DPO & COMPLIANCE

Do You Need a Data Protection Officer in Kenya?

By Muchangi Patrick, Advocate of the High Court of Kenya

Every business that touches personal data in Kenya sits somewhere on a spectrum: from "we should probably tidy this up" to "we are one complaint away from an ODPC enforcement notice." Where a Data Protection Officer (DPO) fits into that depends on what you process, at what scale, and who you process it for.

What the law actually requires

The Data Protection Act, 2019 requires certain data controllers and processors to designate a DPO — broadly, where the core activities involve regular and systematic monitoring of data subjects on a large scale, or large-scale processing of sensitive personal data such as health, biometric, or financial information. Public bodies generally fall within this requirement as well.

If none of that describes your business, the Act does not force your hand. But "not legally required" and "not a good idea" are different questions.

When it's worth appointing one anyway

- **You hold customer financial or health data** — fintech, digital lending, insurance, and health-tech businesses attract more scrutiny, and a named DPO gives regulators and partners someone to point to.
- **You're raising investment** — data protection due diligence is now routine, and a functioning DPO role signals maturity to investors and enterprise customers.
- **You've had a near-miss** — a close call with a breach, a vendor mishandling data, or a customer complaint is usually the moment compliance stops being theoretical.
- **You transfer data across borders** — outsourced processing, cloud vendors, or a parent company abroad all raise cross-border transfer questions that someone needs to own.

> A DPO doesn't have to be a full-time hire. Many growing businesses start with an outsourced or fractional DPO — someone who owns the role without sitting on payroll — and formalise it as they scale.

What the role actually does, day to day

Beyond the compliance-certificate version of the job, a working DPO monitors internal compliance, advises on data protection impact assessments for new products, acts as the contact point for the ODPC and for data subjects, and is usually the first call when something goes wrong with data — which is the scenario the role exists for in the first place.

The honest starting point

Before appointing anyone, it's worth mapping what data you actually hold, where it sits, and who can already see it. Most compliance gaps are found in that exercise, not in the eventual policy document. A short audit answers the DPO question far more reliably than reading the Act in isolation.

Not sure where your business stands?

A short conversation usually clarifies more than a long checklist.

Book a compliance consultation