

WALLENJE

PRIVACY POLICY

Wallets & Vaults Ltd

Effective Date: 3 September 2026

Last Updated: 3 September 2026

This Privacy Policy explains how Wallets & Vaults Ltd (“Wallets & Vaults”, “we”, “us”, or “our”) collects, uses, stores, discloses and protects personal data when you use Wallenje, including the Wallenje mobile application, website, related services and support channels (collectively, the “Services”).

1. Who We Are

Wallenje is a virtual asset wallet and custody platform operated by Wallets & Vaults Ltd, a Kenyan-owned company. For purposes of applicable data protection law, Wallets & Vaults may act as a data controller for personal data it determines the purposes and means of processing, and may use data processors to provide specific services on its behalf.

Company: Wallets & Vaults Ltd

Product: Wallenje

Country: Kenya

Privacy contact: privacy@walletsandvaults.com

Registered/Business Address: Karen, Nairobi, Kenya

Data Protection Officer/Privacy Contact: Chief Executive Officer (CEO)

2. Scope of This Policy

This Policy applies to personal data collected through the Wallenje application, website, account and wallet registration processes, identity and compliance processes, transactions, customer support, communications, security systems and other interactions with the Services.

This Policy does not govern third-party websites, applications, blockchain networks, exchanges, payment providers or other services that have their own privacy policies. Transactions recorded on public blockchains may remain publicly accessible and may not be capable of being altered or deleted by us.

3. Personal Data We May Collect

Depending on how you use the Services, we may collect the following categories of information:

- **Account and contact information:** name, email address, telephone number, username, account identifiers and communication preferences.
- **Identity and KYC information:** information needed to verify identity or meet legal and regulatory requirements, which may include identification details, date of birth, nationality/residency information, verification results and information reasonably required for customer due diligence.
- **Financial and transaction information:** wallet addresses, transaction history, asset and transaction details, payment-related information, transaction status, fees and information required to detect suspicious or unauthorized activity.

- **Device and technical information:** device model, operating system, application version, IP address, device identifiers, network information, crash information, diagnostic information and security-related logs.
- **Usage information:** features used, pages or screens viewed, session information, preferences and interactions with the Services.
- **Support and communications:** messages, requests, feedback and information you provide when contacting customer support.
- **Compliance and risk information:** information used to satisfy applicable AML/CFT, sanctions, fraud prevention, risk management, legal and regulatory obligations.
- **Information received from third parties:** information from identity-verification providers, fraud-prevention providers, blockchain analytics providers, payment or infrastructure providers, regulators or other lawful sources.

4. Information We Do Not Intentionally Collect

Wallenje is not designed to request your wallet recovery phrase, private key or other secret authentication material through customer support. You should never disclose such information to us or to anyone claiming to represent Wallenje. Where a service does not require us to possess such information, we do not intentionally collect it.

5. How We Use Personal Data

- Create, maintain and administer Wallenje accounts and wallets.
- Provide wallet, custody, transfer, buy, sell and other enabled Services.
- Authenticate users and protect accounts and transactions against unauthorized access.
- Perform identity verification and customer due diligence.
- Prevent, detect and investigate fraud, money laundering, terrorist financing, sanctions violations and other unlawful activity.
- Monitor transactions and manage financial, operational and security risks.
- Process and reconcile transactions, fees and related records.
- Provide customer support and respond to enquiries.
- Maintain, secure, troubleshoot and improve the Services.
- Send service, security, compliance and administrative communications.
- Meet legal, regulatory, court, law-enforcement and governmental requirements.
- Establish, exercise or defend legal claims and protect our rights, users and property.
- Conduct analytics and service improvement using appropriate safeguards and, where practical, aggregated or de-identified information.

6. Legal Bases for Processing

We process personal data only where permitted by applicable law. Depending on the circumstances, the legal basis may include consent; performance of a contract or steps requested before entering into a contract; compliance with a legal or regulatory obligation; protection of vital or legitimate interests; or another lawful basis recognized by applicable data protection law.

Where processing is based on consent, you may withdraw consent where permitted by law. Withdrawal does not affect processing that occurred before withdrawal or processing that we are legally required or otherwise permitted to continue.

7. KYC, AML/CFT and Regulatory Processing

Because Wallenje may provide services involving virtual assets, we may be required to collect and retain information for customer identification, transaction monitoring, sanctions screening, fraud prevention, record-keeping and regulatory reporting. We may process additional information where necessary to comply with applicable Kenyan law and, where relevant, the requirements of regulators and competent authorities.

Regulatory requirements may require us to retain information even after an account is closed or a user requests deletion. Where a legal retention obligation applies, we will retain only what is necessary for that obligation and will securely dispose of or anonymize information when the applicable retention period ends.

8. Blockchain and Public Ledger Information

Wallenje may interact with public or permissioned blockchain networks. Blockchain transactions can contain wallet addresses, transaction amounts, timestamps, transaction identifiers and other information that may be visible to participants or publicly accessible depending on the network.

Blockchain records are generally immutable. We may not be able to delete, correct or alter information that has already been recorded on a blockchain. You should therefore consider the public and permanent nature of blockchain transactions before initiating a transaction.

9. How We Share Personal Data

We do not sell personal data as a business model. We may disclose or make personal data available where reasonably necessary and lawful, including to:

- Service providers and data processors supporting hosting, cloud infrastructure, identity verification, security, analytics, customer support, communications and other operations.
- Blockchain, transaction-monitoring and compliance service providers.
- Payment, banking or financial infrastructure providers where required to provide an enabled service.
- Professional advisers such as auditors, lawyers and consultants, subject to appropriate confidentiality obligations.
- Regulators, law-enforcement agencies, courts, government authorities or other competent bodies where required or permitted by law.
- Entities involved in a corporate transaction such as a merger, acquisition, restructuring or sale of assets, subject to applicable law and appropriate safeguards.
- Other parties where you have given a valid authorization or where disclosure is otherwise lawful.

10. International Data Transfers

Some of our service providers or infrastructure may process personal data outside Kenya. Where personal data is transferred outside Kenya, we will use appropriate safeguards and comply with applicable Kenyan data protection requirements concerning cross-border transfers, including where required obtaining consent or ensuring an adequate level of protection or other lawful transfer mechanism.

11. Data Retention

We retain personal data only for as long as reasonably necessary for the purposes described in this Policy, including to provide Services, maintain business and financial records, meet legal and regulatory obligations, resolve disputes, enforce agreements, prevent fraud and protect the security of our systems.

Retention periods vary by the type of information and the reason it was collected. Certain KYC, transaction, compliance and audit records may need to be retained for periods prescribed by applicable law. When information is no longer required, we will delete, anonymize or securely dispose of it, subject to technical and legal limitations.

12. Data Security

We use reasonable technical and organizational measures designed to protect personal data against unauthorized access, alteration, disclosure, loss, misuse or destruction. Measures may include access controls, authentication, encryption where appropriate, monitoring, logging, secure development practices, backups and staff or contractor confidentiality obligations.

No internet-connected system can be guaranteed to be completely secure. You are responsible for protecting your account credentials and device and for promptly notifying us of suspected unauthorized activity.

13. Cookies and Similar Technologies

Our website and online services may use cookies, SDKs, pixels or similar technologies to maintain functionality, remember preferences, understand usage and improve security and performance. Where required by law, we will seek consent for non-essential technologies. You may be able to manage certain cookies through your browser or device settings.

14. Your Data Protection Rights

Subject to applicable law and any lawful limitations, you may have rights including the right to be informed about the processing of your personal data; access personal data held about you; request correction of inaccurate or misleading data; request deletion or erasure where legally available; object to certain processing; request restriction of processing in applicable circumstances; request data portability where applicable; and withdraw consent where processing is based on consent.

These rights are not absolute. For example, we may need to retain or process information to comply with legal, regulatory, fraud-prevention, dispute-resolution or record-keeping obligations.

15. How to Exercise Your Rights

To make a privacy request, contact us using the details in Section 1. We may need to verify your identity before acting on a request to protect your information from unauthorized disclosure. We will respond within the period required by applicable law.

If you believe your data protection rights have been infringed and your concern is not resolved by contacting us, you may have the right to lodge a complaint with the Office of the Data Protection Commissioner (ODPC) in Kenya or another competent supervisory authority, as applicable.

16. Children and Age Restrictions

The Services are intended for persons who are legally eligible to use the relevant financial or virtual asset services. We do not knowingly collect personal data from children where such collection is prohibited by applicable law. If you believe a child has provided personal data to us improperly, please contact us so that we can assess and take appropriate action.

17. Third-Party Services and Links

The Services may integrate with or link to third-party services. Those third parties may collect or process information under their own privacy policies. We are not responsible for the privacy practices of third parties that we do not control.

18. Automated Decision-Making and Risk Systems

We may use automated tools, rules, scoring systems or analytics to help detect fraud, security threats, sanctions risks, unusual activity or compliance concerns. Where applicable law provides rights relating to solely automated decision-making or profiling, you may contact us to exercise those rights.

19. Changes to This Privacy Policy

We may update this Policy from time to time to reflect changes to the Services, technology, legal requirements or our privacy practices. We will publish the updated version through appropriate channels and update the “Last Updated” date. Where required by law, we will provide additional notice or obtain consent.

20. Contact Us

For privacy questions, data protection requests or concerns about the handling of your personal data, contact:

Wallets & Vaults Ltd

Product: Wallenje

Email: privacy@walletsandvaults.com

Address: Karen, Nairobi, Kenya

Privacy/Data Protection Contact: Chief Executive Officer (CEO)

21. Important Legal Notice

This Privacy Policy is intended as a business-ready privacy-policy draft and should be reviewed by qualified Kenyan legal counsel and, where applicable, your data protection/compliance officer before publication. In particular, the final version should be aligned with Wallenje’s actual data flows, vendors, retention schedule, consent mechanisms, security controls, regulatory status and applicable Kenyan data protection and virtual asset requirements.