Euniron Solutions & Technology Limited

Data Use Policy

Company: Euniron Solutions & Technology Limited **Registered Address:** 6th Parklands Road, Office Suites A10, Nairobi, Kenya **Effective Date:** February 19, 2026 **Last Updated:** February 19, 2026 **Version:** 1.0 **Contact:** privacy@eunironsolutions.co.ke

1. Introduction

This Data Use Policy ("Policy") describes how Euniron Solutions & Technology Limited ("Euniron," "we," "us," or "our") collects, uses, stores, shares, and protects personal data obtained through our services, including but not limited to our events and ticketing platform, payment processing systems, and messaging channels operated via the WhatsApp Business API.

This Policy is published in compliance with applicable data protection laws, including the Kenya Data Protection Act, 2019, the EU General Data Protection Regulation (GDPR), and Meta Platforms, Inc. ("Meta") requirements for WhatsApp Business API usage.

We are committed to protecting user privacy, processing data lawfully, and maintaining full transparency about how personal information is handled across all our services and communication channels.

2. Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person, including but not limited to names, phone numbers, email addresses, dates of birth, gender, payment information, and device identifiers.
Data Subject	An individual whose personal data is collected, stored, or processed by Euniron.
Processing	Any operation performed on personal data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure,

	dissemination, alignment, restriction, erasure, or destruction.
Data Controller	Euniron Solutions & Technology Limited, which determines the purposes and means of processing personal data.
Data Processor	A third party that processes personal data on behalf of Euniron, including but not limited to payment gateways, email service providers, and messaging platforms.
WhatsApp Business API	The application programming interface provided by Meta Platforms, Inc. for business-to-customer communication via the WhatsApp messaging platform.
Consent	A freely given, specific, informed, and unambiguous indication of the Data Subject's agreement to the processing of their personal data.

3. Scope

This Policy applies to:

- All personal data collected through our events and ticketing platform (web and mobile interfaces).
- All personal data processed through WhatsApp Business API messaging channels.
- All personal data shared with or received from third-party service providers acting as Data Processors.
- All personal data of customers, event attendees, prospective customers, website visitors, and business contacts.
- All employees, contractors, and agents of Euniron who handle personal data.

This Policy applies regardless of the country of residence of the Data Subject and covers data processed within and outside the Republic of Kenya.

4. Data We Collect

4.1 Data Collected Directly from Users

Data Category	Specific Data Points	Purpose	Collection Point
Identity Data	Full name, date of birth, gender	Account creation, ticket personalization, event entry	Purchase form, registration form

		verification, demographic analytics	
Contact Data	Email address, phone number (including WhatsApp number)	Transactional communications, ticket delivery, customer support, WhatsApp messaging	Purchase form, WhatsApp opt-in
Transaction Data	Purchase history, ticket types, quantities, payment amounts, payment references, payment method	Order processing, payment verification, refunds, financial reporting	Payment flow
Event Data	Events attended, ticket types purchased, check-in status	Service delivery, event analytics, personalized recommendations	Platform usage
Communication Data	WhatsApp messages, email correspondence, support tickets	Customer support, service delivery, dispute resolution	WhatsApp Business API, email, support portal
Preference Data	Communication preferences, language preferences, notification settings	Service personalization, communication management	Account settings

4.2 Data Collected Automatically

Data Category	Specific Data Points	Purpose
Device Data	Device type, operating system, browser type	Service optimization, security
Usage Data	Pages visited, features used, session duration	Service improvement, analytics
Log Data	IP address, access timestamps, error logs	Security monitoring, debugging

4.3 Data Received from Third Parties

Source	Data	Purpose
Payment Providers (M-Pesa / Safaricom)	Payment confirmation, transaction reference, payment status	Payment verification, receipt generation
WhatsApp / Meta	Phone number, WhatsApp profile name, message delivery status	Message delivery, customer communication

5. How We Use Personal Data

5.1 Lawful Bases for Processing

We process personal data based on the following lawful grounds:

a) Contract Performance (Article 6(1)(b) GDPR / Section 30 Kenya DPA)

- Processing ticket purchases and delivering event access.
- Sending transactional messages (purchase confirmations, e-tickets, QR codes, event reminders).
- Processing payments and refunds.

b) Consent (Article 6(1)(a) GDPR / Section 32 Kenya DPA)

- Sending marketing messages via WhatsApp, email, or SMS.
- Collecting and processing date of birth and gender for demographic analysis.
- Sharing data with third parties for marketing purposes.

c) Legitimate Interest (Article 6(1)(f) GDPR / Section 30 Kenya DPA)

- Fraud prevention and security monitoring.
- Service improvement and analytics.
- Customer support and dispute resolution.

d) Legal Obligation (Article 6(1)(c) GDPR / Section 30 Kenya DPA)

- Tax reporting and financial compliance.
- Responding to lawful government or regulatory requests.
- Compliance with anti-money laundering (AML) regulations.

5.2 Specific Uses of Personal Data

Use Case	Data Used	Lawful Basis
Process ticket purchases	Name, email, phone, payment data	Contract
Deliver e-tickets and QR codes via email and WhatsApp	Name, email, phone, purchase details	Contract
Send payment confirmations via WhatsApp	Phone, purchase details, payment reference	Contract

Send event reminders via WhatsApp	Phone, name, event details	Contract / Consent
Customer support via WhatsApp	Phone, name, message history, purchase history	Contract / Legitimate Interest
Marketing messages and promotions via WhatsApp	Phone, name, purchase history	Consent
Demographic analytics and reporting	Date of birth, gender, purchase history	Consent / Legitimate Interest
Fraud detection and prevention	Transaction data, device data, IP address	Legitimate Interest
Financial reporting and tax compliance	Transaction data, payment data	Legal Obligation

5.3 WhatsApp Business API Specific Uses

We use the WhatsApp Business API exclusively for the following purposes:

1. **Transactional Notifications**: Order confirmations, e-ticket delivery, payment receipts, and QR code delivery.
2. **Service Updates**: Event changes, venue updates, schedule modifications, and cancellation notices.
3. **Customer Support**: Responding to customer inquiries, resolving complaints, and processing refund requests.
4. **Event Reminders**: Sending reminders for upcoming events that the customer has purchased tickets for.
5. **Marketing Communications**: Promotional messages about upcoming events, exclusive offers, and loyalty rewards — **only with explicit prior opt-in consent**.

We do **NOT** use WhatsApp Business API for:

- Unsolicited commercial messages without prior consent.
- Sharing personal data with other businesses for their independent use.
- Automated decision-making that produces legal effects on Data Subjects.
- Profiling for discriminatory purposes.
- Selling or renting user data to third parties.
- Sending messages unrelated to our events and ticketing services.

---

6. Data Sharing and Third-Party Processors

6.1 Categories of Recipients

Recipient	Data Shared	Purpose	Safeguards
Meta Platforms, Inc. (WhatsApp Business API)	Phone number, message content, delivery metadata	Message delivery via WhatsApp	Meta's Data Processing Terms, EU-US Data Privacy Framework
Safaricom PLC (M-Pesa)	Phone number, transaction amount	Payment processing	Safaricom's data protection policies, CBK regulations
MailerSend (Email provider)	Email address, name, ticket details	Email delivery (confirmations, e-tickets)	Data Processing Agreement, GDPR compliance
DigitalOcean, Inc. (Cloud hosting)	All platform data (encrypted at rest)	Infrastructure and hosting	SOC 2 Type II certified, Data Processing Agreement
Event Organizers	Attendee name, ticket type, check-in status	Event management and access control	Data sharing agreement, limited to event-specific data

6.2 Data Sharing Principles

- We share only the minimum data necessary for each purpose (**data minimization**).
- All third-party processors are bound by Data Processing Agreements (DPAs) that require equivalent data protection standards.
- We do **not** sell, rent, license, or trade personal data to any third party.
- We do **not** share personal data with third parties for their own marketing purposes without explicit Data Subject consent.
- Cross-border data transfers are conducted in compliance with applicable data protection laws, using Standard Contractual Clauses (SCCs) or equivalent mechanisms where required.

6.3 Cross-Border Data Transfers

Personal data may be transferred to and processed in countries outside Kenya, including:

- **United States**: Meta Platforms (WhatsApp), DigitalOcean infrastructure.
- **European Union**: DigitalOcean Frankfurt data center (primary hosting).

All cross-border transfers are protected by:

- Standard Contractual Clauses (SCCs) approved by the European Commission.

- Adequacy decisions where applicable.
- Data Processing Agreements with all recipients.
- Encryption in transit (TLS 1.2+) and at rest (AES-256).

---

7. Data Retention

7.1 Retention Schedule

Data Category	Retention Period	Justification
Purchase and transaction data	7 years from transaction date	Tax and financial compliance (Kenya Income Tax Act, Companies Act)
User identity and contact data	Duration of active relationship + 3 years	Contract performance and legitimate interest in re-engagement
WhatsApp message history	90 days from message date	Customer support and dispute resolution
Payment references and receipts	7 years from transaction date	Financial audit and regulatory compliance
Marketing consent records	Duration of consent + 3 years	Proof of consent for regulatory purposes
Event attendance records	3 years from event date	Analytics, loyalty programs, and dispute resolution
Log and security data	12 months from generation	Security monitoring and incident investigation
Inactive account data	Deleted after 24 months of inactivity	Data minimization principle

7.2 Retention Principles

- Data is retained only for as long as necessary to fulfill the purposes described in this Policy.
- Upon expiration of the retention period, data is securely deleted or anonymized.
- Data Subjects may request earlier deletion subject to applicable legal retention obligations.
- Backup copies are purged within 30 days of primary data deletion.

---

8. Data Security

8.1 Technical Measures

Measure	Implementation
Encryption in Transit	TLS 1.2+ enforced on all API endpoints, HTTPS-only access
Encryption at Rest	AES-256 encryption for database storage
Access Control	Role-based access control (RBAC) for all systems; principle of least privilege enforced
Network Security	Private VPC network for inter-service communication; public access limited to API Gateway only
Firewall	UFW-based firewall rules; service ports bound to VPC interfaces only
Authentication	JWT-based API authentication; SSH key-only access for infrastructure
Monitoring	Real-time log monitoring; automated alerts for suspicious activity
Vulnerability Management	Regular dependency updates; container-based isolation for all services

8.2 Organizational Measures

- All employees and contractors with data access undergo data protection training.
- Data protection impact assessments (DPIAs) are conducted for new processing activities.
- Incident response procedures are documented and tested annually.
- Access to personal data is logged and auditable.
- Third-party processors are assessed for security compliance before engagement.
- Non-disclosure agreements (NDAs) are executed with all personnel handling personal data.

8.3 Incident Response

In the event of a personal data breach:

1. The breach is contained and assessed within **24 hours** of discovery.
2. The Office of the Data Protection Commissioner (Kenya) is notified within **72 hours** where required by law.
3. Affected Data Subjects are notified **without undue delay** if the breach is likely to result in a high risk to their rights and freedoms.

4. Remedial measures are implemented and documented.
5. A post-incident review is conducted to prevent recurrence.

---

9. Data Subject Rights

Under applicable data protection laws, Data Subjects have the following rights:

Right	Description	How to Exercise
Right of Access	Obtain confirmation of whether personal data is being processed and request a copy of such data.	Email privacy@euniron solutions.co.ke
Right to Rectification	Request correction of inaccurate or incomplete personal data.	Email or WhatsApp support
Right to Erasure	Request deletion of personal data where there is no compelling reason for continued processing.	Email privacy@euniron solutions.co.ke
Right to Restrict Processing	Request limitation of processing in specific circumstances.	Email privacy@euniron solutions.co.ke
Right to Data Portability	Receive personal data in a structured, commonly used, machine-readable format.	Email privacy@euniron solutions.co.ke
Right to Object	Object to processing based on legitimate interest or direct marketing.	Email, WhatsApp, or unsubscribe link
Right to Withdraw Consent	Withdraw previously given consent at any time without affecting the lawfulness of prior processing.	Email, WhatsApp, or account settings
Right to Lodge a Complaint	Lodge a complaint with the Office of the Data Protection Commissioner, Kenya, or the relevant supervisory authority.	ODPC Kenya: complaints@odpc.go.ke

9.1 Exercising Your Rights

- Requests are acknowledged within **3 business days**.
- Requests are fulfilled within **30 calendar days** of receipt, unless an extension is justified.
- Identity verification may be required before processing a request.

- There is no fee for exercising data subject rights, unless requests are manifestly unfounded or excessive.

9.2 WhatsApp-Specific Opt-Out

Users may opt out of WhatsApp communications at any time by:

- Sending "STOP" to our WhatsApp Business number.
- Updating communication preferences in their account settings.
- Contacting privacy@eunironsolutions.co.ke.

Opt-out from marketing messages does not affect transactional messages related to active purchases or ongoing services.

---

10. Consent Management

10.1 How We Obtain Consent

- **Explicit opt-in** is required before sending marketing messages via WhatsApp or email.
- Consent is collected through clear, affirmative action (e.g., checking an unchecked box, clicking "I agree," or sending a specific keyword via WhatsApp).
- Pre-checked boxes or implied consent mechanisms are **not** used.
- Consent requests are presented in clear, plain language separate from other terms and conditions.

10.2 Consent Records

We maintain records of all consents, including:

- The identity of the Data Subject.
- The date and time consent was given.
- The method by which consent was given.
- The specific purposes for which consent was granted.
- Any subsequent withdrawal of consent.

10.3 Withdrawal of Consent

- Consent may be withdrawn at any time through the methods described in Section 9.2.
- Withdrawal of consent is processed within **48 hours**.
- Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

11. Children's Data

- Our services are not directed at individuals under the age of **18 years**.
- We do not knowingly collect personal data from children under 18.
- If we become aware that we have collected personal data from a child under 18, we will take immediate steps to delete such data.
- Event organizers are responsible for ensuring age-appropriate access to their events.

12. Cookies and Tracking

- Our web platform uses essential cookies required for service functionality (session management, authentication).
- Analytics cookies are used only with explicit user consent.
- We do not use tracking cookies for behavioral advertising.
- Users can manage cookie preferences through their browser settings or our cookie consent banner.
- A separate Cookie Policy is available on our website.

13. Automated Decision-Making

- We do not engage in solely automated decision-making that produces legal effects or similarly significant effects on Data Subjects.
- Customer tier classifications (for loyalty programs) are based on transaction history and are used solely for internal segmentation and service personalization.
- Data Subjects have the right to request human intervention in any automated processing that affects them.

14. Changes to This Policy

- We reserve the right to update this Policy to reflect changes in our practices, technology, legal requirements, or other factors.

- Material changes will be communicated to users via email and/or WhatsApp notification at least **14 days** before taking effect.
- The "Last Updated" date at the top of this Policy will be revised accordingly.
- Continued use of our services after the effective date of changes constitutes acceptance of the revised Policy.
- Previous versions of this Policy are available upon request.

---

15. Governing Law and Jurisdiction

- This Policy is governed by and construed in accordance with the laws of the Republic of Kenya.
- The Kenya Data Protection Act, 2019 and its subsidiary legislation apply to all processing activities described herein.
- For Data Subjects in the European Economic Area, the GDPR applies in addition to Kenyan law.
- Disputes arising under this Policy shall be subject to the exclusive jurisdiction of the courts of Nairobi, Kenya, unless applicable law requires otherwise.

---

16. Data Protection Officer

For questions, concerns, or requests related to this Policy or our data practices, contact:

Data Protection Officer Euniron Solutions & Technology Limited 6th Parklands Road, Office Suites A10 Nairobi, Kenya

Email: privacy@eunironsolutions.co.ke **WhatsApp:** Available on our business profile **Response Time:** Within 3 business days

---

17. Regulatory Registration

Euniron Solutions & Technology Limited is registered with the Office of the Data Protection Commissioner (ODPC), Kenya, in accordance with Section 18 of the Data Protection Act, 2019.

This document constitutes the official Data Use Policy of Euniron Solutions & Technology Limited. By using our services, you acknowledge that you have read, understood, and agreed to the terms of this Policy.

Euniron Solutions & Technology Limited 6th Parklands Road, Office Suites A10, Nairobi, Kenya

---

Document Reference: ESTL-DUP-2026-001 Classification: Public