

GLOBAL PRIVACY & DATA PROTECTION POLICY

Application: LoanVault MFI Multi-Tenant Platform | **Document ID:** LV-POL-2026-V1
Effective Date: September 3, 2026 | **Framework:** Kenya Data Protection Act 2019 (ODPC), EU GDPR, SOC 2 Trust Principles[cite: 1]

ODPC COMPLIANT GDPR ARTICLE 28 ALIGNED SOC 2 TYPE II MAPPED AES-256 STORAGE

REGULATORY STATUS UNDER DATA PRIVACY LAW: In compliance with the Kenya Data Protection Act 2019 and international privacy regulations, the **Tenant Organization** acts as the **Data Controller**, deciding why and how personal data is processed[cite: 1]. **LoanVault MFI** operates strictly as the **Data Processor**, hosting and computing system records solely upon the instructions of the Controller[cite: 1].

1. SCOPE AND CATEGORIES OF PERSONAL DATA COLLECTED

To provide credit administration, savings ledgers, and institutional management, the platform processes the following data classes:

- Identity & Demographic Records:** Full legal names, national identity/alien ID/passport numbers, residential addresses, email accounts, and verified phone numbers[cite: 1].
- Beneficiary & Estate Allocation Records:** Next of Kin designations, relationship categories, percentage benefit distributions, and emergency contact phone lines.
- Financial & Operational Ledgers:** Loan amounts requested, evaluation statuses, repayment transaction references, M-Pesa receipt IDs, savings contributions, and historical arrears ledger items[cite: 1].
- System Telemetry & Audit Logs:** Access dates, IP addresses, immutable administrative transaction audit events, and user interaction histories required for forensic accounting[cite: 1].

2. LAWFUL GROUNDS FOR PROCESSING

Processing executed through LoanVault MFI relies on the following lawful bases under statutory privacy law:

- Performance of a Contract:** Processing necessary to fulfill loan contracts, compute interest schedules, and execute ledger accounting between the member and the organization.
- Compliance with Legal Obligations:** Retention of mandatory transaction logs, audit trails, and anti-money laundering (AML) / counter-terrorist financing (CTF) verification histories.
- Explicit Consent:** Explicit opt-in authorizations provided during user onboarding, next-of-kin beneficiary submissions, or public testimonial sharing[cite: 1].

3. TECHNICAL & ORGANIZATIONAL SECURITY CONTROLS (SOC 2 ARCHITECTURE)

- Multi-Tenant Isolation:** Strict Row-Level Security (RLS) policies are enforced at the database layer. No tenant organization or affiliated user can query, inspect, or leak data across institutional boundaries[cite: 1].
- Cryptographic Protection:** In-transit communications are secured with TLS 1.3 encryption. Tenant payment secrets (e.g., M-Pesa Consumer Keys, Secrets, and Passkeys) are encrypted at rest using AES-256 via a dedicated `MPESA\_MASTER\_KEY`[cite: 1].
- Immutable Audit Trails:** Sensitive modifications—including role elevation, balance updates, and loan approvals—are committed to append-only audit tables to eliminate untraceable tampering[cite: 1].

4. SUB-PROCESSORS AND THIRD-PARTY DATA DISCLOSURES

Personal and financial records are never leased, monetized, or shared with secondary advertisers. Data transfer is restricted strictly to operational sub-processors:

- **Financial Settlement Gateways:** Safaricom Daraja M-Pesa or partner banking switches, solely to transmit payment parameters necessary to execute customer-initiated STK pushes[cite: 1].
- **Transactional Communications:** Authenticated email relays (operating under verified platform domains like `no-reply@loanvaultmfi.com`) solely to transmit payment receipts, activation links, and security alerts[cite: 1].
- **Statutory Authorities:** Regulatory bodies (ODPC, Central Bank of Kenya, law enforcement) upon receipt of an authentic, legally binding, and enforceable court warrant.

5. MANDATORY DATA BREACH PROTOCOL (72-HOUR WINDOW)

In accordance with ODPC guidelines and international data protection standards, if an unauthorized perimeter breach, leak, or malicious exfiltration impacting personal data occurs, the Platform Provider will notify affected Tenant Administrators within seventy-two (72) hours of technical verification, providing an impact assessment and corrective remediation actions.

6. DATA RETENTION, MINIMIZATION & ARCHIVING

Financial ledger lines, member loan records, and audit events are retained for the statutory financial archiving period (a minimum of 5 to 7 years) as required by financial auditing regulations. Data cannot be unilaterally deleted where an active financial liability, unsettled loan balance, or legal dispute remains open.

7. DATA SUBJECT RIGHTS & FORMAL REDRESS

Under the Kenya Data Protection Act 2019 and global privacy laws, registered members maintain enforceable rights to[cite: 1]:

- Request access to all personal data profiles maintained in the system[cite: 1].
- Demand rectification of obsolete, erroneous, or misleading records[cite: 1].
- Object to processing or withdraw consent where statutory retention obligations do not apply.

Members should lodge data requests directly with their Tenant Organization's Data Protection Officer. Escalated technical inquiries or notices may be submitted via the platform's support module or directly to `support@loanvaultmfi.com` / `loanvaultmfi@gmail.com`[cite: 1].