KAVIPAY.IO

COMPREHENSIVE PRIVACY POLICY

Last Updated: February 9, 2026
Effective Date: February 9, 2026

PloutosLabs International Ltd
(Trading as Kavipay.io)

TABLE OF CONTENTS

1. INTRODUCTION AND SCOPE

1.1 Welcome to Kavipay

Thank you for choosing Kavipay.io ("Kavipay," "we," "us," or "our"), a financial technology service operated by PloutosLabs International Ltd, a company duly incorporated and registered in the Federal Republic of Nigeria with Registration Number RC 8059896. Kavipay is a comprehensive payment card and financial services platform that enables users to access virtual and physical payment cards, conduct cryptocurrency and fiat currency transactions, pay utility bills, and manage their financial activities securely and efficiently.

1.2 Purpose of This Privacy Policy

This Privacy Policy describes in detail how PloutosLabs International Ltd collects, uses, stores, shares, and protects your personal data when you:

- Access, browse, or use the Kavipay website located at https://kavipay.io
- Download, install, or use the Kavipay mobile application on iOS or Android devices
- Create an account or register for Kavipay Services
- Apply for, receive, activate, or use any Kavipay payment card (virtual or physical)
- Fund your Kavipay account or cards using cryptocurrency or Nigerian Naira
- Conduct transactions, purchases, withdrawals, or transfers using Kavipay Services
- Pay utility bills, purchase airtime, or access other bill payment services
- Contact our customer support team via any communication channel
- Participate in surveys, promotions, contests, or marketing campaigns
- Interact with us on social media platforms or through third-party integrations

1.3 Your Consent and Agreement

By accessing, registering for, or using any Kavipay Service, you explicitly acknowledge that you have read, understood, and AGREE to be legally bound by this Privacy Policy in its entirety. If you do not agree with any provision of this Privacy Policy, you must immediately cease all use of Kavipay Services and refrain from providing any personal data to us.

Your continued use of Kavipay Services after any amendments or updates to this Privacy Policy constitutes your acceptance of those changes. We will notify you of material changes through email, in-app notifications, or prominent notices on our website.

1.4 Scope and Applicability

This Privacy Policy applies to all personal data collected, processed, or stored by Kavipay through:

- Our website and mobile applications
- Physical card delivery services provided through Speedaf Logistics
- Card issuance and banking services provided through Safe Haven Microfinance Bank
- Virtual card programs operated by Sudo.africa and Payscribe
- Payment processing and transaction services
- Customer support interactions across all channels
- Marketing and promotional communications
- Third-party integrations and partner services

2. DATA CONTROLLER AND CONTACT INFORMATION

2.1 Identity of Data Controller

The data controller responsible for the collection, processing, and protection of your personal data is:

PloutosLabs International Ltd (trading as Kavipay.io)
Registered Company Number: RC 8059896
Registered Office Address: NO. 15 , WOKOGOLOMA STREET, D-LINE, PORT HARCOURT, RIVERS STATE, NIGERIA
Principal Place of Business: 1st Floor, Right Wing, Inside Sunbeth fuel Station, Opposite Dunamis Glory Dome Airport Road Lugbe Abuja
Country of Incorporation: Federal Republic of Nigeria

2.2 Data Protection Officer

We have appointed a dedicated Data Protection Officer (DPO) who is responsible for overseeing our data protection strategy, ensuring compliance with the Nigeria Data Protection Regulation (NDPR) and other applicable laws, and serving as your primary point of contact for all privacy-related inquiries.

Data Protection Officer Contact Information:
Email: dpo@kavipay.io

2.3 General Contact Information

For general inquiries, customer support, or non-privacy related matters:

- General Email: support@kavipay.io
- Privacy Inquiries: privacy@kavipay.io
- Security Issues: security@kavipay.io
- Marketing Opt-Out: marketing-optout@kavipay.io
- Data Rights Requests: datarights@kavipay.io
- Complaints: complaints@kavipay.io
- Website: https://kavipay.io
- Phone Support: 0700 CALL KAVIPAY (0700 2255 5284729)
- Business Hours: Monday - Friday, 8:00 AM - 5:00 PM WAT

3. DEFINITIONS AND INTERPRETATION

In this Privacy Policy, unless the context otherwise requires, the following terms shall have the meanings set forth below:

Account: means your Kavipay user account created to access and use our Services, including all associated data, settings, and preferences.

AML: means Anti-Money Laundering laws, regulations, and compliance requirements applicable in Nigeria and other relevant jurisdictions.

Biometric Data: means unique physical characteristics used for identification and authentication purposes, including but not limited to fingerprints, facial recognition data, voice patterns, and iris scans.

Card: means any payment card issued through Kavipay Services, including virtual cards (VISA, Mastercard) and physical cards (Verve, Afrigo).

CBN: means the Central Bank of Nigeria, the apex regulatory authority for banking and financial services in Nigeria.

Cryptocurrency: means digital or virtual currency that uses cryptography for security and operates on blockchain technology, including but not limited to USDT, BUSD, BNB, and other tokens supported by Kavipay.

Data Subject: means any identified or identifiable natural person whose personal data we process, including Kavipay users, website visitors, and service applicants.

GDPR: means the General Data Protection Regulation (EU) 2016/679, applicable to data processing activities involving individuals in the European Economic Area.

KYC: means Know Your Customer procedures and identity verification processes required by law and financial regulations.

NDPR: means the Nigeria Data Protection Regulation 2019, the primary data protection legislation in Nigeria.

Personal Data: means any information relating to an identified or identifiable natural person, including names, contact details, identification numbers, financial information, location data, online identifiers, and any other data that can directly or indirectly identify an individual.

Processing: means any operation performed on personal data, including collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, transmission, erasure, or destruction.

Services: means all products, services, features, and functionalities offered by Kavipay, including card services, payment processing, bill payments, cryptocurrency funding, and related services.

Transaction: means any financial operation conducted using Kavipay Services, including purchases, withdrawals, transfers, bill payments, and card funding.

User: means any person who accesses, registers for, or uses Kavipay Services, including account holders, cardholders, and website visitors.

4. CATEGORIES OF PERSONAL DATA WE COLLECT

4.1 Identity and Contact Information

We collect the following identity and contact data:

- Full legal name (including any former names, aliases, or maiden names)
- Date of birth and age
- Gender and nationality
- Residential address (current and/or previous addresses for verification purposes)
- Email address (primary and/or secondary)
- Mobile phone number and/or landline number
- Emergency contact information
- Preferred language and communication preferences

4.2 Government-Issued Identification Data

To comply with Nigerian KYC and AML regulations, we collect:

- National Identification Number (NIN)
- Bank Verification Number (BVN)
- International Passport number and details
- Driver's License number and details
- Voter's Card information
- Tax Identification Number (TIN)
- Copies of government-issued identification documents
- Verification photographs and selfies
- Nationality and citizenship status
- Place of birth and country of residence

4.3 Financial and Transaction Data

We collect and process comprehensive financial information, including:

- Bank account numbers and details (Nigerian and international accounts)
- Account balances and transaction history
- Payment card information (card numbers, expiry dates, CVV - processed securely through PCI DSS compliant partners)
- Cryptocurrency wallet addresses and balances
- Transaction amounts, dates, times, and locations
- Merchant information and transaction descriptions
- Payment methods and preferences
- Source of funds declarations
- Income information and employment details

- Spending patterns and transaction categorization
- Bill payment history and utility account numbers
- Currency exchange rates and conversion data
- Fee and charge information
- Refund and dispute records

4.4 Technical and Device Data

When you access Kavipay Services, we automatically collect technical data:

- Device identifiers (IMEI, device ID, advertising ID)
- Device type, model, manufacturer, and operating system
- Mobile network information (carrier name, network type)
- IP address (static and dynamic)
- MAC address and network identifiers
- Browser type, version, and language settings
- Screen resolution and device orientation
- Time zone and locale settings
- Installed applications and app permissions granted
- App version and update history
- Crash reports and error logs
- Performance data and diagnostic information

4.5 Location Data

We collect various types of location information:

- Precise GPS location (when you grant location permissions)
- Approximate location derived from IP address
- Cell tower triangulation data
- Wi-Fi access point information
- Location-based transaction data (ATM locations, merchant locations)
- Delivery addresses for physical cards
- Billing addresses
- Location history and patterns

4.6 Behavioral and Usage Data

We track how you interact with Kavipay Services:

- Login and logout times
- Features and services used
- Navigation paths and click patterns
- Time spent on different screens and features
- Search queries and filters applied

- Settings and preferences configured
- Notifications opened and interactions
- In-app messages and communications
- Customer support interactions and chat transcripts
- Survey responses and feedback provided
- Marketing email opens and click-through rates

4.7 Biometric and Authentication Data

For security and authentication purposes, we may collect:

- Fingerprint templates (stored securely on your device)
- Facial recognition data (for identity verification and app authentication)
- Voice recordings and patterns (for voice authentication features)
- Behavioral biometrics (typing patterns, swipe gestures)
- Liveness detection data (to prevent spoofing)
- Document authentication data (security features on ID documents)

4.8 Social Media and Public Information

If you connect social media accounts or provide public information:

- Social media profile information (name, profile picture, user ID)
- Friends lists and social connections
- Posts, comments, and interactions on our social media channels
- Publicly available information from social media platforms
- Referral information when you invite friends

4.9 Employment and Occupation Data

For regulatory compliance and risk assessment:

- Employer name and address
- Job title and description
- Industry and sector of employment
- Length of employment
- Monthly or annual income range
- Business registration information (for business accounts)
- Proof of income documents

4.10 Communication and Correspondence Data

We retain records of communications with you:

- Email correspondence
- Live chat transcripts
- Phone call recordings (with your consent)

- SMS and push notification content
- Customer support tickets and resolution history
- Complaint records and investigation files
- Feedback and survey responses

5. SOURCES OF PERSONAL DATA

5.1 Information You Provide Directly

Most personal data we collect comes directly from you when you:

- Complete the registration and account creation process
- Submit Know Your Customer (KYC) verification documents
- Apply for virtual or physical payment cards
- Fund your account using bank transfers or cryptocurrency
- Conduct transactions and make purchases
- Pay bills and utilities through our platform
- Update your profile information and settings
- Contact customer support for assistance
- Participate in surveys, promotions, or contests
- Submit feedback or reviews
- Communicate with us via email, chat, phone, or social media

5.2 Licensed Banking and Financial Partners

We receive personal data from our authorized service providers:

Safe Haven Microfinance Bank (CBN Licensed):

- Banking transaction records
- Account opening and closure information
- Credit history and financial standing
- KYC verification results
- Suspicious activity reports
- Regulatory compliance data

Sudo.africa (PCI DSS Compliant - VISA/Mastercard Programs):

- Virtual card issuance data
- Transaction authorization records
- Fraud detection and prevention data
- Card network compliance information
- Chargeback and dispute records

Payscribe (PCI DSS Compliant Card Services):

- Card provisioning information
- Payment processing data
- Security and authentication records
- Transaction settlement data

5.3 Logistics and Delivery Partners

Speedaf Logistics provides us with:

- Delivery confirmation records
- Shipment tracking information
- Recipient verification data
- Delivery address accuracy confirmations
- Proof of delivery photographs and signatures
- Failed delivery attempt records

6. LEGAL BASIS FOR PROCESSING

Under the Nigeria Data Protection Regulation (NDPR) 2019 and other applicable laws, we process your personal data on the following legal bases:

6.1 Consent

You have provided explicit, informed, and freely given consent for us to process your personal data for specific purposes. We obtain consent through:

- Registration and account creation acceptance checkboxes
- Explicit opt-in for marketing communications
- Permission grants for location access, camera, biometric authentication
- Acceptance of this Privacy Policy

You may withdraw your consent at any time through account settings or by contacting us at datarights@kavipay.io. However, withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal and may limit your ability to use certain Services.

6.2 Contract Performance

Processing is necessary to perform our contractual obligations to you under:

- Kavipay Terms and Conditions
- Card Issuance Agreements
- Service Level Agreements with third-party providers
- Delivery contracts for physical cards

This includes processing necessary to provide Services, process transactions, issue and manage cards, and fulfill all contractual promises made to you.

6.3 Legal Obligation

We are required by law to process certain personal data to comply with:

- Central Bank of Nigeria (CBN) banking and payment regulations
- Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements
- Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) laws
- Nigeria Data Protection Regulation (NDPR) 2019
- Tax reporting obligations (Federal Inland Revenue Service requirements)
- Economic and Financial Crimes Commission (EFCC) directives
- Court orders, legal proceedings, and regulatory investigations
- Nigeria Deposit Insurance Corporation (NDIC) requirements
- Financial Reporting Council of Nigeria (FRCN) standards

6.4 Legitimate Interests

Processing is necessary for our legitimate business interests or those of third parties, provided these interests do not override your fundamental rights and freedoms:

- Fraud prevention and security monitoring
- Risk assessment and credit evaluation
- Network and information security
- Business analytics and service improvement
- Protecting against legal liability
- Enforcing our Terms and Conditions
- Mergers, acquisitions, and corporate reorganizations
- Debt collection and payment recovery

7. PURPOSES OF DATA PROCESSING

We process your personal data for the following specific purposes:

7.1 Account Management and User Services

- Creating, maintaining, and managing your Kavipay account
- Authenticating your identity and verifying account access
- Processing account updates, changes, and closures
- Managing your profile settings and preferences
- Providing customer support and responding to inquiries
- Sending account notifications and service updates
- Processing password resets and security verifications

7.2 Card Issuance and Management

- Issuing virtual VISA and Mastercard cards through licensed partners
- Processing applications for physical Verve and Afrigo cards
- Activating and deactivating cards
- Managing card limits, controls, and restrictions
- Processing card replacement requests
- Generating virtual card numbers and security codes
- Coordinating physical card delivery through Speedaf Logistics

7.3 Transaction Processing and Payment Services

- Processing purchases, payments, and transfers
- Authorizing and settling transactions
- Converting between currencies (crypto to fiat, fiat to crypto)
- Processing bill payments (electricity, airtime, internet, cable TV)
- Recording transaction history and generating statements
- Processing refunds, reversals, and chargebacks
- Calculating and applying fees and charges

7.4 Compliance and Regulatory Requirements

- Conducting Know Your Customer (KYC) verification
- Performing Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)
- Monitoring for suspicious transactions and money laundering
- Filing Suspicious Transaction Reports (STRs) with authorities
- Maintaining records for regulatory inspections and audits
- Responding to requests from law enforcement and regulators
- Complying with international sanctions and embargo lists
- Reporting large cash transactions as required by law

7.5 Security and Fraud Prevention

- Detecting and preventing fraudulent transactions
- Monitoring for unusual account activity
- Implementing risk-based authentication
- Investigating security incidents and breaches
- Protecting against unauthorized access and cyber threats
- Conducting security audits and penetration testing
- Implementing fraud detection algorithms and machine learning models

8. DATA SHARING AND DISCLOSURE

We may share your personal data with the following categories of recipients:

8.1 Service Providers and Business Partners

We share data with trusted partners who provide essential services:

- Safe Haven Microfinance Bank - Banking services, card issuance, account management
- Sudo.africa - VISA and Mastercard virtual card programs (PCI DSS compliant)
- Payscribe - Card provisioning and payment processing (PCI DSS compliant)
- Speedaf Logistics - Physical card delivery and shipment tracking
- Cloud hosting providers - Data storage and infrastructure services
- IT security firms - Cybersecurity, threat detection, and incident response
- Identity verification services - KYC/AML compliance and document authentication
- Payment gateways and processors - Transaction routing and settlement
- Customer support platforms - Ticketing, live chat, and help desk systems
- Marketing and analytics providers - Campaign management and data analysis

9. INTERNATIONAL DATA TRANSFERS

While Kavipay primarily operates in Nigeria and processes data within Nigerian jurisdiction, some of our service providers may process personal data in other countries, including:

- Cloud hosting services (AWS, Google Cloud, Microsoft Azure) with data centers outside Nigeria
- Payment networks (VISA, Mastercard) with global processing infrastructure
- Software-as-a-Service (SaaS) providers with international operations
- Cybersecurity and fraud detection services with cross-border capabilities

9.1 Safeguards for International Transfers

When we transfer personal data internationally, we ensure adequate protection through:

- Standard Contractual Clauses (SCCs) approved by the Nigeria Data Protection Bureau
- Adequacy assessments of destination countries' data protection frameworks
- Binding Corporate Rules for multinational service providers
- Certification schemes and codes of conduct
- Explicit consent for transfers where required
- Contractual obligations requiring equivalent data protection standards

10. DATA SECURITY AND PROTECTION MEASURES

We implement comprehensive technical and organizational security measures to protect your personal data:

10.1 Technical Security Controls

- 256-bit AES encryption for data at rest
- TLS 1.3 encryption for data in transit
- End-to-end encryption for sensitive communications
- Multi-factor authentication (MFA) for account access
- Biometric authentication (fingerprint, facial recognition)
- Hardware Security Modules (HSMs) for cryptographic key management
- Tokenization of payment card data
- Firewalls and intrusion detection/prevention systems (IDS/IPS)
- DDoS protection and traffic filtering
- Regular security patches and vulnerability management
- Secure coding practices and code review processes
- Penetration testing and security audits

10.2 Organizational Security Measures

- Access controls based on role-based permissions (RBAC)
- Employee background checks and security clearances
- Mandatory privacy and security training for all staff
- Non-disclosure agreements (NDAs) for employees and contractors
- Incident response and disaster recovery plans
- Business continuity management procedures
- Regular security awareness campaigns
- Third-party security assessments and due diligence
- Secure development lifecycle (SDLC) practices

11. DATA RETENTION AND DELETION

We retain your personal data only for as long as necessary to fulfill the purposes outlined in this Privacy Policy, unless a longer retention period is required or permitted by law.

11.1 Retention Periods by Data Category

Account Information: Duration of account + 7 years after closure

Transaction Records: 10 years from transaction date (CBN requirement)

KYC/AML Documentation: Minimum 7 years after account closure (EFCC requirement)

Communication Records: 3 years from last communication

Marketing Data: Until consent withdrawal + 30 days

Technical Logs: 12 months from collection

Security Incident Records: 7 years from incident resolution

Complaint Records: 6 years from complaint resolution

Legal Documents: Duration of limitation period + 2 years

11.2 Secure Deletion Procedures

When retention periods expire, we securely delete or anonymize your data using:

- Cryptographic erasure of encryption keys
- Overwriting of storage media with random data
- Physical destruction of hardware containing sensitive data
- Anonymization techniques that prevent re-identification
- Regular purging of backup systems

12. YOUR RIGHTS AS A DATA SUBJECT

Under the Nigeria Data Protection Regulation (NDPR) 2019, you have the following rights:

12.1 Right to Access

You have the right to:

- Request confirmation of whether we process your personal data
- Obtain a copy of your personal data in our possession
- Receive information about how we use and share your data
- Access your data processing history

We will provide this information within 30 days of your request, free of charge for the first request per year.

12.2 Right to Rectification

You may request correction of inaccurate or incomplete personal data. We will update your information within 14 days and notify all third parties with whom we shared the incorrect data.

12.3 Right to Erasure (Right to Be Forgotten)

You may request deletion of your personal data when:

- The data is no longer necessary for the purposes collected
- You withdraw consent and no other legal basis exists
- You object to processing and we have no overriding legitimate grounds
- The data was unlawfully processed
- Erasure is required by law

This right is subject to legal retention requirements (e.g., CBN regulations requiring 7-10 year retention of financial records).

12.4 Right to Object

You may object to processing based on legitimate interests or for direct marketing purposes. We will cease processing unless we demonstrate compelling legitimate grounds that override your interests.

12.5 Right to Data Portability

You have the right to receive your personal data in a structured, commonly used, machine-readable format (CSV, JSON, PDF) and transmit it to another service provider.

12.6 Right to Restrict Processing

You may request restriction of processing when:

- You contest the accuracy of your personal data
- Processing is unlawful but you prefer restriction over erasure
- We no longer need the data but you need it for legal claims
- You have objected to processing pending verification of legitimate grounds

12.7 How to Exercise Your Rights

To exercise any of these rights:

- Send email to: datarights@kavipay.io
- Use the in-app 'Data Rights Request' feature
- Contact our Data Protection Officer at: dpo@kavipay.io

We will respond to requests within 30 days and may require identity verification to prevent unauthorized access.

13. AUTOMATED DECISION-MAKING AND PROFILING

Kavipay uses automated decision-making and profiling for the following purposes:

13.1 Fraud Detection and Prevention

We use machine learning algorithms to:

- Analyze transaction patterns for suspicious activity
- Assess risk scores for unusual transactions
- Flag potential fraud in real-time
- Block high-risk transactions automatically

You have the right to request human review of automated decisions that significantly affect you.

13.2 Credit and Risk Assessment

We may use automated systems to:

- Evaluate creditworthiness for card limits
- Assess eligibility for services and features
- Determine transaction approval or decline
- Calculate risk-based pricing and fees

13.3 Personalization and Recommendations

We use profiling to:

- Recommend relevant services and features
- Customize app interface and user experience
- Provide spending insights and financial tips
- Suggest bill payment reminders

You may opt out of profiling for marketing purposes through account settings.

14. COOKIES AND TRACKING TECHNOLOGIES

We use cookies and similar technologies to enhance your experience. For comprehensive information, please refer to our separate Cookies Policy at https://kavipay.io/cookies

14.1 Types of Cookies We Use

- Strictly Necessary Cookies - Essential for website and app functionality
- Performance Cookies - Analytics and usage statistics
- Functional Cookies - Remember preferences and settings
- Targeting Cookies - Personalized advertising
- Social Media Cookies - Social sharing and login features

14.2 Managing Cookie Preferences

You can control cookies through:

- Cookie consent banner when first visiting our website
- Website footer 'Cookie Settings' link
- Mobile app Settings > Privacy > Cookies
- Browser settings (Chrome, Safari, Firefox, Edge)
- Mobile device settings (iOS, Android)

15. MARKETING COMMUNICATIONS AND PREFERENCES

15.1 Types of Marketing Communications

With your consent, we may send you:

- Promotional emails about new features and services
- SMS notifications about special offers and discounts
- Push notifications about campaigns and promotions
- In-app messages about product updates
- Personalized recommendations based on your usage

15.2 Opting Out of Marketing

You can unsubscribe from marketing communications:

- Click 'Unsubscribe' link in promotional emails
- Reply 'STOP' to marketing SMS messages
- Disable push notifications in app settings
- Email: marketing-optout@kavipay.io
- Adjust preferences in Account > Settings > Notifications

Note: Even if you opt out of marketing, we will still send transactional messages (account alerts, security notifications, regulatory updates).

16. THIRD-PARTY SERVICES AND INTEGRATIONS

Kavipay integrates with various third-party services. Each service provider has its own privacy policy governing their data practices:

16.1 Payment Network Providers

- VISA Inc. - Privacy Policy: https://www.visa.com/privacy
- Mastercard International - Privacy Policy: https://www.mastercard.com/privacy
- Nigeria Inter-Bank Settlement System (NIBSS) - Verve and Afrigo networks

16.2 Service Providers

- Safe Haven MFB - https://safehavenmfb.com/privacy
- Sudo.africa - https://sudo.africa/privacy
- Payscribe - https://payscribe.ng/privacy
- Speedaf Logistics - https://speedaf.com/privacy

17. CHILDREN'S PRIVACY AND AGE VERIFICATION

Kavipay Services are intended exclusively for persons 18 years of age and older. We do not knowingly collect personal data from minors.

17.1 Age Verification Process

- Self-declaration during registration
- Government-issued ID verification (must show age 18+)
- Bank Verification Number (BVN) age check
- National Identification Number (NIN) age verification

18. DATA BREACH NOTIFICATION PROCEDURES

18.1 Our Commitment to Breach Response

In the event of a personal data breach, we will:

- Contain the breach and assess the scope within 24 hours
- Notify the Nigeria Data Protection Bureau (NDPB) within 72 hours
- Inform affected users without undue delay
- Provide details of the breach, potential consequences, and remedial actions
- Offer identity protection services if applicable
- Conduct a full investigation and implement preventive measures

19. SPECIAL CATEGORIES OF PERSONAL DATA

Kavipay does not intentionally collect or process special categories of personal data (sensitive data) including racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data (except for authentication), health data, or information about sex life or sexual orientation.

20. SOCIAL MEDIA AND PUBLIC COMMUNICATIONS

When you interact with us on social media platforms, public posts may be viewed by others. We may collect your username and public profile information. Never share sensitive account information via social media.

21. CHANGES TO THIS PRIVACY POLICY

We reserve the right to modify this Privacy Policy at any time. Material changes will be communicated via email (30 days advance notice), website banner, in-app notification, or SMS. Continued use after changes constitutes acceptance.

22. DISPUTE RESOLUTION AND COMPLAINTS

For privacy concerns, contact complaints@kavipay.io or dpo@kavipay.io. We will respond within 21 days. You may escalate to the Nigeria Data Protection Bureau (NDPB) at info@ndpb.gov.ng

23. REGULATORY COMPLIANCE AND CERTIFICATIONS

Kavipay maintains compliance with NDPR 2019, CBN Guidelines, Money Laundering Act 2022, Cybercrimes Act 2015, PCI DSS Level 1 (through partners), and other applicable regulations.

24. CONTACT INFORMATION AND DATA PROTECTION OFFICER

Data Protection Officer: dpo@kavipay.io
Privacy Inquiries: privacy@kavipay.io
Data Rights Requests: datarights@kavipay.io
Security: security@kavipay.io
Complaints: complaints@kavipay.io

PloutosLabs International Ltd (trading as Kavipay.io)
Website: https://kavipay.io
Support: support@kavipay.io

25. APPENDIX: PARTNER PRIVACY PRACTICES

Our licensed service providers maintain their own privacy policies:

- Safe Haven Microfinance Bank - CBN Licensed - https://safehavenmfb.com/privacy
- Sudo.africa - PCI DSS Compliant - https://sudo.africa/privacy
- Payscribe - PCI DSS Compliant - https://payscribe.ng/privacy
- Speedaf Logistics - NIPOST Licensed - https://speedaf.com/privacy

By using Kavipay Services, you acknowledge that you have read, understood, and agree to be bound by this Privacy Policy.

Document Version: 1.0 | Language: English | Jurisdiction: Federal Republic of Nigeria