



LEGAL TAKE

— AI & DATA PRIVACY · GUIDE

# Data Privacy and AI: What Kenyan Businesses Need to Know

OCTOBER 2026

YOUR CONTACT

Fidel Mwaki

MANAGING PARTNER

ADVOCATES · COMMISSIONERS FOR OATHS · NOTARY PUBLIC

Kenya now has a mature data protection regime and an active regulator. As businesses adopt AI tools, the same rules apply to the personal data those tools use. The question for boards is no longer whether the law applies, but whether the business can show it complies.

#### KEY POINTS

- Most businesses handling personal data must register with the Data Commissioner.
- Breaches must be reported within 72 hours of becoming aware of them.
- AI tools are covered by the same rules: lawful basis, transparency and human review.

## The rules in brief

**The Data Protection Act, 2019** sets out how personal data must be collected, used, stored and shared, and gives individuals enforceable rights.

**Registration.** Data controllers and processors above the thresholds in the 2021 Registration Regulations must register with the Office of the Data Protection Commissioner (ODPC), and renew.

**Lawful basis and purpose.** Every use of personal data needs a lawful basis, such as consent, contract or legal obligation, and must stay within the purpose for which it was collected.

**Individuals' rights.** People can ask to see, correct or delete their data, and object to certain processing, including decisions made solely by automated means.

**Enforcement.** The ODPC can issue enforcement notices and fines of up to KES 5 million or 1% of annual turnover, whichever is lower, and individuals can claim compensation.

## Moving data across borders

Transfers outside Kenya are allowed where there are appropriate safeguards, such as adequate protection in the destination country, contractual protections, or the individual's consent. Certain

processing of sensitive and public-interest data may need to stay in Kenya. Cloud and SaaS contracts should say where data is held and who can access it.

For businesses trading across the continent, the AfCFTA Protocol on Digital Trade, adopted in February 2024, points towards closer alignment of data rules across Africa over time.

## Using AI responsibly

Kenya launched its National AI Strategy in March 2025. There is no standalone AI statute yet, so the Data Protection Act is the main legal framework for AI that uses personal data. In practice:

**Know what data goes in.** Staff should not paste client or employee personal data into public AI tools without a lawful basis and an approved tool.

---

**Assess high-risk uses.** A Data Protection Impact Assessment is required where processing is likely to pose a high risk, which includes many AI uses such as profiling or screening.

---

**Keep a human in the loop.** Decisions with legal or similar effects on people, such as hiring or credit, should not rest on automated processing alone.

---

**Check your vendors.** AI providers that handle your data are processors. Your contract should cover security, confidentiality, location and use of data for training.

---

**Be transparent.** Tell people when AI is used in decisions about them.

---

## Kenya's draft AI policy

The draft Kenya Artificial Intelligence and Other Emerging Technologies Policy, 2026 sets out a risk-based approach: the higher the risk an AI system poses, the stronger the safeguards. It proposes a National AI Council, an AI Office and a Kenya AI Safety Institute, with binding rules to follow in a dedicated law. Until then, the Data Protection Act remains the main legal framework for AI that uses personal data.

Businesses deploying AI in decisions about people, such as hiring, lending or pricing, should expect requirements on human oversight, documentation and a route to challenge decisions.

# Compliance checklist

| AREA               | WHAT GOOD LOOKS LIKE                                                                     |
|--------------------|------------------------------------------------------------------------------------------|
| Registration       | Registered with the ODPC as controller or processor, and renewed on time.                |
| Records            | A map of the personal data you hold, why, where and for how long.                        |
| Notices            | Clear privacy notices for customers, staff and website visitors.                         |
| Contracts          | Data processing terms with vendors, including AI and cloud providers.                    |
| AI policy          | An approved list of tools and rules on what data can be used with them.                  |
| Impact assessments | DPIAs completed for high-risk processing, including AI.                                  |
| Breach plan        | A tested plan to notify the ODPC within 72 hours and, where needed, the people affected. |
| Training           | Regular training for staff who handle personal data.                                     |

## Building a programme that works

The gap we see most often is not awareness but ownership: staff know data matters, but not who decides. A practical programme takes about six months:

| WHEN          | FOCUS    | RESULT                                                                    |
|---------------|----------|---------------------------------------------------------------------------|
| Weeks 1 to 2  | Mobilise | Owners appointed, interim rules on AI tools and CCTV issued               |
| Weeks 2 to 6  | Map      | Registers of personal data, AI tools, CCTV and vendors; gaps identified   |
| Weeks 4 to 8  | Draft    | Policies, procedures, data-sharing terms and approval forms               |
| Months 2 to 3 | Launch   | Data protection officer appointed, policies approved, role-based training |
| Months 3 to 5 | Embed    | Retention, access, vendor and CCTV controls in daily use                  |
| Month 6       | Test     | Controls sampled, a breach exercise run and gaps closed                   |

Training works best by role. Finance teams need to protect bank details and verify payments; HR handles medical data, background checks and monitoring; marketing needs consent for leads and campaigns; property and customer teams share data with contractors and managers every day.

## What is at stake

Beyond fines, the ODPC publishes its determinations, and complaints from customers and employees are rising. A data incident also affects contracts, lender and investor due diligence, and reputation. Most issues we see are avoidable with basic governance put in place early.

### COMMON GAPS WE SEE

- Registration lapsed or never completed.
- Staff using public AI tools with client data.
- No data processing terms with key vendors.
- No breach plan, so the 72-hour window is missed.
- CCTV footage shared without a documented request and approval.

### TALK TO US

Every situation is different. This is where we get specific to yours.

**Fidel Mwaki**  
MANAGING PARTNER

[consult@fmcadvocates.com](mailto:consult@fmcadvocates.com)

+254 725 762 784

Kalson Towers, 1st Floor, Right Wing

The Crescent, off Parklands Road

Westlands, Nairobi, Kenya

[fmcadvocates.com](http://fmcadvocates.com)



### LEGAL TAKE BY FMC ADVOCATES

*This publication is general information, not legal advice on your circumstances. The law may change after publication, so please speak to us before acting.* © 2026 FMC Advocates LLP