

Legal
Alert



Transferring Data Out of Kenya Just Got a Rulebook Thanks to the ODPC's Latest Guidelines



Transferring Data Out of Kenya Just Got a Rulebook

Thanks to the ODPC's Latest Guidelines

Data Protection | Technology | Cross-Border Trade

Introduction

The Office of the Data Protection Commissioner (ODPC) has published its Guidance Notes for Cross-border Data Transfers, 2026, signed by Data Commissioner, Ms. Immaculate Kassait. The guidance operationalises Part VI of the Data Protection Act, 2019 and Regulation 40 of the Data Protection (General) Regulations, 2021, under which personal data may leave Kenya through four gates only:

1. appropriate safeguards,
2. an adequacy decision by the Data Commissioner,
3. necessity, or
4. the data subject's consent.

The headline sits in the annexes. The Office has issued Kenya's own standard contractual clauses. One is set for controller-to-controller transfers and another for controller-to-processor transfers, ready to drop into transfer agreements, together with application forms for the approval of binding corporate rules. The data-export regime now comes with the paperwork included.

The New Toolkit

Standard clauses, Kenyan edition. The annexed clauses are built to be incorporated into a legally binding instrument under Regulation 40(a) and carry the Regulation 48 minimums:

1. the parties' obligations,
2. verification and audit rights,
3. named destination countries,
4. onward-transfer limits,
5. breach notification,

6. return or deletion on exit, and
7. Kenyan governing law.

Adapt them to the transfer, never dilute them. They prevail over any weaker clause in the contract around them.

- **A real route for binding corporate rules.** Multinational groups can now seek ODPC approval of BCRs for intra-group transfers under Regulation 42, with separate applications for controllers and for processors. Valid Binding Corporate Rules (BCRs) must bind every group entity and employee, name a Kenyan entity with the means to accept liability, handle complaints, and submit to ODPC audits. Material changes trigger fresh approval.
- **The Commissioner keeps the last word.** Ratifying the Malabo Convention or signing a reciprocal data protection agreement with Kenya supports a finding of appropriate safeguards, but nothing is automatic. Section 49(2) lets the Data Commissioner assess adequacy case by case, and section 49(3) lets her prohibit, suspend or condition any transfer. The Data Sharing Code, 2025 adds a duty to notify the Office of cross-border transfers.

What Stays Home and What Follows The Data

- **Localisation survives every gate.** Section 50 requires personal data processed for the strategic interests of the state to run on servers in Kenya or to keep "at least one serving copy" in a Kenyan data centre. Regulation 26 deems that to cover civil registration and legal identity systems, elections, public finance systems, protected computer systems, basic education, and primary and secondary healthcare. No adequacy decision, and no contract, erases this duty.



Transferring Data Out of Kenya Just Got a Rulebook

Thanks to the ODPC's Latest Guidelines

Data Protection | Technology | Cross-Border Trade

What Stays Home and What Follows The Data (Continued)

- **The cloud is a transfer.** Hosting personal data on servers outside Kenya is a cross-border transfer in law. The guidance expects due diligence on providers, data processing agreements, impact assessments for high-risk deployments, and encryption both in transit and at rest.
- **Obligations travel with the data.** An onward transfer by the foreign recipient needs the Kenyan sender's prior written authorisation, proof of equivalent protection at the next destination, and a binding contract, with the first recipient staying fully liable. Onward transfers for the recipient's own purposes, such as analytics, profiling or marketing, are "strictly prohibited".
- **Sensitive data carries a double lock.** Section 49(1) demands the data subject's explicit consent plus confirmation of appropriate safeguards before health, biometric, family or similar data crosses the border, and both must be reflected in the transfer documents themselves.

Ongoing Compliance Obligations : Our Take Home on The Guidelines

- **Map each cross-border flow you run,** including cloud hosting, payroll, CRM and group reporting. Offshore cloud storage is itself a transfer in law, and picking the right gate starts with finding the flow.
- **Pin the legal justification before data moves.** Every transfer needs one of four bases: appropriate safeguards, an ODPC adequacy decision, necessity (contract, legal claim, legitimate interest, vital interest or public interest), or the data subject's explicit consent.

- **Secure the transfer with a binding instrument.** Incorporate the ODPC's Standard Clauses, controller-to-controller or controller-to-processor as the case demands, and line up contracts written before these clauses existed against the Regulation 48 minimums, upgrading wherever they fall short. Multinational groups should price the BCR route now that a formal approval path exists: one approved framework vs transfer by transfer negotiations.
- **High-risk transfers need an impact assessment first.** Section 31 of the Act requires a **DPIA** before the transfer, refreshed whenever a material change such as a new category of data alters the risk.
- **Notify the ODPC.** The Data Sharing Code, 2025 requires controllers and processors transferring personal data outside Kenya to do so to allow the Office to see and monitor cross-border flows.
- **Record every transfer, every time.** Regulation 41(2) demands a formal log: date and time, recipient, justification, a description of the data and the safeguards relied on, produced to the Data Commissioner on request. The paper trail is the compliance.
- **Be ready to prove safeguards on demand.** Demonstration runs before, during and after the transfer, which means live data-processing agreements, current impact assessments, working breach-notification protocols and audit rights you can exercise.
- **Vet the recipients, not just the contracts.** Audit and inspection rights extend to every onward recipient and sub-processor. Where a recipient can no longer comply, suspend the transfer or terminate the arrangement without delay, and have the data returned.
- **Keep the fundamentals running for as long as the data is out.** Data subjects retain their rights wherever the data sits, and requests must be answered within statutory timeframes. Breaches affecting transferred data trigger notification duties. Retention clocks, secure deletion, encryption and authentication standards, staff training and periodic provider reviews for cloud deployments all continue.

CONTRIBUTORS



Thomas Louis
Founding Partner
tlouis@tladvocates.com



Basil Ogolla
Trainee Advocate
bgilbert@tladvocates.com

For more info, contact us.

TRUSTED COUNSEL. BOLD FUTURES

info@tladvocates.com
+254 115 702 315
www.tladvocates.com

Prepared by Thomas Louis Advocates for general information only. This is not legal advice.

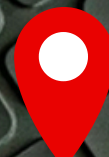


**THOMAS LOUIS
ADVOCATES**

TRUSTED COUNSEL | BOLD FUTURES

 **info@tladvocates.com**

 **+254 115 702 315**

 **Millenium Business
Park, Langata Road,
Karen**

www.tladvocates.com

