ISSUE BRIEF

GLOBAL

Cross-Border Data Flows in Africa: Examining Policy Approaches and Pathways to Regulatory Interoperability

Author: Mercy King'ori, FPF, June 2025

FUTURE OF PRIVACY FORUM

Executive Summary

This Issue Brief explores existing policy and legal approaches to inter-African cross-border data flows, focusing on ongoing sub-regional initiatives, the evolving taxonomy for cross-border data flows across the continent, and existing tools for facilitating such transfers. Its drafting benefited from feedback received during a side event on “Securing Safe and Trustworthy Cross-Border Data Flows” organized by FPF on May 8, 2025 during the NADPA-RAPDP Conference in Abuja, Nigeria. The Issue Brief is accompanied by an Annex that outlines cross-border data transfer provisions across Kenya, Nigeria, South Africa, Rwanda, and Ivory Coast.

Table of Contents

Introduction

Cross-border data flows are critical to Africa's digital economy, enabling trade, innovation, and access to continental and global markets. As the drive towards data-driven technologies among businesses and governments grows, the ability to transfer personal data across borders efficiently and securely has become a key policy concern for the continent, a position supported by the African Union (AU) and its Member States.[1] With this overarching goal in mind, the AU has released numerous policy recommendations and promoted the Malabo Convention, all of them placing emphasis on the free flow of personal data.[2] Additionally, the AU Data Policy Framework (AU DPF) provides a blueprint for Member States developing data governance frameworks to support intra-African trade and the eventual creation of a single African digital market. It emphatically states that "a key characteristic of the free flow of goods and services is the free flow of data."[3] Similarly, Article 20 of the Protocol on Digital Trade provides a general rule allowing data flows.

As Member States are currently integrating the AU DPF into their respective national laws, key decisions such as the nature of cross-border data flows provisions in their data governance regimes are likely to receive greater attention. The implementation process comes amid the African Continental Free Trade Area (AfCFTA) Secretariat announcing the release of eight annexes to the Protocol on Digital Trade, including one on cross-border data flows,[4] marking the first continental initiative that addresses data flows comprehensively. A repeated concern around cross-border data flows has been the need to ensure continental policy and legal alignment for data flows where countries have adopted diverse regulatory approaches to cross-border data transfers, reflecting broader debates on data sovereignty, economic development, and privacy protection.

Some Member States have enacted stringent requirements on the processing of personal and sensitive data, such as strict data localization requirements, while others promote open data flows. While discussed across various data governance debates on the continent, differences in the social, political, and economic contexts have been used to explain the varied approaches to cross-border data flows provisions, despite the overall aspiration pointing towards promoting the free flow of data within the continent with measured restrictions. The challenge then lies in balancing these interests—ensuring

[1] African Union Interoperability Framework for Digital ID
https://au.int/sites/default/files/documents/43393-doc-AU_Interoperability_framework_for_D_ID_English.pdf
[2] Malabo Convention https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
[3] African Union Data Policy Framework
https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf
[4] AfCFTA Secretariat announces the adoption of eight annexes to the Protocol on Digital Trade
https://x.com/AfCFTA/status/1891226358208196833

data protection and addressing widely referenced concerns of national security, while fostering economic integration and digital innovation across the continent.

This draft for discussion examines the current state of policy and legal approaches to inter-African cross-border data flows, focusing on ongoing sub-regional initiatives, the evolving taxonomy for cross-border data flows across the continent, and existing tools for facilitating such transfers. It then explores potential pathways towards an interoperable framework for cross-border data flows, identifying key policy considerations to balance data protection, economic integration, and regulatory alignment. By providing a structured assessment of existing efforts and future directions, this brief aims to support policymakers and stakeholders in advancing a balanced and interoperable approach to cross-border data flows within Africa. Lastly, this Issue Brief is accompanied by an Annex that outlines cross-border data transfer provisions across **Kenya, Nigeria, South Africa, Rwanda, and Ivory Coast**, using a set of comparative metrics. The Annex is a useful tool for stakeholders wishing to compare and contrast existing provisions for cross-border data flows across Africa, and to identify both challenges and opportunities for regulatory interoperability in this area. The draft will be discussed with participants of the Future of Privacy Forum's side event on cross-border data flows during the NADPA[5] Conference in Abuja on 8 May 2025, and will be enhanced with their feedback.

Policy Efforts for Facilitating Cross-Border Data Flows in Africa: Taxonomy and Tools for Interoperability

This section sheds light on the state of policy and legislative efforts for cross-border data flows across the continent. It delves into three key areas: ongoing sub-regional efforts towards interoperability, taxonomy of existing regimes on the continent, and tools for transfers as found in the national laws of most countries on the continent.

Ongoing Sub-Regional Efforts Towards Regulatory Interoperability

Having acknowledged the onerous task of creating a single framework for data-related policies, including privacy and data protection, the AU continues to leverage existing regional economic communities (RECs) to create an interoperable policy framework for its Member States. Historically known for their crucial efforts in driving peacekeeping and security efforts in the continent, RECs are now seen as key drivers for an interoperable approach to data governance, including on cross-border data flows.

[5] Network of African Data Protection Authorities

Their involvement in privacy and data protection regulation is not new, with early efforts beginning more than a decade ago with the Support for the Harmonisation of the ICT Policies in Sub-Saharan Africa project (HIPSSA) that resulted in existing data protection model laws and frameworks in four of the eight RECs.[6] However, these frameworks have had minimal impact on the content of the laws of their Member States. Several reasons exist for these including that some are non-binding, such as the Southern Africa Development Community (SADC) Model Law, while others were created at a time when individual Member States already had draft cyber laws in place as was the case during the drafting of the East Africa Community (EAC) Cyberlaws Framework.

These renewed efforts at utilizing RECs as the drivers for more aligned data governance frameworks seek to build on early efforts by amending existing sub-regional frameworks as well as developing new frameworks. For instance, the revision of the Economic Community of East African States (ECOWAS) Supplementary Act on Personal Data Protection is currently ongoing.[7] In the SADC region, there are plans to amend the data protection model law. Additionally, the SADC Secretariat released a call for consultants to assist with the modernization of the model law.[8] In East Africa, the East African Data Governance Framework is being developed,[9] as well as a proposed EAC Data Protection and Privacy Act.[10] It is envisioned that the amendments and development of new frameworks will address areas of inconsistencies between the Malabo Convention (which is also under amendment), and existing regional frameworks that address cross-border data flows. For instance, the Malabo Convention prohibits the flow of data outside AU territories without adequate protection, but remains silent on data transfers between Member States, despite countries having varied thresholds for cross-border data transfers.

Additionally, comprehensive interoperability requires that all RECs consider data protection frameworks that include cross-border data flows provisions as well as ensuring that the legislative proposals are legally binding. Owing to the differing priorities and levels of development at the time of drafting the RECs frameworks under HIPSSA, a nascent ICT industry at the time, the Intergovernmental Authority on Development (IGAD) and the Union du Maghreb Arab (UMA) did not create their own regional data protection frameworks. However, it is nevertheless important that Member States of these RECs

[6] Future of Privacy Forum. RECs Report: Towards a Continental Approach to Data Protection in Africa. February2024 https://fpf.org/blog/recs-report-towards-a-continental-approach-to-data-protection-in-africa/
[7] Revision of the Supplementary Act A/SA.1/01/10 on the Protection of Personal Data in the ECOWAS Region https://citizenengagement.nepad.org/engagement/revision-of-the-supplementary-act-asa10110-on-the-protection-of-personal-data-in-the-ecowas-region
[8] SADC Secretariat released a call for consultants to assist with the revision and modernization of the model law https://www.sadc.int/sites/default/files/2022-03/MODEL_LAWREOI_-_Revision_of_SADC_Data_Protection_Model_Law_04022022.pdf
[9] EAC set to advance Data Governance and Protection with development of a regional Policy Framework https://www.eac.int/press-releases/3195-eac-set-to-advance-data-governance-and-protection-with-development-of-a-regional-policy-framework
[10] EAC launches innovative Data Governance Training Programme for Judges https://www.eac.int/press-releases/311-digital-transformation/3326-eac-launches-innovative-data-governance-training-programme-for-judges

consider them as part of contributing to an interoperable cross-border data flows regime in the continent. This is particularly important as more IGAD and UMA Member States currently have data protection laws, such as Ethiopia and Somalia. Similarly, the Draft EAC legal framework for Cyberlaws,[11] which will soon be replaced by the East African Data Governance Framework, did not contain provisions on cross-border data flows. Furthermore, some RECs frameworks impose restrictions on the flow of data to other AU Member States outside their REC such as the SADC, ECOWAS, and ECCAS. The restrictions are stronger in the SADC, where restrictions on cross-border data flows found in national laws have extraterritorial effect on other SADC Member States.[12]

Taxonomy of Cross-Border Data Flows Regimes in Africa

As sub-regional efforts continue to shape interoperable data protection and cross-border data flows frameworks in Africa, a diverse range of approaches continues to emerge nationally. Understanding the taxonomy of cross-border data flows in Africa requires examining the various legal, policy, and institutional mechanisms that govern data transfers at both national and regional levels. Such frameworks often reflect differing priorities, from economic integration and digital trade facilitation, to data sovereignty and privacy protection. While some approaches align with globally recognized data protection frameworks, others emphasize national control over data flows. Broadly, jurisdictions on the continent can be split into two categories:

- The first encompasses countries with no cross-border data flows provisions, either because such provisions are omitted from the law or countries lack comprehensive data protection laws in entirety. However, it is possible that countries in the latter category have sectoral laws with implications for cross-border data transfers, as is the case in Ghana, for example.

- The second includes countries with restrictions for transferring personal data to other African countries, thus impacting data flows within and outside the continent.

Cross-Border Data Flows Tools and their Implementation in Africa

Building on the taxonomy of cross-border data flows models in Africa, it is essential to highlight the current tools that facilitate cross-border data transfers in the continent. Ideally, these tools serve as mechanisms for ensuring compliance with data protection laws while enabling the movement of data across jurisdictions. A cursory look at African data protection laws shows the existence of commonly

[11] Harmonizing Cyberlaws Regulations: The Experience of EAC https://au.int/sites/default/files/newsevents/workingdocuments/27223-wd-harmonizing_cyberlaws_regulations_the_experience_of_eac1.pdf
[12] RECs Report: Towards a Continental Approach to Data Protection in Africa, 2024 https://fpf.org/blog/recs-report-towards-a-continental-approach-to-data-protection-in-africa/

known data transfer tools. However, the specific mechanisms available vary from country to country. This section briefly explores the state of implementation of the varying existing means for transferring personal data across Africa, assessing their availability, effectiveness, and role in shaping the continent's landscape for cross-border data flows.

Cross-border data transfer tools such as **adequacy decisions, standard contractual clauses (SCCs), binding corporate rules (BCRs), certification mechanisms, and derogations** are referenced in various African data protection laws. However, their effectiveness remains weak in most jurisdictions often due to the absence of regulatory guidelines, institutional capacity constraints, and fragmented legal approaches across the continent.

Existence of an Adequate Level of Protection and Related Adequacy Decisions

The **requirement for an adequate level of protection in the recipient country is the most common mechanism** for cross-border data transfers in many data protection laws in the continent. Data Protection Authorities (DPAs) are tasked with assessing whether the recipient country's legal framework provides an adequate level of protection based on criteria stipulated in the different laws. Despite the existence of this tool in most Member States' laws, unified guidelines on such assessments are yet to be developed, and the legal framework remains fragmented with countries opting to develop parameters unilaterally, despite having very similar data protection legal frameworks.[13] Assessments of adequacy are already being conducted, as seen from the work of DPAs in Botswana[14] and Nigeria.[15] However, this has not been without its challenges, especially on the rationale used to make such determinations, resulting in courts intervening to mandate DPAs to establish appropriate assessment methodologies that comply with national laws. For instance, in Nigeria, the High Court annulled a whitelist of countries where data could be transferred freely on the grounds that the assessment did not comply with the legal requirements for assessing adequacy.[16]

Closely related to the standard of an adequate level of protection are adequacy decisions, which are granted by regulatory authorities—such as the European Commission (EC) under the General Data Protection Regulation (GDPR) in the European Union. African countries are not new to the process, with

[13]Boshe P. African Data Protection Laws – Current Regulatory Approaches, Policy Initiatives, and the Way Forward https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3947664

[14] Botswana: Minister of State President publishes Transfer of Personal Data Order 2022 https://www.dataguidance.com/news/botswana-minister-state-president-publishes-transfer

[15] Federal High court nullifies part of the adequacy of the "whitelist" on International data transfer and calls for review of the list https://ikigaination.org/federal-high-court-nullifies-part-of-the-adequacy-of-the-whitelist-on-international-data-transfer-and-calls-for-a-review-of-the-list/#:~:text=list%20%2D%20ikigaination.org-,Federal%20High%20court%20nullifies%20part%20of%20the%20adequacy%20of%20the,for%20review%20of%20the%20list.&text=We%20are%20excited%20to%20share,data%20transfers%20has%20been%20delivered

[16] Ibid.

several countries having unsuccessfully attempted to obtain an adequacy decision from the EC,[17] while others, such as Keny,a are in discussions with the body for an adequacy determination.[18] Other countries have received adequacy determinations from authorities outside the European Union, such as Bahrain's recognition of Egypt, Morocco, and Nigeria[19] as providing an adequate level of protection of personal data.

Ideally, adequacy decisions or the existence of an adequate level of protection eliminate the need for further safeguards. However, some laws introduce nuance by imposing additional requirements even when the legal framework of the recipient country or organization is deemed adequate after an assessment. For example, in Mauritius, while the law provides for transfer mechanisms such as adequacy, the country's data protection authority may still require the transferring entity to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests for such transfers.[20] Several reasons can explain this regulatory caution, including weak enforcement mechanisms and differing interpretations of adequacy, as evidenced by different standards for assessing adequacy.

Certification Mechanisms

Certification mechanisms are a relatively new tool for cross-border data flows among African countries, featuring mostly in post-GDPR laws. As a means for cross-border data transfers, certification mechanisms involve independent assessments that ensure the recipient meets defined privacy requirements. No African country has yet implemented a functioning certification scheme for cross-border data flows owing to the absence of accreditation bodies to provide oversight and clear guidelines. However, recent developments signal growing interest. Seychelles' new Data Protection Act, enacted in 2023, explicitly recognizes certification mechanisms as a transfer mechanism, aligning with global best practices. Section 47(5) provides that the Commission may authorise the transfer of personal data to another country provided that country is part of a cross-border privacy rules system that meets the requirements stipulated under this section.[21] Meanwhile, Nigeria has announced plans to join the Cross-Border Privacy Rules (CBPR) Forum, an international certification framework that enables

[17] Data Protection Regimes in Africa: too far from the European 'adequacy' standard? https://academic.oup.com/idpl/article-abstract/3/1/42/643986?redirectedFrom=PDF
[18] Data Protection: Kenya and the EU launch very first Adequacy Dialogue on the African continent https://www.eeas.europa.eu/delegations/kenya/data-protection-kenya-and-eu-launch-very-first-adequacy-dialogue-african-continent_en?s=352
[19] Musa S, Oloyede R, et al, 2022, Roundup on Data Protection in Africa. https://assets-global.website-files.com/641a2c1dcea0041f8d407596/644d2c11739815a42ff6bd88_Round-up-of-data-protection-Africa-2022.pdf
[20] Section 36(4), Mauritius Data Protection Act (2017)
[21] Seychelles Data Protection Act, 2023 https://www.gazette.sc/sites/default/files/2023-12/Act%2024%20-%202023%20-%20Data%20Protection%20Act%202023.pdf

businesses to transfer data while ensuring compliance with privacy principles.[22] This move is enabled by a regulatory framework that makes provision for certification mechanisms.

Standard Contractual Clauses, Binding Corporate Rules, and Derogations

The use of pre-approved contractual agreements is not common practice in the continent, despite being referenced in numerous data protection laws. Currently, Rwanda is the only African country with model SCCs, which were released in February 2024.[23] In the absence of approved SCCs, controllers and processors now navigate compliance through ad-hoc legal agreements.

Despite their lack of popularity, SCCs remain a viable tool for interoperable cross-border data flows in the continent. Where national and continental frameworks vary in their approach to such transfers, SCCs could provide a structured and legally recognized means for organizations to facilitate cross-border data flows while demonstrating compliance.

On derogations, many African data protection laws allow for exceptions to cross-border data transfer restrictions under specific circumstances. These typically include consent from the data subject, contractual necessity, public interest, legal claims, or the protection of vital interests. However, relying on derogations carries risks, as they are typically designed for specific, exceptional cases rather than serving as a foundation for routine data transfers. Additionally, African DPAs have not provided extensive guidance on the scope and limits of these.

Paths to Interoperable Cross-Border Data Transfers for the Continent and Proposed Policy Considerations

The AU, in its mandate to harmonize policies in the continent, has proposed paths to alignment within the data governance space that could also be useful for cross-border data transfers. Using the SWOT methodology, the AU Data Policy Framework provides a situational analysis that identifies several overarching strengths, weaknesses, opportunities, and threats, which, if built and worked upon, can set the continent on the path towards an interoperable regulatory ecosystem for cross-border data transfers. This section builds on the AU's assessment by proposing policy considerations that countries and their respective RECs can adopt to bolster the strengths and opportunities as well as address

[22] U.S. Department of Commerce, Joint Statement on Harnessing Artificial Intelligence, Facilitating Data Flows and Empowering Digital Upskilling Between the United States Department of Commerce and the Nigerian Ministry of Communications, Innovation and Digital Economy https://www.commerce.gov/news/press-releases/2024/07/joint-statement-harnessing-artificial-intelligence-facilitating-data#:~:text=To%20further%20advance%20our%20shared,tool%20to%20facilitate%20trusted%20data

[23] Standard Contractual Clauses for Personal Data Transfer Outside Rwanda, 2024 https://dpo.gov.rw/assets/documents/Personal-Data-Transfer-Outside-Rwanda-Standard-Contractual-Clauses.pdf

weaknesses and threats identified. In the Table below, the strengths, weaknesses, opportunities, and threats are the ones identified by the AU in the DPF (in the first column), to which we suggest policy considerations that address each of them (in the second column).

Strengths Identified by the AU	**Proposed Policy Considerations**
"Existence of foundational regional data governance instruments"	• Use the Malabo Convention and other AU instruments such as the Protocol on Digital Trade and its Annex dedicated to cross-border data flows as a baseline for developing trusted standards. • Develop a continental interoperability framework that maps and compares national laws to these instruments, encouraging mutual recognition and legal alignment to enable trusted data flows.
"Existence of regional and continental courts to enable harmonised dispute resolution"	• Expand existing continental redress mechanisms to handle data protection issues, including on cross-border data transfers disputes. This will provide legal certainty for businesses and ensure individuals can access remedies across borders.
"Fewer and less developed data protection laws that provide great potential for early, rapid continental harmonization enabling cross-border trade"	• Support AU-guided model laws and regulatory toolkits that countries can adopt or adapt. • Promote co-drafting initiatives across countries to ensure alignment from the initial drafting, reducing fragmentation and enabling a smoother path to cross-border data transfers.
"Regional Economic Communities (RECs) to support economic aspects of data policy initiatives"	• Empower RECs to serve as data policy incubators, piloting cross-border data-sharing sandboxes and harmonized compliance schemes such as joint DPA initiatives or REC-level certifications. These efforts can later scale to the continental level, driven by economic integration goals.
Weaknesses Identified by the AU	**Proposed Policy Considerations**
"Inconsistencies in the treatment of data in data protection frameworks owing to non-harmonized data governance regimes"	• Continued facilitated peer reviews and regulatory cooperation forums between DPAs, such as NADPA, to promote alignment of interpretations and enforcement practices. • Promote a "mutual recognition mechanism" to allow data to flow between countries with equivalent protections as opposed to taking unilateral national measures.

"Localization rules that limit the cross border flow of information necessary for local value creation and establishment of a single market"	• Construe alternate modalities to protect national interests without unnecessarily restricting regional data flows, through evidence-based, targeted, and limited policy interventions. • Introduce model legal transfer mechanisms such as AU standard contractual clauses and consent templates to facilitate lawful and secure data transfers. • Encourage periodic review mechanisms and economic impact assessments to ensure alignment with the digital trade objectives of the existing localization rules identified by the AU.
Opportunities Identified by the AU	**Proposed Policy Considerations**
"Global efforts to develop and harmonize data policy and governance frameworks"	• Continue developing an African position on global data governance, grounded in regional instruments like the Malabo Convention, to guide engagement in key fora. The recent endorsement of the Africa Digital Compact is a step in the right direction. • Ensure interoperability by adopting flexible, principles-based standards that accommodate local context while enabling international data flows.
Threats Identified by the AU	**Proposed Policy Considerations**
"Constantly changing data protection and privacy risks"	• Promote adaptive regulatory approaches, including regulatory sandboxes and sunset clauses, to test rules in line with technology. • Adopting flexible, principles-based standards that accommodate broad interpretation based on new risks.
"Discriminatory, automated (algorithm-based) decision-making risks resulting from the invisibility and underrepresentation of categories of people in datasets, and algorithm modeling shortcomings"	• Support data governance frameworks that mandate demographic representation in datasets used in automated decision-making. • Invest in African-led research in artificial intelligence and standard setting to ensure local contexts and values are reflected in model design and deployment.
"Inadequate levels of international policy cooperation required to deal with global data issues, including access, integrity, security, equity, rights, and ethics"	• Advocate for multilateral data governance mechanisms through AU representation in global forums for policy cooperation on data-related issues identified as priorities by the AU. • Forge partnerships with regional and global institutions to

	co-develop norms, share best practices, and promote cross-border trust frameworks.
"Inability of some countries to overcome the challenges of creating enabling environments necessary to realize opportunities"	• Promote continued regional resource-sharing agreements, including DPA staff exchanges and shared compliance tools, to close capacity gaps. • Create incentives for public-private partnerships to build trust frameworks across under-resourced regions.

Conclusion

While many African data protection laws recognize the importance of cross-border data flows as well as a variety of mechanisms for secure cross-border data flows, their operationalization remains weak in most jurisdictions. This gap creates legal uncertainty both for companies and other organizations transferring personal data, as well as individuals whose personal data is processed. It also hinders digital trade and limits regulatory effectiveness, leading to a complex compliance environment for controllers and processors across the continent. Key steps towards addressing these challenges will include building consensus on the legal provisions of cross-border data flows and enacting implementation frameworks that align with these rationalized legal provisions.

Annex: Country Comparison of Cross-Border Data Transfer Provisions across Kenya, Nigeria, South Africa, Rwanda, and Ivory Coast

Comparison Metrics

1. **Transfer mechanisms**

   Do the laws and regulations provide for commonly known mechanisms for cross-border data transfers?

2. **DPA oversight of transfers**

   Do the laws and regulations require regulatory approval before data can be transferred? Some laws and regulations mandate pre-transfer authorizations that can be in the form of:

   a. Prior approval from the DPA.

   b. Notification or declaration-based systems, where organizations must report transfers but do not need pre-approval.

3. **Institutional cooperation among DPAs**

   Do the laws and regulations encourage harmonization and mutual assistance?

   Effective cross-border data transfers regulation requires regional cooperation between DPAs. A notable form of cooperation relates to information-sharing mechanisms between DPAs.

4. **Data subject rights in data transfers**

   Do the laws and regulations require that individuals retain rights over their data even after a transfer?

   Commonly referenced data subject rights in the event of a data transfer include:

   a. Right to be informed before their data is transferred abroad;

   b. Right to object to a transfer if they believe it affects their privacy; and

   c. Right to obtain redress in case of unauthorized access.

5. **General data localization requirements**

   Do the laws and regulations mandate local storage of specific data types? Localization approaches include:

   a. Absolute localization where all data must be stored within national borders; or

   b. Sector-specific localization such as children's data, financial, health, or government data must be stored locally.

6. **Penalties for non-compliance with cross-border data transfers provisions**

Do the laws and regulations impose financial penalties for unauthorized data transfers?

Country	Transfer Mechanisms	Data Subject Rights	General Data Localization	Cooperation Among DPAs	DPA Oversight	Fines and Penalties
Kenya	Section 48 of Data Protection Act 2019 provides numerous bases for transfer of personal data out of Kenya.	Section 29 provides that a data subject has the right to be notified about the use of their personal data, including if it will be transferred out of the country.	Section 50 of provides that the Minister of ICT has powers to mandate the processing of certain personal data locally on grounds of the strategic interests of the state or protection of revenue.	Section 8 lists one of the functions of the ODPC as promoting international cooperation on data protection matters.	Section 48(a) and 49(1) provides that the ODPC is charged with reviewing the safeguards put in place.	Section 63 provides for imposing an administrative fine for violating any section of the law.
Nigeria	Section 41 of Nigeria Data Protection Act 2023 provides for bases for transferring personal data.	Section 34 provides for various rights in the event of a data transfer, including the right to be notified when data will be transferred to third countries or international organizations.	Section 41(4) grants the NDPC powers to develop regulations that designate categories of personal data that may not be transferred to other countries.	Section 5(j) explicitly lists one of the functions of the NDPC as engaging with national and regional authorities to develop strategies for regulation of cross-border data transfers.	Section 41(3) provides that the NDPC may make regulations requiring data controllers and data processors to notify it of the measures in place when relying on any of the grounds for transferring personal data as well as	Section 48 provides that, where the NDPC is satisfied that a data controller or processor has violated the Act, it can impose an enforcement order or a sanction, which can take various forms provided for under

					explain their adequacy based on the criteria for adequacy under Section 42.	Section 48(2).
South Africa	Section 72(1) of the Protection of Personal Information Act provides a list of lawful bases for transfer of personal data.	Section 5 provides for data subjects' rights that apply generally to all forms of processing personal data, including cross-border data transfers.	POPIA does not include provisions on data localization.	Section 40 places on the Information Regulator a duty to co-operate on a national and international basis with other persons and bodies concerned with the protection of personal information, including facilitating cross-border cooperation in the enforcement of privacy laws.	Section 57(1)(d) explicitly mandates prior authorization for cross-border data transfers if the transfer involves sensitive personal data, children's data where the foreign country does not provide an adequate level of protection as provided under section 72. Section 57(2) provides that the requirements of prior authorization may be	Section 59 makes it an offense not to obtain prior authorization, liable to a penalty in the form of a fine or imprisonment not exceeding 12 months or both (Section 107).

					expanded to other forms of personal data where the processing poses a risk to the legitimate interests of the data subject. However, Section 57(3) introduces an exception to the requirement for prior authorization where a code of conduct applicable to a particular sector exists. The IR has approved numerous Codes of Conduct and is generally open to approving them where the correct procedure for obtaining them is followed.	

Rwanda	Article 48 of Law No. 058/2021 provides a list of lawful bases for transferring personal data. It also adds that the DPA can expand the bases for transfers.	Article 42(10) and 18(5) provide for the data subjects to be notified where personal data will be transferred out of the country. Additionally, a data subject is required to provide consent where a controller or processor relies on consent as the basis for cross-border data transfers.	Article 50 imposes a general ban on the transfer of personal data by requiring controllers and processors to store personal data in Rwanda, except where they hold a valid registration certificate issued by the supervisory authority authorizing storage outside the country.	Article 27(8) creates a duty for the Data Protection Office to cooperate with authorities, organizations or entities operating within the country or abroad in the protection of personal data and privacy.	Article 30(7) requires controllers or processors to list the countries to which personal data may be transferred during registration. Article 48(1) requires controllers to obtain prior authorization for cross-border data transfers from the supervisory authority after providing proof of appropriate safeguards with respect to the protection of personal data. Article 49 requires data controllers or processors to sign a written contract	Compared to most countries, Rwanda explicitly provides for the offense of transferring personal data contrary to the law. Article 56 provides that, upon conviction, a person is liable to an imprisonment of not less than one year but not more than three years and a fine.

					when transferring personal data outside Rwanda, outlining each party's responsibilities to ensure legal compliance, and allows the supervisory authority to set contract rules, request proof of compliance, or suspend transfers to protect data subjects' rights.	
Ivory Coast	While Law No. 2013-450 envisions cross-border data transfers, it does not categorize the various means for processing of personal data.	During collection of personal data, Article 28 requires a controller or processor to notify the data subject on the possibility of transferring personal data out of the country.	Article 6 and 8 exempt certain forms of personal data processing from receiving prior authorization, effectively creating a conditional prior authorization	The law does not provide for instances of collaboration.	Article 7 requires a controller or processor to provide prior authorization for cross-border data transfers.	Article 51 allows the data protection authority to impose sanctions—including temporary or permanent withdrawal of authorization and financial penalties—on a data controller or

			regime. It is also worth noting that where the authority does not provide feedback within a month of seeking approval this amounts to a rejection for prior authorization as per Article 11.			subcontractor who fails to comply with the law after being notified. The penalty amount depends on the severity of the breach and any gains from it, and may not exceed 10 million CFA francs or, in cases of repeated violations or companies, up to 500 million CFA francs or 5% of annual turnover. These penalties apply alongside any criminal sanctions.

Washington, DC | Brussels | Singapore | Tel Aviv

info@fpf.org

FPF.org