC checks:

4. Dojah — dojah.io/privacy
5. Smile Identity — smileidentity.com/privacy-policy

18.4 Logistics Partner Policy. Our logistics partner processes personal data in connection with shipment booking and delivery:

6. Terminal Africa — terminalafrica.com/privacy-policy

AFRIQ GLOBAL MARKET LIMITED

Privacy Policy — Version 3.0 (Final) | Effective: 1 September 2026

www.afriqglobal.org | davidsopekan@afriqglobal.org

This document supersedes Privacy Policy v2.1 (5 August 2026) in its entirety.

Classification: PUBLIC | End of Privacy Policy v3.0