Data Protection Policy

QE-JA Real Estate Management System

Effective Date: 1 March 2026
Last Updated: 28 February 2026

1. Introduction and Commitment

Hatari Technologies Limited is deeply committed to protecting the personal data of all individuals whose information is processed through the QE-JA Real Estate Management System platform. This Data Protection Policy outlines our framework for ensuring compliance with:

- The Kenya Data Protection Act, 2019 (DPA)
- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- All other applicable data protection and privacy legislation

As a B2B platform serving property management organizations across East Africa, we recognize that we process significant volumes of personal data on behalf of our clients and their tenants. This policy demonstrates our accountability and transparency.

2. Kenya Data Protection Act (DPA) Compliance

The Kenya DPA, enacted in 2019, is the primary data protection legislation governing our operations. We comply with all provisions including:

2.1 Registration with the ODPC

We are registered with the Office of the Data Protection Commissioner (ODPC) as both a data controller and data processor, as required under Section 18 of the DPA.

2.2 Lawful Processing (Section 25)

All personal data processed through the Platform is done so on a lawful basis:

- Consent of the data subject (e.g., tenant background checks, identity verification)
- Performance of a contract (e.g., providing Platform services to subscribers)
- Compliance with a legal obligation (e.g., tax reporting, audit trails)
- Legitimate interest (e.g., fraud prevention, security)

2.3 Consent Management

For processing that requires consent (particularly tenant background checks and identity verification):

- Consent is collected digitally through DocuSeal (white-labeled as "Digital Consent")
- Consent is freely given, specific, informed, and unambiguous
- Records of consent are maintained and auditable
- Consent can be withdrawn at any time without affecting the lawfulness of prior processing

2.4 Data Subject Rights (Section 26)

We facilitate the exercise of all rights guaranteed under the Kenya DPA:

- Right to be informed about data collection and processing
- Right of access to personal data
- Right to rectification of inaccurate data
- Right to deletion of personal data
- Right to restrict processing
- Right to data portability
- Right to object to processing

2.5 Sensitive Personal Data (Section 44)

Where the Platform processes sensitive personal data (including national identification numbers for tenant verification), additional safeguards are applied:

- Explicit consent is obtained before processing
- Enhanced encryption and access controls are in place
- Processing is limited to what is strictly necessary

3. General Data Protection Regulation (GDPR) Compliance

Although primarily operating in East Africa, we comply with the GDPR to protect any EU/EEA data subjects and to maintain the highest international standards.

3.1 Data Protection Principles (Article 5)

We adhere to all GDPR data protection principles:

- Lawfulness, fairness, and transparency: Clear communication about how data is processed
- Purpose limitation: Data is collected for specified, explicit, and legitimate purposes
- Data minimization: Only data necessary for the stated purpose is collected
- Accuracy: We maintain mechanisms for data correction and updates
- Storage limitation: Data is retained only as long as necessary
- Integrity and confidentiality: Appropriate security measures protect all personal data
- Accountability: We can demonstrate compliance with all principles

3.2 Data Protection by Design and Default (Article 25)

Privacy is embedded into the Platform architecture:

- Organization-level data isolation ensures each client's data is logically separated
- Role-based access controls limit data access to authorized personnel
- AI models are designed to operate on aggregated, anonymized data where possible
- Default settings prioritize privacy (e.g., minimum data collection, secure defaults)

3.3 Data Protection Impact Assessment (Article 35)

We conduct DPIAs for high-risk processing activities including:

- AI-powered tenant risk scoring
- Qeja Tenant Network cross-property data sharing
- Identity verification through third-party services

3.4 International Data Transfers (Articles 44-49)

Where data is transferred outside Kenya or the EEA:

- Standard Contractual Clauses (SCCs) are in place with all sub-processors
- We assess the data protection laws of recipient countries
- Supplementary measures are implemented where necessary

3.5 Data Breach Notification (Articles 33-34)

In the event of a personal data breach:

- The ODPC and relevant supervisory authorities are notified within 72 hours
- Affected data subjects are notified without undue delay if the breach poses a high risk
- All breaches are documented with root cause analysis and remediation steps

4. Data Processing Activities

4.1 Platform-Level Processing (Hatari Technologies as Data Controller)

- User account management and authentication
- Platform analytics and service improvement
- Qeja Tenant Network operation
- Identity verification services

4.2 Organization-Level Processing (Hatari Technologies as Data Processor)

- Tenant personal data management on behalf of property management organizations
- Financial transaction processing (M-Pesa verification, bank reconciliation)
- Communications sent to tenants on behalf of organizations
- AI-powered analytics on organizational data

5. AI and Automated Decision-Making

The Platform uses AI for predictive analytics. Under both the Kenya DPA (Section 35) and GDPR (Article 22):

- AI predictions are advisory only and do not constitute automated decision-making with legal effects
- Human oversight is always involved in tenancy decisions
- Data subjects have the right to contest decisions influenced by AI predictions
- We provide meaningful information about the logic, significance, and consequences of AI processing
- AI models are regularly audited for fairness and bias

6. Data Security Measures

We implement comprehensive technical and organizational measures:

6.1 Technical Measures

- AES-256 encryption at rest
- TLS 1.2+ encryption in transit
- Google Cloud Platform infrastructure with SOC 2 Type II certification
- Automated vulnerability scanning and patching
- Multi-factor authentication for administrative access
- Database-level encryption and access logging

6.2 Organizational Measures

- Data protection training for all staff
- Background checks for employees with data access
- Confidentiality agreements with all personnel and contractors
- Regular security audits and penetration testing
- Incident response plan with defined roles and escalation procedures

7. Data Retention and Deletion

Our retention policy ensures data is not kept longer than necessary:

- Active subscription: Data retained for the duration of service
- Post-termination: Complete data export within 48 hours of request
- Grace period: 30 days after termination to verify exported data
- Permanent deletion: After 30 days, all data is permanently and irreversibly erased
- Deletion certificate: Available upon request confirming complete data removal
- Backup purge: All backup copies are also deleted within the same timeframe

8. Sub-Processors

We engage the following categories of sub-processors, all bound by data processing agreements:

- Cloud infrastructure: Google Cloud Platform (data hosting and processing)
- Identity verification: SmileID (tenant identity checks, white-labeled)
- Digital consent: DocuSeal (consent form collection, white-labeled)
- Communication services: Configured per-organization (Email, SMS, WhatsApp)

9. Data Protection Officer

We have appointed a Data Protection Officer who can be contacted at:

Data Protection Officer
Hatari Technologies Limited
Nairobi, Kenya
Email: info@hataritech.com

10. Complaints

If you believe your data protection rights have been violated, you have the right to:

- Contact our Data Protection Officer
- Lodge a complaint with the Office of the Data Protection Commissioner (ODPC), Kenya
- Lodge a complaint with the relevant supervisory authority under the GDPR

11. Policy Review

This Data Protection Policy is reviewed and updated at least annually, or whenever there are significant changes to our data processing activities, applicable legislation, or organizational structure.