LAW LAB AFRICA

RESEARCH WING · REPORT SERIES

MOVING DATA OUT OF AFRICA, COUNTRY BY COUNTRY

The Cross-Border Transfer Rulebook

44 of Africa's 54 states now govern cross-border data transfers by statute, and the statutes do not agree. A matrix of 44 regimes read against their primary texts: adequacy, safeguards, consent, regulator authorisation and the localisation traps, plus the one question that decides most transfers.

44	44	33	5
TRANSFER REGIMES IN FORCE	VERIFIED IN THE MATRIX	REQUIRE REGULATOR SIGN-OFF	MANDATE DATA LOCALISATION

Wanjiku Karanja
Founder & Lead Consultant, Law Lab Africa
July 2026 · research.lawlab.africa

Law Lab Africa Research Wing · Wanjiku Karanja · July 2026 · research.lawlab.africa

How do you lawfully move personal data out of an African country? For 44 of Africa's 54 states the answer now sits in a data protection statute, and the statutes do not agree. This rulebook reads the transfer provisions country by country against the primary texts, codes each regime into one comparable matrix, and names the single question that decides most transfers: whether the regulator has to say yes first. Every cell traces to a named statute. Legal information, not legal advice.

DRAFT FOR REVIEW. Publishes only after editor sign-off; `[W-CHECK]` flags mark claims the editor verifies personally before publication.

---

1. The question multinationals actually ask

A company running payroll in Nairobi, a call centre in Accra and a data warehouse in Frankfurt asks one question of every jurisdiction it touches: *can I send this data home, and what do I have to do first?* Across Africa the answer divides into three tests, and a regime can impose one, two or all three.

- **Adequacy.** Does the destination country offer an "adequate" or "sufficient" level of protection? 41 of the 44 verified regimes recognise an adequacy route.
- **Appropriate safeguards.** Can you carry your own protection with you, via standard contractual clauses, binding corporate rules or a comparable instrument? 31 regimes recognise safeguards.
- **Regulator authorisation.** Must the data protection authority approve the transfer before it happens? This is the test that separates the continent, and the one most compliance teams underestimate.

The rulebook's central finding is that legislation is no longer the binding constraint on cross-border transfers in Africa. The mechanism is. Two companies moving identical data out of two neighbouring states can face completely different obligations: one files nothing and self-assesses, the other cannot lawfully press "send" until a regulator signs off.

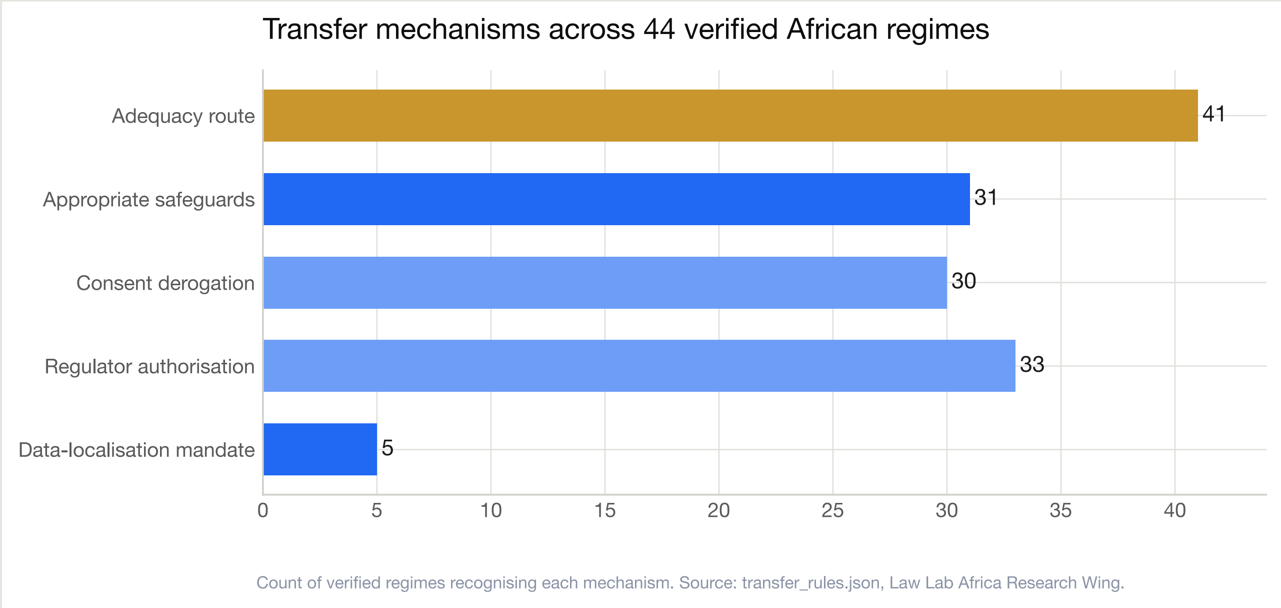

Fig. 1 · How many verified regimes recognise each mechanism. Source: transfer-rules dataset.

2. The matrix

Each row is a regime read against its primary statute. A cell shown as a dash means that mechanism was not established at cell level from the verified text; it is not a claim that the mechanism is absent. Legal-basis citations for every row are in the appendix.

COUNTRY	REGION	ADEQUACY	SAFEGUARDS	CONSENT	AUTHORISATION	LOCALISATION
Algeria	North	Yes	Yes	Yes	Required	No mandate
Egypt	North	Yes	No	Yes	Required	No mandate
Morocco	North	Yes	Yes	Yes	Required	No mandate
Tunisia	North	Yes	No	No	Required	No mandate
Benin	West	Yes	Yes	Yes	Required	No mandate
Burkina Faso	West	Yes	Yes	Yes	Required	No mandate
Cape Verde	West	Yes	Yes	Yes	Conditional	No mandate
Côte d'Ivoire	West	Yes	No	No	Required	No mandate
Ghana	West	No	Yes	—	Not required	No mandate
Guinea	West	Yes	No	No	Required	No mandate
Mali	West	Yes	Yes	No	Required	No mandate
Mauritania	West	—	—	—	Required	No mandate
Niger	West	Yes	Yes	Yes	Required	No mandate
Nigeria	West	Yes	Yes	Yes	Not required	No mandate
Senegal	West	Yes	Yes	Yes	Conditional	No mandate
Togo	West	Yes	Yes	Yes	Conditional	No mandate
Cameroon	Central	Yes	Yes	No	Required	No mandate
Central African Republic	Central	Yes	Yes	Yes	Conditional	No mandate
Chad	Central	Yes	Yes	Yes	Conditional	No mandate
Democratic Republic of the Congo	Central	Yes	Yes	Yes	Required	No mandate
Equatorial Guinea	Central	Yes	No	Yes	Conditional	No mandate

COUNTRY	REGION	ADEQUACY	SAFEGUARDS	CONSENT	AUTHORISATION	LOCALISATION
Gabon	Central	Yes	Yes	Yes	Required	No mandate
Republic of the Congo	Central	Yes	Yes	Yes	Conditional	No mandate
São Tomé and Príncipe	Central	Yes	Yes	Yes	Conditional	No mandate
Burundi	East	Yes	Yes	No	Conditional	No mandate
Comoros	East	Yes	No	No	Required	No mandate
Djibouti	East	Yes	Yes	Yes	Conditional	No mandate
Ethiopia	East	Yes	No	Yes	Conditional	Broad
Kenya	East	Yes	Yes	Yes	Not required	Sensitive data
Madagascar	East	Yes	—	—	Conditional	No mandate
Malawi	East	Yes	Yes	Yes	Not required	No mandate
Mauritius	East	Yes	Yes	Yes	Not required	No mandate
Rwanda	East	No	Yes	Yes	Conditional	Broad
Seychelles	East	Yes	Yes	—	—	No mandate
Somalia	East	Yes	Yes	Yes	Not required	No mandate
Tanzania	East	Yes	—	—	Conditional	No mandate
Uganda	East	Yes	—	Yes	Not required	No mandate
Angola	Southern	Yes	—	Yes	Required	No mandate
Botswana	Southern	Yes	Yes	Yes	Conditional	Broad
Eswatini	Southern	Yes	Yes	—	Not required	No mandate
Lesotho	Southern	Yes	Yes	Yes	Not required	No mandate
South Africa	Southern	Yes	Yes	Yes	Not required	No mandate
Zambia	Southern	Yes	Yes	Yes	Conditional	Broad

COUNTRY	REGION	ADEQUACY	SAFEGUARDS	CONSENT	AUTHORISATION	LOCALISATION
Zimbabwe	Southern	Yes	—	—	Conditional	No mandate

This matrix covers 44 of the 44 states with a data protection law in force (100%). The remaining 0 in-force regimes are read but not yet confirmed against a clean primary text, and are held out of the published matrix rather than guessed at (Section 6). 10 states have no comprehensive law in force and so impose no dedicated transfer regime at all.

3. The authorisation divide

The most useful single line a practitioner can draw across the continent is this: **does the regulator have to approve the transfer first?**

In 33 of the 44 verified regimes (75%) the authority sits somewhere in the transfer path, whether as an outright pre-condition or a conditional approval for non-adequate destinations. 16 require prior authorisation outright: Algeria, Angola, Benin, Burkina Faso, Cameroon, Comoros, Côte d'Ivoire, Democratic Republic of the Congo, Egypt, Gabon, Guinea, Mali, Mauritania, Morocco, Niger, Tunisia. These are the francophone and lusophone regimes, built on the pre-GDPR French model in which the *Commission* authorises transfers as a matter of course. A controller in Algiers, Kinshasa, Niamey, Nouakchott, Rabat or Luanda who treats a transfer as a self-assessment has already broken the law.

The contrast is the anglophone common-law group, which mostly borrowed the GDPR's later architecture of self-assessed adequacy and safeguards: Eswatini, Ghana, Kenya, Lesotho, Malawi, Mauritius, Nigeria, Somalia, South Africa, Uganda let a controller transfer on the strength of its own adequacy or safeguards analysis, with no transfer-by-transfer sign-off. Kenya, Nigeria and South Africa, the three largest markets in the group, all run this model. The practical consequence is that pan-African transfer programmes cannot run on one template. The instrument that satisfies South Africa's section 72 (a binding agreement) does nothing for Morocco's article 43, where the CNDP's express authorisation is the operative act.

The timing difference is the part that reaches operations, not just legal. In a self-assessment jurisdiction a new data flow can go live the day the safeguards are documented; in an authorisation jurisdiction the same flow waits on a regulator's decision cycle, which in several of these authorities runs to quarterly sittings. A launch plan that assumes the Kenyan timeline for a Congolese or Algerian subsidiary is a launch plan that slips. The safeguards column carries its own trap: recognising "appropriate safeguards" in a statute is not the same as a regulator having published usable standard contractual clauses, and in most of these markets no official clause set exists yet, so the safeguards route is available in law but unbuilt in practice.

4. The localisation traps

5 verified regimes go beyond conditioning transfers and require certain data to stay in the country: Botswana, Ethiopia, Kenya, Rwanda, Zambia. They split into two tiers: targeted mandates over defined data categories, and broad rules that reach every controller.

Kenya. Section 50 of the Data Protection Act lets the Cabinet Secretary require processing of prescribed categories, on grounds of the strategic interests of the state or protection of revenue, to be done through a server or data centre located in Kenya. It is a standing power over defined categories, not a general residency rule, and it sits alongside the section 49 restriction that sensitive personal data may leave Kenya only with the data subject's consent and confirmed safeguards.

Zambia. Section 70(1) of the 2021 Act requires ALL personal data to be processed and stored on a server or data centre located in Zambia, with the Minister able to prescribe categories that may be stored abroad; sensitive personal data must stay in Zambia absolutely, with no ministerial carve-out (section 70(3)). For a regional health-tech or fintech platform, that is the difference between one continental database and a Lusaka-resident copy.

Botswana. Section 74 of the 2024 Act carries a proviso most summaries miss: a copy of any personal data transferred abroad must remain in Botswana for the period of processing. That is a local-copy mandate on every transfer, and it sits inside the transfer chapter itself.

Ethiopia. Article 22 of the 2024 Proclamation, headed "Data Sovereignty", requires personal data collected in Ethiopia to be stored on a server or data centre located in the country, lets the Authority designate critical data that may be processed only in Ethiopia, and makes cross-border transfer of sensitive data subject to prior approval.

Rwanda. Article 50 of the 2021 law makes in-country storage the default: storing personal data outside Rwanda is lawful only for a controller or processor holding a registration certificate from the supervisory authority that authorises it.

Localisation is the mechanism most likely to be missed in diligence because it often does not appear in the transfer chapter at all; it lives in a separate processing, storage or security provision. A matrix that reads only the transfer article misses it, which is exactly why this rulebook codes localisation as its own column.

5. Enforcement is not hypothetical

Transfer rules across most of the continent have never produced a public sanction, which tempts controllers to treat them as dormant. Angola is the counter-example worth pricing in. Its data protection authority fined the explosives group **MAXAM USD 150,000 in 2024 for an unlawful transfer of personal data to the United Kingdom** (verified against the APD's own published deliberation notice, 2026-07-11; tracker record ao-apd-2024-0001 in the enforcement dataset), one of the few published cross-border enforcement actions on the continent and a direct signal that the authorisation requirement in the francophone-lusophone group has teeth. The absence of published transfer decisions elsewhere reflects the continent's wider publication gap, not an absence of exposure. That gap is measured in the companion report, Enforcement in the Dark.

6. What this rulebook does not claim

The matrix publishes 44 regimes and withholds 0. Every published cell was read against the primary statute, because law-firm country summaries repeatedly get transfer thresholds wrong, and a matrix that lawyers cite cannot inherit those errors. The July 2026 verification pass closed the backlog by working through the full 44-statute archive, re-reading figures and pivotal words on scanned texts from the page images. The honesty lines that remain are different ones. A cell the text does not establish renders as "not established", never guessed. Egypt is coded from the Arabic statute's unofficial English translation and carries that caveat. The 10 states with no comprehensive law in force are data points, not gaps. And the matrix codes what the statutes say: it does not track implementing regulations, published clause sets or regulator practice, which is where several of these regimes diverge from their text. Mapping a specific jurisdiction's transfer regime at that operational depth, on demand, is the work this rulebook is built to sell.

7. Using this rulebook

This matrix is a map, not advice. It tells a general counsel which of the three tests a jurisdiction imposes and where the authorisation and localisation traps sit, so that the expensive question, the one that needs a lawyer, gets asked in the right place. Read it as a triage tool: a "Required" or "Conditional" cell in the authorisation column means budget for regulator engagement and lead time before the flow can start; a localisation entry means the architecture question comes before the contract question; a row of established adequacy and safeguards cells with no authorisation means the work is documentation a competent team can do in-house. The matrix does not resolve any of these; it tells you which one you are in.

Law Lab Africa maintains the underlying dataset, verifies regimes to order, and advises on transfer strategy across the jurisdictions covered here. To commission a jurisdiction-specific transfer opinion, a transfer-mapping exercise for a portfolio of markets, or verification of one of the 0 regimes still held out of the published matrix, write to research@lawlab.africa.

Methodology

Every cell is coded by `build_dataset.py` from the primary transfer provisions of each state's data protection statute, and computed into this report by `analyze.py`. A regime is marked **verified** only when read against the primary text and at least one core mechanism (an adequacy route or an authorisation requirement) is established; regimes verified against archived primary texts this cycle include the Democratic Republic of the Congo (arts. 187, 188, 202), the Republic of the Congo (arts. 23 to 25), Algeria (arts. 44 to 45), Morocco (arts. 43 to 44), Niger (arts. 62 to 63), São Tomé and Príncipe (arts. 19 to 20) and Kenya (ss. 48 to 50). Mechanism columns: **adequacy** (destination must offer an adequate or sufficient level of protection); **safeguards** (controller-supplied instruments such as standard contractual clauses or binding corporate rules); **consent** (the data subject's consent as a transfer basis or derogation); **authorisation** (whether the regulator must approve the transfer, as an outright requirement or a conditional one); **localisation** (a residency mandate for some or all data). A cell shown as a dash means the mechanism was not established at cell level, never that it is absent. Corrections: research@lawlab.africa, under the correction policy.

Legal basis for every published row:

COUNTRY	LEGAL BASIS	VERIFIED
Algeria	Algeria Law 18-07, arts. 44-45	2026-07-07
Egypt	Egypt PDPL 151/2020, arts. 14-16	2026-07-11
Morocco	Morocco Law 09-08, arts. 43-44	2026-07-07
Tunisia	Tunisia Organic Law 2004-63, arts. 50-52	2026-07-11
Benin	Benin Digital Code Book V (Law 2017-20), arts. 391-392	2026-07-11
Burkina Faso	Burkina Faso Law 001-2021, arts. 42-44	2026-07-11
Cape Verde	Cape Verde Law 133/V/2001 as am. by Law 121/IX/2021, arts. 35-36	2026-07-11
Côte d'Ivoire	Cote d'Ivoire Law 2013-450, arts. 1, 7, 26	2026-07-11
Ghana	Ghana DPA 2012 (Act 843), s.18(2)	2026-07-07
Guinea	Guinea Law L/2016/037, arts. 1, 28	2026-07-11
Mali	Mali Law 2013-015, art. 11	2026-07-11
Mauritania	Mauritania Law 2017-020	2026-07-07
Niger	Niger Law 2022-59, arts. 62-63	2026-07-07
Nigeria	NDPA 2023, Part VIII	2026-07-07
Senegal	Senegal Law 2008-12, arts. 49-51	2026-07-11
Togo	Togo Law 2019-014, arts. 28-31	2026-07-11
Cameroon	Cameroon Law 2024/017, s.32	2026-07-11
Central African Republic	CAR Law 24.001 (2024), arts. 21-27	2026-07-11

COUNTRY	LEGAL BASIS	VERIFIED
Chad	Chad Law 007/PR/2015, arts. 29-32	2026-07-11
Democratic Republic of the Congo	DRC Digital Code 2023, arts. 187(6), 188(10), 200-202	2026-07-07
Equatorial Guinea	Equatorial Guinea Law 1/2016, arts. 27-28	2026-07-11
Gabon	Gabon Law 001/2011 as am. by Law 025/2023, arts. 171-174	2026-07-11
Republic of the Congo	Congo Law 29-2019, arts. 23-25	2026-07-07
São Tomé and Príncipe	Sao Tome Lei 3/2016, arts. 19-20	2026-07-07
Burundi	Burundi Law 1/03 (2026), arts. 15-16	2026-07-11
Comoros	Comoros Loi 14-029/AU (2014), arts. 9, 43(h), 45(f)	2026-07-11
Djibouti	Djibouti Digital Code 2025, arts. 99-103	2026-07-11
Ethiopia	Ethiopia PDPP 1321/2024, arts. 18-22	2026-07-11
Kenya	Kenya DPA 2019, ss.48-50	2026-07-07
Madagascar	Madagascar Law 2014-038	2026-07-07
Malawi	Malawi DPA 2024, ss.38-40	2026-07-11
Mauritius	Mauritius DPA 2017, s.36	2026-07-07
Rwanda	Rwanda Law 058/2021, arts. 48-50	2026-07-11
Seychelles	Seychelles DPA 2023	2026-07-07
Somalia	Somalia DPA 2023, arts. 30-31	2026-07-11

COUNTRY	LEGAL BASIS	VERIFIED
Tanzania	Tanzania PDPA 2022	2026-07-07
Uganda	Uganda DPPA 2019, s.19	2026-07-07
Angola	Angola LPDP 2011 (Lei 22/11)	2026-07-07
Botswana	Botswana DPA 2024 (Act 18 of 2024), ss.74-78	2026-07-11
Eswatini	Eswatini DPA 2022	2026-07-07
Lesotho	Lesotho DPA 2011, s.52	2026-07-11
South Africa	POPIA s.72	2026-07-07
Zambia	Zambia DPA 2021, ss.70-71	2026-07-11
Zimbabwe	Zimbabwe CDPA 2021 [Chapter 12:07]	2026-07-07

Citing this report. Wanjiku Karanja, *The Cross-Border Transfer Rulebook* (Law Lab Africa Research Wing, July 2026), research.lawlab.africa/reports. Free to cite and quote with attribution; commercial reuse of the underlying dataset is licensed separately.

Law Lab Africa is a technology-law consultancy and research house. The Research Wing turns African regulatory activity into structured intelligence: the tracker, the landscape survey, the laws library and this report series. For alerts as the matrix grows, subscribe at research.lawlab.africa/reports.