

Data Protection Compliance in Kenya and Tanzania

The Compliance Question Has Changed

Across East Africa, organisations now depend on personal data to recruit employees, serve customers, deliver public services, secure premises, process payments and run digital platforms. The information may be ordinary - names, phone numbers and identification details - or highly sensitive, including health, biometric, financial and location data.

The central question is no longer simply whether an organisation has a privacy policy. It is whether the organisation can demonstrate that its actual practices protect personal data every day.

Across East Africa, businesses and public institutions are collecting more personal data than ever before. Customer records, employee files, identification documents, mobile-money details, medical information, CCTV footage, biometric data, website analytics and digital-marketing databases have become part of everyday operations.

Yet many organisations still treat data protection as an information-technology issue, a registration exercise or a privacy notice copied from another website. That approach is no longer sufficient.

Kenya and Tanzania now have operational data-protection regimes, active regulators and formal enforcement mechanisms. Kenya's framework has been enforced for several years, while Tanzania has entered a decisive enforcement phase following the expiry of its voluntary registration period on 8th April 2026.

The central message for organisations operating in either country is clear: data-protection compliance must move from policy documents to daily business practice.

THE CORE MESSAGE
Compliance must move from policy documents to daily business practice.

WHO IS AFFECTED

- Employers and recruitment teams
- Schools, clinics and professional firms
- Hotels, retailers and loyalty programmes
- Financial institutions and mobile-money businesses
- Property managers, logistics companies and security providers
- Non-profits, churches, associations and public bodies

CONTROLLER, PROCESSOR - OR BOTH?

An organisation may determine why and how data is used, process information for another party, or perform both roles. The legal obligations and registration position should be assessed for each activity.

EXECUTIVE TAKEAWAY

A registration certificate is not a compliance programme. Regulators and courts increasingly expect evidence that lawful processing, security, accountability and individual rights are embedded in everyday operations.

Two Countries, One Operating Discipline



DAUD AND MATTHYSE ADVOCATES

The legal architecture and the organisations caught by it

Issue	Kenya	Tanzania
Principal law	Data Protection Act, 2019	Personal Data Protection Act, 2022
Regulator	Office of the Data Protection Commissioner (ODPC)	Personal Data Protection Commission (PDPC)
Registration	Thresholds and mandatory categories apply	Registration before collection or processing, subject to statutory scope
Cross-border transfers	Lawful transfer mechanisms and safeguards	PDPC permit framework and applicable safeguards
Enforcement	Complaints, determinations, notices, penalties and audits	Registration, complaints, permits and enforcement

Kenya

The Data Protection Act, 2019 is supported by regulations on general processing, registration, complaints and enforcement. The ODPC oversees compliance.

Tanzania

The Personal Data Protection Act, 2022 came into force on 1st May 2023. The Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 provide further operational requirements.

Territorial scope

The Tanzanian Act applies to Mainland Tanzania and Zanzibar, but does not apply to non-Union matters in Zanzibar. Organisations operating there should assess the scope relevant to their activities.

Controller, processor - or both?

A controller determines why and how personal data is processed. A processor handles personal data on behalf of a controller. Assess each activity: an organisation may perform both roles.

Registration and Enforcement

Country-specific requirements and practical consequences

KENYA: REGISTRATION AND RENEWAL

The small-entity registration exemption generally requires both annual turnover or revenue below KES 5 million and fewer than ten employees. Mandatory processing categories remain registrable regardless of those thresholds.

An organisation acting as both controller and processor must submit separate applications for the two roles where registration is required. Certificates are valid for 24 months unless cancelled; renewal should be sought at least 30 days before expiry.

ENFORCEMENT IN PRACTICE

In its publication of 20th November 2024, the ODPC reported 7,223 registered data handlers, 138 DPIAs reviewed, 192 advisories, 58 audits and inspections, 68 determinations, 68 enforcement notices and 11 penalty notices. These are historical figures, not October 2026 totals.

Administrative penalties may reach KES 5 million or, for an undertaking, one per cent of its preceding financial year's annual turnover, whichever is lower. Enforcement orders, compensation claims and, for relevant offences, criminal consequences may also arise.

TANZANIA: THE GRACE PERIOD HAS ENDED

The Act prohibits collection or processing without registration as a controller or processor, subject to its scope and applicable exemptions. The PDPC's notice dated 26th March 2026, confirmed that the voluntary registration period would end on 8th April 2026.

Organisations should complete the PDPC registration process, identify their controller and processor roles, appoint the required data protection officer and maintain the supporting information required by the Commission.

CROSS-BORDER TRANSFERS

Tanzania operates a permit framework for transfers abroad. Regulation 20 provides for a written application before transfer; approval and conditions are addressed in regulations 20-22. Assess the applicable requirements before using overseas cloud storage, payroll platforms or group databases.

Ask where data is stored, which entity receives or accesses it, what legal basis and safeguards apply, and which permits are needed. An overseas email or cloud service can involve an international transfer even when no employee manually sends a file abroad.

From Legal Requirements to Regulatory Scrutiny

Published Regulatory Activity and What it Means for Organisations

Data-protection regulation involves more than registration. Published regulator figures record complaints, formal decisions, enforcement notices and other outcomes. Organisations should understand these different measures and maintain records that explain how their processing decisions comply with the law.

Kenya: Enforcement at a Glance

ODPC cases recorded up to 31st May 2025

Measure	Reported figure
Complaints registered	7,611
Determinations	247
Enforcement notices	112
Penalty notices	19
Compensation orders	134
Complaints resolved through alternative dispute resolution	52

Source: ODPC Data Bulletin, 15th Edition; cases recorded up to 31st May 2025.

Tanzania: Published Regulatory Activity

PDPC website figures labelled August 2026

Measure	Reported figure
Registered organisations	15,146
Complaints received	445
Data-transfer permits reported	121
Determinations	6

Source: Tanzania PDPC, Impact in Numbers

- Source: PDPC, “Impact in Numbers”, accessed 23rd October 2026. The website describes the permit measure as “Data Transfer Permits Offered.”
- These are dated published figures, not live totals. The Kenya and Tanzania figures cover different reporting periods and categories and should not be used to compare enforcement intensity.

What the Figures Mean

A complaint is an allegation requiring assessment; it does not, by itself, establish a violation. Determinations, enforcement notices, penalty notices and compensation orders represent different types of regulatory action. They should not be added together as though each represents a separate organisation or case.

The practical lesson is that organisations need to explain their decisions and produce supporting records when questions arise.

What Organisations Should Be Ready to Produce

A practical accountability file should bring together:

- Processing records: What personal data is held, why it is needed, the applicable lawful basis and who is responsible.
- Risk assessments: DPIAs where required, identified risks and evidence that agreed safeguards were implemented.
- Supplier and transfer records: Due-diligence findings, contracts, recipients, destinations and applicable permits or safeguards.
- Incident and request records: What happened, when the organisation became aware, decisions taken, responses issued and reasons for any notification decision.
- Governance evidence: Assigned responsibilities, staff training, management review and progress on corrective actions.

Where Compliance Most Often Breaks Down



DAUD AND MATTHYSE ADVOCATES

Although awareness is growing, compliance often remains incomplete. The most common shortcomings are not limited to sophisticated cyberattacks. They arise from ordinary business practices.

1. REGISTRATION IS NOT COMPLIANCE

Registration is important, but a certificate does not prove that every processing activity is lawful.

An organisation may be registered and still violate the law by collecting excessive information, using data for an undisclosed purpose, retaining records indefinitely, ignoring access requests or sharing information with an unsecured vendor.

Registration should be the product of a wider data-governance programme—not a substitute for one.

2. DOCUMENT THE LAWFUL BASIS

Organisations frequently assume that consent is required for everything or, conversely, that possessing information automatically gives them permission to use it.

Before collecting data, an organisation should document the legal basis for each purpose. Depending on the applicable law and circumstances, the basis may include consent, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a public task or a legitimate interest.

Consent must be informed, specific and freely given. It should not be hidden in lengthy terms and conditions or bundled with unrelated activities. Individuals must also be able to withdraw consent where processing relies on it.

3. PRIVACY NOTICES MUST MATCH REALITY

Statements such as “we value your privacy” do not explain what an organisation actually does with personal information.

A proper privacy notice should identify the organisation, the categories of information collected, purposes and legal bases, recipients, retention periods, international transfers, security arrangements, individual rights and the channel for questions or complaints.

The notice must match actual operations. Publishing a polished privacy policy while staff follow entirely different practices creates additional risk.

4. COLLECT ONLY WHAT IS NECESSARY

Some organisations collect national identification numbers, dates of birth, family details, photographs or location data merely because a form has space for them.

Every field should be justified. If the organisation cannot explain why a particular item is necessary, it should not collect it.

Data minimisation lowers regulatory exposure and reduces the potential harm caused by a breach.

5. RETENTION REQUIRES A SCHEDULE

“Keep everything in case it becomes useful” is not a lawful retention strategy. Organisations should establish retention periods for employee records, unsuccessful job applications, customer files, CCTV footage, financial information, visitor logs, marketing databases and archived correspondence. At the end of the relevant period, data should be securely deleted, destroyed or anonymised unless a valid legal reason requires continued retention.

6. CONTROL VENDORS AND PROCESSORS

Payroll companies, cloud providers, software vendors, marketing agencies, call centres, security firms and outsourced human-resource providers may all process personal data. The organisation that appoints a supplier cannot simply transfer its responsibilities to that supplier.

Contracts should define permitted processing, confidentiality, security requirements, assistance with individual requests, breach reporting, use of subcontractors, international transfers and deletion or return of information when the relationship ends.

Supplier due diligence should occur before data is shared—not after an incident.

7. IDENTIFY INTERNATIONAL TRANSFERS

Many organisations transfer data internationally without recognising it. Using an overseas email service, cloud platform or customer-management system can constitute a cross-border transfer.

Kenyan organisations must assess whether an appropriate legal basis and safeguards exist for a transfer. Before transferring personal data outside Tanzania, organisations must comply with the PDPC transfer-permit framework and obtain the required permit, alongside the applicable safeguards.

The location of every important vendor’s servers should therefore form part of procurement and compliance reviews.

8. PREPARE FOR BREACHES BEFORE THEY OCCUR

A data breach is not limited to hacking. It may include sending an email attachment to the wrong person, losing an unencrypted laptop, publishing personal information online, exposing a database, allowing excessive employee access or disposing of documents insecurely.

In Kenya, a controller must notify the ODPC without delay and within 72 hours where unauthorised access or acquisition creates a real risk of harm to the affected person. A processor must notify the controller without delay and, where reasonably practicable, within 48 hours. Notification to affected individuals is subject to statutory requirements and exceptions.

Organisations should not wait for an incident before deciding who will investigate, contain, document and report it.

9. RECOGNISE AND MANAGE INDIVIDUAL RIGHTS

Individuals may have rights to receive information about processing, access their personal data, correct inaccurate information, object to certain processing and request deletion or restriction in appropriate circumstances.

These requests may arrive through reception staff, social media, email or a call centre. If employees do not recognise them, statutory response periods can expire before the request reaches the appropriate person.

10. ASSESS HIGH-RISK PROCESSING EARLY

A Data Protection Impact Assessment, or DPIA, helps an organisation identify privacy risks before introducing high-risk processing.

In Tanzania, under regulation 33, an assessment must be conducted before processing where the statutory trigger is met, including large-scale public monitoring or processing sensitive personal data concerning children or vulnerable groups.

In Kenya, a DPIA is required where processing is likely to create a high risk to individuals’ rights and freedoms. The assessment should happen before deployment, not after a system has already caused harm.

How Daud and Matthyse Advocates Can Help



DAUD AND MATTHYSE ADVOCATES

We help organisations in Kenya and Tanzania move from risk and uncertainty to lawful, sustainable and defensible data-protection practices. Our support is practical, tailored to your sector and scaled to your operations, so you can protect people's data and your organisation's reputation. We start by understanding how your data flows, what risks exist and what the law requires. We help you build the policies, processes and controls that turn legal requirements into day-to-day practice. We ensure compliance becomes part of how your organisation is governed, measured and improved.

 1. ASSESS	 2. BUILD	 3. EMBED
Data-processing reviews: Assess how personal data is collected, used, shared and stored. Controller and processor roles: Clarify roles, document responsibilities and accountability. Lawful bases assessment: Match each processing activity to a valid lawful basis and document it. Data mapping: Create clear maps of data flows, systems, third parties and cross-border transfers. Registration support: Guide registration with the ODPC in Kenya and, where applicable, with PDPC in Tanzania. DPO guidance: Define the DPO's mandate, resourcing, independence and reporting lines. Permits and authorisations: Assist with PDPC transfer-permit applications and assess any additional approvals required for the proposed processing. International transfers: Assess safeguards, contracts and permits for transfers outside Kenya or Tanzania.	Privacy notices: Draft clear, role-appropriate notices for customers, staff and other individuals. Retention schedules: Design and implement retention rules aligned to legal and business needs. Vendor and processor controls: Draft and negotiate data-processing agreements and set due-diligence standards. Breach response and compliance workflows: Establish practical processes for breach notification and handling access, correction, deletion and restriction requests. Staff training and awareness: Deliver tailored training for all roles, including leadership. Security controls (risk-based): Advise on technical and organisational safeguards and coordinate implementation with your IT and security teams.	Internal audits and gap assessments: Test what is in place and identify what needs strengthening. Board and management reporting: Provide clear dashboards and insight for informed oversight. Evidence of accountability: Organise records, policies and decisions to demonstrate compliance to regulators.

OUR 90-DAY IMPLEMENTATION ROADMAP

DAYS 1–30: STABILISE	DAYS 31–60: BUILD	DAYS 61–90: EMBED
• Kick-off and stakeholder alignment • Data processing review and risk assessment • Quick wins and immediate risk mitigation • Foundational policies and notices draft • Prioritised action plan agreed	• Implement policies, procedures, and workflows • Vendor contracts and due diligence • Staff training rollout • Permits, registrations and transfer safeguards • Security controls strengthened	• Internal audit and testing • Board reporting and metrics • Evidence and records organised • Continuous improvement plan in place • Compliance embedded in business-as-usual



Turn compliance from a document into demonstrable daily accountability.

Daud and Matthyse Advocates stands with you to protect individuals, strengthen trust and build resilient organisations in Kenya and Tanzania.

info@dandmadvocates.com

+254 702 097339 | +254 704 999333

LEGAL DISCLAIMER

This report provides general information on data protection and regulatory compliance in Kenya and Tanzania. It is not intended to constitute, and should not be relied upon as, legal advice.

For advice on your specific circumstances, please consult Daud and Matthyse Advocates.