

ODPC GUIDANCE NOTE

Moving personal data out of Kenya, lawfully

A new ODPC guidance note spells out exactly how cross-border data transfers must work. If your business uses a foreign cloud provider, runs multinational payroll, or works with international partners, this affects you today — not eventually.

ANALYSIS6 MIN READ DATA PROTECTION & PRIVACY

BY PATRICK MUCHANGI, FOUNDER & ADVOCATE — MUCHANGI PATRICK & CO. ADVOCATES · PUBLISHED MAY 2026

Download PDF

Cross-border data flow is routine business activity — and in Kenya, it is also a regulated one. The Office of the Data Protection Commissioner has published a comprehensive Guidance Note on Cross-Border Data Transfers, building on the Data Protection Act, 2019. Here is what it actually requires, in the order you'll need to act on it.

§1 The legal foundation

Part VI of the Data Protection Act — Sections 48 to 50 — is the entire spine of this framework. Three sections, three very different obligations.

SECTION 48

General conditions

Sets the baseline: transfer only proceeds where "appropriate safeguards" can be proven to the Data Commissioner.

SECTION 49

Sensitive data

Stricter rules apply — explicit consent becomes mandatory on top of safeguards.

SECTION 50

Data localisation

Data in the "strategic interest of the state" must stay on servers physically located in Kenya.

§2 Four lanes out of the country

Every lawful transfer takes one of four routes. Only one is currently unavailable in practice — and it's the one that sounds easiest.

Adequacy decision **NOT YET AVAILABLE**

A Data Commissioner finding that a country's protections are essentially equivalent to Kenya's. No such list has been published yet — so this route doesn't exist in practice for now.

B

Appropriate safeguards **MOST COMMON ROUTE**

Legally binding protections built into the transfer itself.

Binding Corporate Rules

Standard Contractual Clauses

Reciprocal agreements

Legally binding instruments

C

Necessity (derogations)

Narrow, situational exceptions — contract performance, public interest, legal claims, vital interests, or compelling legitimate interest that doesn't override the data subject's rights.

D

Explicit consent

The fallback route: the data subject is informed of the risks and agrees anyway. Mandatory — not optional — for sensitive personal data.

PRACTICAL READ

With adequacy decisions off the table, **almost every serious transfer today runs on Lane B** — safeguards you build and document yourself, not a status Kenya grants your destination country.

§3 Sensitive data needs both, not either

Race, health status, ethnicity, genetic and biometric data, sexual orientation, marital and family details — Section 49 stacks two requirements rather than offering a choice.



Explicit consent

Informed, specific agreement from the data subject, after disclosure of the risks involved.



Confirmed safeguards

Proof that appropriate technical and legal protections are in place at the receiving end.

§4 What compliance actually looks like


Identifying a legal basis is step one. The ODPC's guidance expects an operational layer on top of it.

§1 Data Protection Impact Assessment. Required for high-risk processing involving cross-border transfer.


§2 **Documentation & record-keeping.** Date and time, recipient's name, justification, and a description of the data — for every transfer.

§3 **Onward transfer control.** A recipient can't pass data to a third party without your prior written authorisation, and you remain liable if they do it wrong.


A written transfer agreement should cover:

 **Unlimited audit rights**


Unfettered access to verify the recipient's data protection systems.

 **Technical & organisational safeguards**

Clearly defined security measures for confidentiality, integrity and availability.

 **Liability & indemnity**

Who's responsible, and for what, if something goes wrong.

 **Data subject rights**

A clear mechanism for handling data subject requests at the recipient end.

§5 When data can't leave at all

Section 50 carves out six categories of data considered strategically important to the state — for these, at least one serving copy must stay on a server physically located in Kenya.



Civil registration & legal identity



Elections administration



Public finance systems



Protected computer systems



Early childhood & basic education



Primary & secondary healthcare

Minimum bar: **at least one serving copy** of the data must sit in a Kenyan data centre — full local processing isn't always required, but a local fallback copy is.

§6 What non-compliance costs



KES 5,000,000

MAXIMUM PENALTY FOR NON-COMPLIANT CROSS-BORDER TRANSFERS

§7 Four steps to get compliant

1

Map your data flows

Identify every point personal data leaves Kenya — SaaS tools, cloud services, international partners.

2

Assess your legal basis

For each flow, determine which of the four lanes applies, and document the justification.

3

Implement safeguards

Put Standard Contractual Clauses or Binding Corporate Rules in place where Lane B is your route.

4

Engage with the ODPC

Track the guidance as it firms up, and watch for the eventual adequacy list.

§8 The bottom line

Cross-border transfer compliance in Kenya isn't a box-ticking exercise you complete once — it's an operating discipline. Every new SaaS tool, every new international hire, every new partner integration is a fresh transfer that needs a lane, a safeguard, and a paper trail. Businesses that build this into procurement now will move faster later; those that don't will find their most ordinary vendor decisions turning into compliance reviews.

WHERE THIS GOES NEXT

The ODPC's note is guidance, not yet a finalised adequacy framework. **The list of adequate countries** — when published — will be the single biggest change to how this works. Until then, appropriate safeguards remain the default route.

HOW THIS TOUCHES YOUR DATA PROTECTION EXPOSURE

Cross-border transfer rules are one of the areas the ODPC scrutinises most closely — and one of the easiest to get wrong if your contracts, consent language, or adequacy assessments haven't been reviewed since the guidance changed.

Muchangi Patrick & Co. Advocates advises businesses using foreign cloud providers, SaaS tools, or group-company data sharing on structuring lawful cross-border transfers under Kenya's Data Protection Act. If your business moves personal data outside Kenya, we can help you close the gap.

[Book a Consultation](#)

[Chat on WhatsApp](#)

[See Our Data Privacy Practice](#)

TALK TO US

Muchangi Patrick & Co. Advocates advises fintechs, startups, corporates and institutions on data protection and data privacy compliance across Kenya — from ODPC registration and DPIAs to outsourced DPO services and cross-border data transfer advisory. If the issues raised above touch your business, we can help you get ahead of them.

[Book a Consultation →](#)

[Chat on WhatsApp](#)



This analysis is based on the ODPC's Guidance Note on Cross-Border Data Transfers and the Data Protection Act, 2019, together with the Data Protection (General) Regulations, 2021.

The Compliance Brief is prepared by the Editorial Board of Muchangi Patrick & Co. Advocates · Nairobi · Not legal advice – consult qualified counsel before acting on this analysis.

For essential site functionality and to remember your preferences, we use a small number of cookies. With your consent, we also use cookies to understand how visitors use this site. See our [Cookie Notice](#).

[Essential Only](#)

[Accept All](#)