

DATA PROTECTION ANALYST

REPORTING TO: SENIOR DATA PROTECTION OFFICER

Job Purpose: This role is designed to strengthen the Bank's data protection function by providing technical, operational, administrative and research support while building internal capacity for compliance, risk mitigation, and audit preparedness. The role ensures that technical safeguards, access controls, and data governance measures align with the Data Protection Act, 2019 and internal security standards.

Key Responsibilities:

1. Data Protection Governance & Framework

- Support the implementation and maintenance of the Bank's Data Protection & Privacy Framework.
- Assist in maintaining records of processing activities (ROPAs) across departments.
- Support the documentation, review, and update of data protection policies, procedures, and standards.
- Assist business units in implementing privacy by design and privacy by default principles in processes and systems.
- Maintain registers relating to personal data processing activities and data inventories

2. Technical Data Protection Controls

- Assist in the implementation, configuration, and maintenance of technical data protection solutions such as Data Loss Prevention (DLP).
- Support monitoring of data access controls, privilege management, and authentication safeguards.
- Work with IT and vendors to support the management of DLP technologies and privacy-related security tools.
- Assist in identifying and reporting potential data protection control weaknesses.
- Support implementation of technical safeguards protecting personal and sensitive data.

3. Risk management & DPIAs

- Assist in conducting Data Protection Impact Assessments (DPIAs) for new systems, products, and operational changes.
- Support data mapping exercises and documentation of data flows.
- Assist in identifying privacy risks and documenting mitigation controls.
- Maintain registers of DPIAs, high-risk processing activities, and remediation actions.
- Support privacy risk assessments for projects and third-party engagements.

4. Data Subject Rights & Incidents Management

- Support the administration of data subject rights requests including access, rectification, erasure, and restriction requests.
- Assist in tracking and coordinating responses to data subject access requests (DSARs).
- Support the investigation and documentation of personal data breaches and privacy incidents.
- Assist in maintaining records of personal data breaches and incident responses.
- Support escalation of incidents to the Senior Data Protection Officer where required.

5. Training, Awareness, and Culture

- Support delivery of data protection awareness initiatives and staff training programs.
- Assist in preparing internal privacy communications, newsletters, and guidance materials.
- Research emerging privacy regulations, regulatory guidance, and global data protection trends.
- Support awareness campaigns promoting responsible handling of personal data.
- Provide operational support to business units on data protection queries.

6. Monitoring, Reporting and Assurance

- Support monitoring of compliance with privacy policies, consent requirements, and retention schedules.
- Assist in preparing reports and dashboards on the Bank's data protection posture.
- Support internal audits, regulatory reviews, and compliance assessments.
- Assist in conducting vendor privacy assessments and monitoring third-party data protection obligations.
- Track remediation of identified privacy risks and control gaps.

Academic & Professional Qualifications

- Bachelor's degree in information technology, Computer Science, Information Security, Network Security, Business Information Systems, or related field.
- Certification or training in Data Protection or Privacy (e.g., CIPM, CIPT, ISO Privacy modules).
- Information security certifications such as CISSP, CISM, Network+, CCNP, or equivalent (added advantage).

Experience Requirements

- Minimum 2–4 years' experience in data protection, information security, IT risk, compliance, or data governance roles.
- Experience supporting Data Loss Prevention (DLP) or related information security technologies.
- Experience supporting information security compliance and data governance processes.
- Exposure to banking systems, digital banking platforms, or regulated financial services environments is an added advantage.
- Experience supporting audits, compliance assessments, or risk reviews.

Technical Competencies

- Data Protection & Privacy Governance
- Privacy Risk Assessment & DPIAs
- Data-Breach & Incident Management
- Digital Banking & Data-Driven Technology Risk
- Third-Party & Cross-Border Data Risk
- Information Security & Privacy Controls
- Data Governance & Records Management

ALL applicants **MUST** apply online to email: recruitment@familybank.co.ke; closing date is **30th October 2026**. Canvassing will automatically disqualify the candidate. Only shortlisted candidates will be contacted.

"We are an equal opportunity employer"