



East African Journal of Law and Ethics

eajle.eanso.org

Volume 9, Issue 3, 2026

Print ISSN: 2707-532X | Online ISSN: 2707-5338

Title DOI: <https://doi.org/10.37284/2707-5338>



EAST AFRICAN
NATURE &
SCIENCE
ORGANIZATION

Original Article

Data Localisation, National Security and Public Interest in Cross-Border Data Transfers: Convergence or Divergence in Kenya and Rwanda?

Dr. Rindstone Bilabamu Ezekiel, PhD¹*

¹ Open University of Tanzania, P. O. Box 23409, Dar es Salaam, Tanzania.

* Author for Correspondence Email: rindstone.ezekiel@gmail.com

Article DOI: <https://doi.org/10.37284/eajle.9.3.5862>

Date Published: **ABSTRACT**

25 September 2026

Keywords:

*Convergence,
Data localisation,
Kenya Data Protection
Act,
National security,
Necessity,
Cross-border data
transfer,
Principles-based
regulation,
Proportionality,
Rwanda Data Protection
and Privacy Law.*

This article examines how principles of necessity, proportionality, and regulatory discretion are operationalised in cross-border data transfer regimes in Kenya and Rwanda, with specific focus on national security and data localisation considerations. Despite formal convergence in adopting adequacy-based transfer frameworks, significant variation persists in how these principles are embedded and applied in practice, shaping divergent regulatory outcomes in cross-border data governance. The study addresses the research question: To what extent do Kenya and Rwanda operationalise necessity, proportionality, and discretion in regulating cross-border data transfers through national security and data localisation provisions, and what do these differences reveal about convergence in African data protection regimes? The objectives are to (i) identify the legal bases governing cross-border data transfers in both jurisdictions, (ii) analyse how national security and public interest considerations are structured within these regimes, and (iii) assess the extent to which regulatory discretion produces convergence or divergence in practice. Methodologically, the article adopts a comparative doctrinal legal analysis, focusing on statutory interpretation of Kenya's Data Protection Act 2019 and Rwanda's Law No. 058/2021 on the Protection of Personal Data and Privacy, supplemented by relevant subsidiary regulations. It applies a principles-based evaluation to assess how necessity, proportionality, and discretion are embedded in transfer authorisation and restriction mechanisms. The findings indicate formal convergence in adequacy-based transfer rules but substantive divergence in regulatory architecture: Kenya relies on ex post, enforcement-driven discretion with broad public interest overrides, while Rwanda employs an ex-ante, structured authorisation model incorporating statutory localisation tendencies. The study concludes that convergence remains partial and fragmented, driven more by shared normative frameworks than uniform regulatory execution. It recommends clearer statutory articulation of proportionality standards and more transparent criteria for national security-based transfer restrictions to enhance legal certainty and regional coherence.

APA CITATION

Ezekiel, R. B. (2026). Data Localisation, National Security and Public Interest in Cross-Border Data Transfers: Convergence or Divergence in Kenya and Rwanda?. *East African Journal of Law and Ethics*, 9(3), 516-537. <https://doi.org/10.37284/eajle.9.3.5862>.

CHICAGO CITATION

Ezekiel, Rindstone Bilabamu. 2026. "Data Localisation, National Security and Public Interest in Cross-Border Data Transfers: Convergence or Divergence in Kenya and Rwanda?" *East African Journal of Law and Ethics*, 9 (3), 516-537. <https://doi.org/10.37284/eajle.9.3.5862>.

HARVARD CITATION

Ezekiel, R. B. (2026). "Data Localisation, National Security and Public Interest in Cross-Border Data Transfers: Convergence or Divergence in Kenya and Rwanda?.", *East African Journal of Law and Ethics*, 9(3), pp. 516-537. doi: 10.37284/eajle.9.3.5862.

IEEE CITATION

R. B. Ezekiel. "Data Localisation, National Security and Public Interest in Cross-Border Data Transfers: Convergence or Divergence in Kenya and Rwanda?", *EAJLE*, vol. 9, no. 3, pp. 516-537, Sep. 2026.

MLA CITATION

Ezekiel, Rindstone Bilabamu. "Data Localisation, National Security and Public Interest in Cross-Border Data Transfers: Convergence or Divergence in Kenya and Rwanda?", *East African Journal of Law and Ethics*, Vol. 9, no. 3, Sep. 2026, pp. 516-537, doi:10.37284/eajle.9.3.5862.

INTRODUCTION

Cross-border data transfers have become essential to digital economies, yet growing concerns over national security and data sovereignty have prompted states to adopt increasingly restrictive data governance measures (Tan, 2024; Khasanova & Tai, 2024). Gao (2024) argues that national security is one of the three dominant paradigms shaping contemporary approaches to cross-border data transfers, alongside privacy and economic approaches. In practice, countries increasingly adopt regulatory frameworks that prioritise national security concerns and employ security assessments and transfer controls that effectively function as forms of soft data localisation.

This tension is particularly significant in East Africa, where digital transformation and regional integration depend on the movement of personal and non-personal data across national borders. Kenya and Rwanda provide useful comparative cases because both have emerged as leaders in digital governance (Sekalala & Lake, 2025; Sangwa & Mutabazi, 2025). These countries are at the forefront of digital development and have made digital transformation a central pillar of national development (Arnold, 2022). Against this backdrop, they are developing distinct legal and regulatory approaches to data protection, national security, and cross-border data transfers.

This article examines how the principles of necessity, proportionality, and regulatory discretion are operationalised within their respective legal frameworks, focusing on national security and data localisation in cross-border data transfers. It proceeds from the premise that although both jurisdictions adopt adequacy-oriented approaches broadly aligned with international standards, the incorporation of national security exceptions and localisation-oriented controls reveals key areas of regulatory divergence. By assessing whether data localisation, national security, and public interest frameworks exhibit convergence or divergence, the article contributes to emerging scholarship on African data governance and explores the implications of localisation measures for regional digital integration and regulatory harmonisation.

Kenya's data protection framework is governed by the Data Protection Act (DPA), 2019 and the Data Protection (General) Regulations, 2021, which establish a conditional model for cross-border transfers based on adequacy, appropriate safeguards, consent, and public interest considerations (DPA 2019, ss. 48–50). Rwanda, under Law No. 058/2021 on the Protection of Personal Data and Privacy, adopts a more security-structured regime that incorporates prior authorisation mechanisms and broader regulatory oversight in relation to international transfers (Law No. 058/2021, arts. 48–50, 52). While both

systems formally recognise cross-border data flows, they differ in the extent to which national security and localisation considerations are embedded within transfer authorisation structures.

The research problem addressed in this article is whether apparent convergence in adequacy-based transfer rules translates into substantive convergence in the operationalisation of legal standards governing national security restrictions and data localisation. The article specifically interrogates whether the data protection principles of necessity, proportionality, and regulatory discretion function as consistent constraints across both jurisdictions or whether they are mediated through institutional design in ways that produce divergent regulatory outcomes.

This inquiry is significant for three reasons. First, cross-border data transfers are central to digital trade, cloud computing, and regional integration initiatives, including the African Union's Digital Transformation Strategy for Africa (2020–2030) and the African Continental Free Trade Area (AfCFTA). Article 20(1) of the African Union Protocol on Digital Trade to the Agreement Establishing the African Continental Free Trade Area (2024) provides that "State Parties shall, subject to an Annex on Cross-Border Data Transfers, allow the cross-border transfer of data, including personal data, by electronic means, provided the activity is for the conduct of digital trade by a person of a State Party" (African Union, 2024, Article 20(1)). The Protocol further permits States to restrict cross-border data transfers where necessary to achieve a legitimate public policy objective or protect essential security interests (African Union, 2024, Article 20(2)).

Second, national security exceptions, particularly those relating to risks arising from foreign governmental access to personal data, are increasingly invoked as legal justifications for restricting data flows, contributing to regulatory fragmentation and uncertainty (Kuner, 2021; Gao, 2023; Tan, 2024).

Third, many African jurisdictions have adopted hybrid data protection frameworks influenced by

the European Union General Data Protection Regulation (GDPR) model while simultaneously adapting GDPR-derived norms to indigenous governance priorities, sovereignty concerns, and regional regulatory objectives (Abdulrauf, 2024; Ifeanyi-Ajufo, 2023; Greenleaf, 2021; Makulilo, 2016).

From a theoretical perspective, the article engages principles-based regulation in data protection law, with particular emphasis on necessity, proportionality, and regulatory discretion as interpretive and operational standards. Proportionality functions as a legal framing and analytical tool originating from the Basic Law for the Federal Republic of Germany (Grundgesetz), which is the German constitutional law based upon which Article 20(3) lays the framework for the interpretation of the principle of proportionality (Bundesverfassungsgericht, Apothekenurteil (Pharmacy Case), BVerfGE 7, 377 (1958)). The principle was reiterated in the Cannabis case/decision (Federal Constitutional Court of Germany in which the Court restated the principle of proportionality requiring that a restriction of a constitutional right be suitable, necessary, and proportionate in the strict sense (Bundesverfassungsgericht [BVerfG], 1994, 145 at p. 173). This principle was further constitutionalised in EU fundamental rights law, particularly through the Charter of Fundamental Rights, implying that interferences with data protection rights must be suitable and necessary in relation to legitimate aims (Charter of Fundamental Rights of the European Union, Article 52(1); Tranberg, 2011).

The principle of necessity, in its broad sense, requires that personal data be processed only to the extent required to achieve a legitimate purpose (Organisation for Economic Co-operation and Development [OECD], 2013, para. 8; Council of Europe, 2018, art. 5(4)(c); Bygrave, 2014). However, its practical application, intensity of review, and legal meaning are jurisdiction-specific and function as a boundary or limit requiring that restrictive measures be essential to achieve a legitimate objective. Regulatory

discretion, in turn, determines the extent to which supervisory authorities may interpret and apply these principles in practice.

In Kenya, the Data Protection Act permits cross-border transfers subject to ‘adequacy’, ‘security measures’ or ‘safeguards’, ‘consent’, and ‘public interest’ or security-related considerations, while conferring significant interpretive and enforcement discretion on the Data Commissioner through a framework of structured regulatory discretion (DPA 2019, ss. 49–52). This includes supervisory discretion over cross-border transfers (DPA 2019, s. 49), exemption-gatekeeping discretion in matters such as national security and public interest (DPA 2019, ss. 51–52), and rule-making and interpretive discretion through codes and guidance (DPA 2019, ss. 52–54).

Rwanda’s framework, by contrast, establishes a more structured authorisation-based regime in which the supervisory authority may approve, suspend, or prohibit transfers on specified grounds, including national security and public order considerations (Law No. 058/2021, arts. 48–49, 52). Unlike Kenya, Rwanda’s cross-border data transfer regime reflects a more explicit institutionalisation of security-based controls within its governance framework.

The central argument advanced in this article is that while Kenya and Rwanda demonstrate formal convergence in adopting adequacy-based cross-border transfer regimes, they diverge in the institutional design through which national security and data localisation controls are operationalised. Kenya’s legal framework reflects an ex-post, discretion-heavy enforcement model, whereas Rwanda adopts an ex-ante authorisation model that embeds security considerations into transfer approval structures. These differences significantly shape how principles of necessity, proportionality, and regulatory discretion are applied in practice.

The article contributes to the literature on African data protection law by demonstrating that statutory convergence does not necessarily produce operational convergence. Instead,

institutional design and the allocation of regulatory discretion play a decisive role in shaping the practical meaning of abstract legal principles. It further contributes to broader debates on digital sovereignty and cross-border data governance by showing how national security considerations may function both as exceptions and as structural determinants of data transfer regimes.

The article proceeds as follows: part one presents the introduction; part two is the methodological approaches and scope; part three is the conceptual and analytical framework, which is essentially the doctrinal framework governing cross-border data transfers; part four examines the Kenyan and Rwandan legal regimes individually; part five discusses the operationalisation of principles of necessity, proportionality, and discretion in the determination of national security, public interest in cross-border data transfers, part six provides a comparative assessment of convergence and divergence in their regulatory approaches, and lastly is the conclusion.

METHODOLOGICAL APPROACHES AND SCOPE

This study adopts a comparative doctrinal legal methodology to examine whether and to what extent Kenya and Rwanda converge or diverge in their regulation of national security and data localisation in the context of cross-border personal data transfers. The two regimes of Kenya and Rwanda are picked within the wider East African Community regulatory landscape based on their comparatively advanced data localisation legal frameworks. The legal regimes of these two countries offer a more comparable and practical footprint on how data-localisation conditions and national-security regulatory architecture, together with public interest, are governed and regulated beyond their national borders in transfers of data. The choice was further motivated based on relative transparency in the accessibility of relevant data for comparative elements of convergence and divergence as compared to other remaining jurisdictions. The primary analysis involves the systematic interpretation of primary

legal materials from two jurisdictions. Firstly, relevant primary sources of data for Kenya are the Kenya Data Protection Act, 2019 and the Kenya Data Protection (General) Regulations, 2021. Secondly, primary sources of data for Rwanda include Rwanda's Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy; Rwanda Law No. 26/2017 of 31 May 2017 Establishing the National Cyber Security Authority and Determining its Mission, Organisation and Functioning. The study also used additional guidance documents for regulatory interpretation, including the Kenya Guidance Note on Cross Border Data Transfers¹; Rwanda Data Protection and Privacy implementing guidance notes, registration and data controller/processor guidance on the portal, registration portal requirements, compliance notices, forms, circulars, administrative instructions, and guidance issued by the National Cyber Security Authority (NCSA) pursuant to Law No. 058/2021 available on the Rwanda NCSA website². These sources are supplemented, where relevant, by administrative determinations and judicial decisions to assess both the formal content of the law and its practical application. Secondary sources like journal articles and books discussing the data protection regimes under study are also used in support of an interpretive role in doctrinal and comparative legal analysis through contextualisation, identification of doctrinal debates, analytical framing, and gap filling.

By adopting a functional comparative approach, the study examines how each regime structures the conditions for cross-Border transfers of personal data, accommodates national security interests and public interest considerations, and incorporates explicit or implicit data localisation measures. Attention is paid to the legal rules governing cross-border transfers, the scope and operation of national security exceptions, and the

safeguards applicable when personal data moves beyond national borders.

The analysis is guided by three interpretive frameworks, namely the principles of necessity, proportionality, and regulatory discretion, to evaluate how limitations on data protection rights are justified, constrained, and implemented in practice. It further considers the role of consent as a transfer-enabling mechanism and the extent of discretionary authority vested in regulators and other competent state actors. These analytical frameworks provide a basis for assessing whether restrictions on cross-border data transfers are subject to meaningful legal constraints and accountability mechanisms. To maintain analytical focus, the article does not examine surveillance law, intelligence-gathering powers, or cybercrime enforcement regimes except where they directly affect the regulation of cross-border data transfers under data protection legislation.

Although a growing body of scholarship addresses data localisation, digital sovereignty, and cross-border data governance, little focus has been devoted to how East African data protection regimes operationalise national security exceptions within transfer frameworks or how such exceptions interact with principles of necessity, proportionality, and regulatory discretion. Kenya and Rwanda are examined through the foregrounded dimensions, and the study contributes to a deep understanding of emerging approaches to data governance in East Africa and within the broader framework of the African Union's Digital Transformation Strategy for Africa (2020–2030) and provides a doctrinal basis for assessing whether the two jurisdictions exhibit regulatory convergence or divergence in balancing data mobility and national security in cross-border data flows. This combination of contextual comparability and regulatory variation provides a useful basis for assessing convergence and divergence in data transfer governance.

¹Office of the Data Protection Commissioner. (n.d.). Guidance note on cross-border data transfer. Republic of Kenya. <https://www.odpc.go.ke/wp-content/uploads/2026/04/Guidance-Note-on-Cross-border-Data-Transfers.pdf>.

² National Cyber Security Authority (NCSA): FAQ: Frequently asked Questions on Personal Data Protection and Privacy (n.d). <https://cyber.gov.rw/updates/article/faq-personal-data-protection-and-privacy-law/>.

Understanding the regulatory interplay is essential because the African Union Protocol on Digital Trade to the Agreement Establishing the African Continental Free Trade Area (2024) provides that “State Parties shall allow the cross-border transfer of data, including personal data, by electronic means, provided the activity is for the conduct of digital trade by a person of a State Party.

CONCEPTUAL AND ANALYTICAL FRAMEWORK

Overview

This article develops a doctrinally grounded conceptual framework to structure the comparative assessment of how Kenya and Rwanda regulate cross-border personal data transfers in the context of national security/public interest and data localisation. The framework is designed to operationalise the central research question of whether the two jurisdictions demonstrate convergence or divergence in their legal treatment of data mobility constraints. Rather than treating statutory provisions in isolation, the framework provides an evaluative conceptual model through which legislative texts, subsidiary regulations, and data protection authorities’ regulatory practice are interpreted and compared. The framework is anchored in three core interrelated doctrinal principles, namely: necessity, proportionality, and regulatory discretion, supplemented by the functional role of consent in legitimising cross-border data flows. These concepts are not treated as abstract theoretical constructs but as operational criteria for assessing the legal architecture governing data transfers under the Kenya Data Protection Act, 2019, the *Data Protection (General) Regulations, 2021*, and *Rwanda’s Law No. 058/2021 on the Protection of Personal Data and Privacy*. The framework sits within the existing literature gap on comparative studies on national security and data localisation studies in Africa, particularly in the East African Community jurisdictions of Kenya and Rwanda.

Literature Positioning

A growing body of scholarship on data protection in Africa has examined the rapid proliferation of national data protection statutes and their alignment with global normative models, particularly the EU General Data Protection Regulation (GDPR). Much of this literature emphasises regulatory convergence, institutional transplantation, and the emergence of data sovereignty as a response to the political economy of digitalisation in Africa (Greenleaf, 2021; Kuner, 2020). Within this strand, Kenya and Rwanda are frequently identified as leading jurisdictions in East Africa due to their relatively recent enactment of comprehensive data protection frameworks and their institutional commitment to regulatory oversight of personal data processing and digitalisation drive. However, while these studies provide valuable descriptive accounts of legislative development, they tend to prioritise macro-level themes such as regulatory harmonisation, digital trade, and governance capacity, rather than engaging in fine-grained doctrinal comparison of how specific legal principles operate in practice.

More recent African-centred scholarship has begun to interrogate the rise of data localisation and national security rationales within data governance frameworks, highlighting the increasing tendency of states to assert territorial control over data flows as part of broader digital sovereignty strategies (Makulilo, 2016; Greenleaf, 2021). Yet, even within this emerging literature, analysis often remains generalised, focusing on policy trends or continental regulatory trajectories rather than systematically examining how national security exceptions are structured, interpreted, and operationalised within specific jurisdictional contexts. There is a fairly limited comparative doctrinal engagement with how such exceptions function within cross-border data transfer regimes in Kenya and Rwanda, despite their prominence as regional regulatory leaders within the East African Community region.

This gap is especially evident in relation to the operationalisation of core data protection principles of necessity, proportionality, consent, and regulatory discretion within cross-border data transfer frameworks. While existing studies acknowledge that African data protection laws often incorporate these principles, they rarely examine how they are concretely embedded in decision-making structures governing cross-border transfers, particularly where national security considerations are invoked. For example, the discretion afforded to supervisory authorities in Kenya under the Data Protection Act, 2019, and the more formalised authorisation mechanisms under Rwanda's Law No. 058/2021 have not been systematically compared in terms of their practical implications for data mobility and restriction. Similarly, the interaction between consent-based transfers and overriding public interest or security exceptions remains underexplored in a comparative African context.

Accordingly, this article builds on and extends existing scholarship by undertaking a structured doctrinal comparison of Kenya and Rwanda through the analytical framework of necessity, proportionality, and regulatory discretion. It situates national security exceptions and data localisation tendencies not merely as policy choices, but as legally operational mechanisms embedded within statutory transfer regimes. In doing so, it addresses the underdeveloped area of comparative doctrinal analysis of African data protection systems, particularly with respect to how abstract principles are translated into regulatory practice in the governance of cross-border data flows.

Principles-based Regulation

Conceptually, principles-based regulation in data protection law is described as a regulatory approach that relies on high-level, technology-neutral principles and desired outcomes based on broad accountability, transparency, and adequacy standards rather than detailed, prescriptive rules (Black, 2008). It means organisations are expected to interpret and apply these principles to their specific circumstances and to demonstrate

compliance with the underlying objectives of the law. Based on the principles-based approach, the article provides a structured set of key concepts and analytical principles used to guide how a study interprets, evaluates, and connects legal or empirical phenomena to answer its research question. Firstly, the principle of necessity is employed as a baseline requirement for evaluating the legitimacy of restrictions imposed on cross-border data transfers. The principle of necessity requires that personal data be collected, used, or disclosed only to the extent required for a legitimate purpose and not in a manner that exceeds what is needed to achieve that purpose (Bygrave, 2014; Council of Europe, 2018, art. 5(4)(c); OECD, 2013, para. 8). This means data should not be collected or retained on unrelated subjects or excessive in relation to the legitimate purpose of processing. Even for Governments, any limitation on observing the data protection principles grounded in national security or public interest must be demonstrably connected to a legitimate objective and must not extend beyond what is required to achieve that objective. Within the comparative analysis in this study, the principle of necessity is used to interrogate whether national security exceptions operate as narrowly tailored safeguards or as broad enabling clauses that risk expanding state control over data flows. This conceptual perspective allows the study to distinguish between justified regulatory interventions and potentially overinclusive interferences or restrictions that may function as *de facto* localisation mechanisms.

Secondly, the principle of proportionality operates as the central balancing principle within the framework, providing a structured method for assessing whether restrictions on data transfers are excessive relative to their stated objectives. It is applied to evaluate whether the interference with data protection rights and cross-border data mobility is suitable, necessary, and balanced against competing interests such as national security and regulatory sovereignty. In doing so, proportionality enables a comparative assessment of the intensity of regulatory interference in each jurisdiction and whether safeguards exist to

prevent disproportionate curtailment of data flows. It also provides a bridge between formal legal standards and their practical application by regulatory authorities.

Thirdly, regulatory discretion constitutes a third analytical lens through which the study examines the institutional design of data protection governance in both jurisdictions. It refers to the scope of decision-making authority granted to data protection authorities and other competent state actors in authorising, restricting, or exempting cross-border transfers. The framework assesses whether such discretion is structured by clear statutory criteria or whether it is broadly framed, thereby allowing expansive interpretive authority. Closely related to this is the role of consent as a legal basis for cross-border data transfers. While consent is formally recognised as a legitimising mechanism, the framework critically evaluates its effectiveness in contexts where regulatory overrides, public interest grounds, or national security exceptions may limit its practical significance.

Fourthly, data localisation is defined as the practice of keeping data within the region or territory it originated from. (Cloudflare, n.d., para. 1).³ For example, if entities or organisations collect data in Kenya or Rwanda, they store it in Kenya or Rwanda rather than transferring it to another country for processing. The foregoing analytical mirror collectively supports a structured comparative inquiry into convergence and divergence. Convergence in data protection regimes is understood as the presence of substantively similar legal standards and operational outcomes in the governance of cross-border data transfers, even where statutory wording differs. (Greenleaf, 2021). However, Kuner (2020) argues that convergence means functionally comparable personal data protections and governance outcomes rather than complete uniformity of substantive legal standards; hence, it is a continuing regulatory diversity rather than

strict substantive convergence (Kuner, 2011; Kuner, 2013; Svantesson, 2014).⁴ Divergence, by contrast, refers to differences in legal thresholds, institutional design, enforcement intensity, or the practical application of regulatory powers that result in materially distinct regulatory environments (Harbinja, 2023; Sucker & Beyleveld, 2024). Some studies have suggested that regulatory divergence arises from differing national approaches to data localisation, privacy, and cybersecurity due to evident pluralistic and fragmented tendencies in global data governance trends (Coche, Kolk & Ocelík, 2024). Such pluralistic and fragmented data governance regimes provide leeway for national priorities in data privacy, security interests, and strategic national interests in data governance, thus impacting cross-border data flows. In other words, divergence is conceptualised as a normative decoupling of transfer rules, more particularly through altered standards of adequacy and sovereignty-driven redesign of data export controls.

Although a growing body of scholarship addresses data localisation, digital sovereignty, and the governance of cross-border data flows, relatively limited attention has been devoted to the doctrinal operationalisation of necessity, proportionality, and discretion within African data protection regimes, particularly focusing on comparative analysis of East African regimes of Kenya and Rwanda. More particularly, limited attention has been paid to how national security exceptions and data localisation are structured and operationalised within cross-border data transfer regimes in Kenya and Rwanda in the context of the outlined analytical lens. This article addresses this gap by embedding these analytical principles within a unified evaluative framework capable of systematically comparing statutory design and regulatory practice.

In sum, the conceptual framework provides the model of analysis for the study by translating

³ Cloudflare. (n.d.). What is data localization? Cloudflare Learning Centre. Retrieved June 16, 2026, from

<https://www.cloudflare.com/learning/privacy/what-is-data-localization>

4

abstract legal principles into operational criteria for doctrinal comparison. It enables a disciplined evaluation of how Kenya and Rwanda mediate the tension between data mobility and national security, thereby facilitating a structured determination of whether their regulatory approaches reflect convergence, divergence, or a hybrid form of regulatory alignment in the governance of cross-border personal data flows.

LEGAL FRAMEWORK FOR CROSS-BORDER DATA TRANSFERS

Kenya Cross-Border Data Transfer Model: National Security and Data Localisation

Kenya regulates cross-border personal data transfers through a combination of the Data Protection Act, 2019 (DPA) and the Data Protection (General) Regulations, 2021 (General Regulations). These instruments establish the legal conditions under which personal data may be transferred outside Kenya while ensuring that transferred data remains subject to protections consistent with Kenyan data protection standards. The framework is administered by the Office of the Data Protection Commissioner (ODPC), which is responsible for overseeing compliance with the Act and its subsidiary legislation.

The statutory basis for cross-border transfers is contained in Part VI of the Data Protection Act. Section 48 provides that a data controller or data processor may transfer personal data outside Kenya only where proof of appropriate safeguards has been established or where one of the lawful transfer conditions recognised by the Act applies. The provision establishes the general principle that international transfers are permissible but subject to compliance with statutory requirements designed to protect personal data once it leaves Kenyan territory (DPA, 2019, s. 48).

While section 49 focuses on cross-border personal data transfer, governing the legality and security of outbound transfers and regulatory oversight, section 50 empowers the Cabinet Secretary to

require that certain categories of processing, such as those with bearing on strategic interests of the state, be carried out only through a server or data centre located in Kenya, underscoring the limited degree of data localization regime/ data sovereignty. The data guidance note on cross-border data transfer issued by the Office of the Data Protection Commissioner (ODC) defines data localisation as *‘the regulatory requirement that data about a nation’s citizens or residents is initially collected, processed or stored within the boundaries of a particular “jurisdiction”, such as a country or a geographic region like a regional economic community or bloc’* (ODC, Data Guidance Note, (n.d.) Clauses 1, 10.0).⁵ Further, the data guidance note on cross-border data transfer reinforces section 50 of the DPA, 2019 that requires personal data for the strategic interests of the state to be domiciled in Kenya (ODC, Data Guidance Note, (n.d.) Clauses 10.0). The regulation of outbound transfers recognises several lawful transfer mechanisms which include transfers to jurisdictions that provide an adequate level of protection, transfers based on appropriate safeguards, transfers authorised through the consent of the data subject, and transfers justified by necessity in circumstances recognised by law. Together, these provisions establish a conditional transfer regime that permits international data flows while requiring controllers and processors to demonstrate compliance with prescribed legal standards (DPA, 2019, ss. 49–50).

The detailed operational rules governing cross-border transfers are contained in Regulations 40–49 of the Data Protection (General) Regulations, 2021. For example, Regulation 40 requires a data controller or processor transferring personal data outside Kenya to ensure that the transfer is based on one of the lawful mechanisms recognised under the Act and Regulations. The Regulations recognise four principal transfer mechanisms: adequacy-based transfers, transfers subject to appropriate safeguards, transfers based on consent, and transfers justified by necessity or

⁵ Office of the Data Protection Commissioner. Guidance Note on Cross Border Data Transfer (n.d), Clauses 1, 10.0). [https://www.odpc.go.ke/wp-](https://www.odpc.go.ke/wp-content/uploads/2026/04/Guidance-Note-on-Cross-border-Data-Transfers.pdf)

[content/uploads/2026/04/Guidance-Note-on-Cross-border-Data-Transfers.pdf](https://www.odpc.go.ke/wp-content/uploads/2026/04/Guidance-Note-on-Cross-border-Data-Transfers.pdf)

public interest (Data Protection (General) Regulations, 2021, reg. 40).

Adequacy-based transfers are addressed principally in Regulations 41 and 42. These provisions permit transfers where the receiving jurisdiction, organisation, or recipient affords a level of protection that is considered adequate for the protection of personal data. In determining adequacy, consideration may be given to factors including the legal framework applicable in the destination jurisdiction, the existence of enforceable rights, available remedies, and measures protecting personal data from unlawful access or misuse (Data Protection (General) Regulations, 2021, regs. 41–42).

The Regulations also recognise transfers based on appropriate safeguards. Under this mechanism, personal data may be transferred where contractual arrangements, binding corporate rules, codes of conduct, certification mechanisms, or other legally recognised safeguards ensure the continued protection of personal data following transfer. These safeguards are intended to maintain data protection standards irrespective of the jurisdiction in which the data is subsequently processed (Data Protection (General) Regulations, 2021, regs. 43–44).

Consent constitutes a further lawful basis for transfer. The Regulations permit transfers where the data subject has explicitly consented to the proposed transfer after being informed of the potential risks associated with transferring data to a jurisdiction that may not provide an equivalent level of protection. Consent therefore operates as a recognised legal mechanism through which cross-border transfers may occur in circumstances prescribed by law (Data Protection (General) Regulations, 2021, reg. 46).

The Kenyan framework also incorporates necessity and public-interest grounds as lawful bases for international transfers. Regulation 45 permits transfers where they are necessary for important reasons of public interest recognised under Kenyan law. Additional provisions permit transfers where necessary for the establishment,

exercise, or defence of legal claims, the protection of vital interests, or other circumstances recognised by the Act and Regulations (Data Protection (General) Regulations, 2021, regs. 45–49). These provisions form part of the broader statutory architecture through which the law accommodates public functions and governmental interests within the regulation of cross-border data flows.

National security considerations are incorporated into the legal framework principally through the exemption provisions contained in the Data Protection Act. The DPA exempts certain processing activities from specified data protection obligations such as data protection principles relating to lawful processing, minimisation of collection, data quality, and adopting security safeguards to protect personal data where such processing is strictly necessary and undertaken for reasons of national security or public interest (DPA, 2019, section 51(2(b))). The term national security is defined in the Constitution of Kenya as the ‘*protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests*’ (Constitution of Kenya, 2010, art. 238(1)). Although the provision is not confined to cross-border transfers, it forms part of the broader legal context within which international transfers involving security-related considerations may occur. The element of State security is further reflected in the practice ‘Guidance Note on Cross Border Data Transfer’ issued by the Office of the Data Protection Commissioner, which makes definition of ‘strategic interest of the state’ in the context of cross-border transfers to mean processing activities which form part of a States’ interest that are important for the security, economic prosperity, or influence of a nation and that require data localisation (ODC, Data Guidance Note (n.d.) Clauses 1, 10).

The Act further recognises the role of public interest in limiting the application of certain data protection obligations, which generally justify the

processing of personal data in the public interest, especially lawful processing of personal data⁶. Also, a justification for processing of sensitive health data is provided under section 46(2)(a). However, ‘public interest’ in the context of cross-border data transfers appears in section 48(1)(c)(iii) of the DPA, which explicitly allows transfer where necessary for any matter of public interest.

The term ‘public interest’ is not specifically defined under the Data Protection Act. However, again, the Guidance Note on Cross Border Data Transfer issued by the Office of the Data Protection Commissioner defines ‘Public Interest’ as a collective well-being and the common good of all citizens. This being a practice guidance, it does not offer a final authentic interpretation. Kenya has no settled legal definition of what constitutes ‘public interest’ in the context of data protection principles. Instead, jurisprudentially, the courts have interpreted the concept in general terms as referring to the general welfare of the public and matters in which the public or community as a whole has a stake beyond an individual (*Steyn v. Ruscone*, 2013, para. 41; *Samuel Kerosi Ondieki v. National Hospital Insurance Fund Board of Management*, 2012, para. 14). This interpretation equates to the definition issued under the Guidance Note issued by the ODC.

However, in the context of cross-border (international) data transfers, there is limited judicial guidance publicly available interpreting the phrase ‘public interest’ grounds for bypassing compliance with the principles of data protection entrenched under section 48(1)(c)(iii) of the DPA 2019. Nonetheless, under the DPA, the concept of ‘public interest’ in combination with the necessity-based transfer provisions contained in the Kenya Data Protection (General) Regulations, 2021 creates exemptions to comply with the principles of data processing, protection, consent, and transfer. It provides a legal basis through which public authorities and other actors may rely on security-related or public-interest

considerations when processing or transferring personal data under circumstances prescribed by law (DPA, 2019, ss. 48(c)(iii), 51; Data Protection (General) Regulations, 2021, reg. 45).

As observed in the framing of the statutory provision (section 50), the Kenya data protection regime does not provide or impose a general, wholesale mandatory specific statutory data localisation requirement for all personal data to be stored in Kenya; instead, it provides for data processing through a data server or data centre in Kenya where data involve state interests. In other words, the Kenyan regime relies primarily on a statutory adequacy model and sectoral/policy tendencies, wherein sections 48 and 49 permit cross-border transfers of personal data subject to safeguards, adequacy considerations, consent (for sensitive personal data), and other conditions. These provisions indicate that the DPA generally allows outbound data transfers rather than requiring universal localisation.

While the Kenyan legal framework does not impose a general requirement that personal data be stored or processed exclusively within Kenya, it contains several mechanisms that preserve regulatory oversight over data transferred abroad. The adequacy requirements, safeguard obligations, contractual protections, and transfer conditions contained in the Act and Regulations collectively ensure that personal data transferred outside Kenya remains subject to protections consistent with Kenyan data protection standards. Through these mechanisms, the framework seeks to maintain continuity of protection irrespective of the geographical location of processing.

Compliance with cross-border transfer obligations is supervised by the Office of the Data Protection Commissioner. The Commissioner is empowered to monitor compliance, investigate complaints, conduct inspections, issue enforcement notices, and impose administrative sanctions in accordance with the DPA and the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 (regs.4–21).

⁶ See DPA, 2019 ss.30(1)(b); 46(2)(a); 51(2)(b); 52(1)(b).

Accordingly, Kenya's cross-border transfer regime is characterised by a statutory framework that permits international transfers through recognised legal mechanisms while embedding public-interest, national-security, and accountability considerations within the broader architecture of data protection regulation.

Rwanda's Cross-Border Personal Data Transfer Framework

Rwanda's cross-border personal data transfer framework is principally established under Articles 48–52 of the Law relating to the Protection of Personal Data and Privacy. Collectively, these provisions regulate the transfer of personal data outside Rwanda through a framework built around three interrelated elements. First, the law establishes substantive legal grounds upon which personal data may be transferred across borders. Second, it entrusts supervisory oversight of data processing and cross-border transfers to the National Cyber Security Authority (NCSA). Third, it imposes statutory requirements concerning the storage and protection of personal data, including data localisation obligations. Together, these provisions constitute the core legal framework governing international transfers of personal data from Rwanda.

The substantive legal bases for cross-border data transfers are principally set out under Article 48. Under Article 48(1), Rwanda adopts a prior authorisation-based transfer regime whereby a data controller or data processor may transfer personal data outside Rwanda only after obtaining prior authorisation from the supervisory authority upon demonstrating the existence of appropriate safeguards for the proposed transfer. The provision therefore subjects international transfers to ex-ante regulatory approval. In addition, Article 48(2) establishes a consent-based transfer mechanism by permitting transfers where the data subject has provided explicit consent. However, the existence of consent does not displace the broader statutory framework governing cross-border transfers or the supervisory role exercised by the competent authority.

Article 48(3) further permits cross-border transfers without prior authorisation where such transfers are justified on grounds of necessity. The provision recognises a range of circumstances in which transfers may occur, including where they are necessary for the performance of a contract, the establishment, exercise, or defence of legal claims, the protection of vital interests, the pursuit of legitimate interests subject to appropriate safeguards, public-interest considerations, or obligations arising under international treaties ratified by Rwanda. Consequently, Article 48 establishes three principal transfer mechanisms within Rwanda's legal framework: authorisation-based transfers, consent-based transfers, and necessity-based transfers.

The institutional framework supporting these transfer mechanisms is established through Articles 3, 27, and 28 of the Law. Article 3 defines the “supervisory authority” as the authority responsible for supervising compliance with the Law on Personal Data Protection and Privacy. Under the Law, this authority is the National Cyber Security Authority (NCSA), established under the Law establishing the National Cyber Security Authority in Rwanda (Law No. 26/2017, art. 3). The designation of the NCSA as the supervisory authority is consistently reflected throughout the legislation, including Articles 48 and 49, which require prior authorisation from the supervisory authority for transfers of personal data outside Rwanda.

The supervisory responsibilities of the NCSA are elaborated under Article 27. Under this provision, the Authority oversees implementation of the data protection framework, responds to requests for opinions concerning personal data processing, informs data subjects, controllers, processors, and third parties of their rights and obligations, maintains the register of data controllers and processors, investigates complaints relating to personal data processing, receives and considers appeals from data subjects, advises on matters concerning personal data protection and privacy, and cooperates with national and foreign authorities on data protection matters. These

functions position the NCSA at the centre of Rwanda's data protection governance framework.

Article 28 further reinforces the Authority's regulatory role. Pursuant to Article 28(1), the NCSA may issue registration certificates to data controllers and processors. Article 28(2) mandates the Authority to ensure compliance with the Law, while Article 28(3) requires it to establish regulatory mechanisms ensuring that ICT systems do not threaten privacy and public freedoms. The Authority is additionally empowered under Article 28(4) to develop subsidiary regulations relating to the application of the Law and, under Article 28(5), to issue regulations necessary for implementation and impose administrative sanctions. The combined effect of Articles 3, 27, and 28 is the creation of a supervisory model in which substantial regulatory and administrative functions are concentrated within the NCSA.

A notable feature of Rwanda's implementation framework is that the legislation does not establish a separate and standalone Data Protection Authority comparable to Kenya's Office of the Data Protection Commissioner or the independent national data protection authorities operating within the European Union. Although the legislation repeatedly refers to the "supervisory authority", it does not contain an express provision stating that "there is hereby established a Data Protection Authority" or "there is hereby established a Data Protection and Privacy Office". Rather, data protection oversight is institutionally integrated within the broader structure of the NCSA.

In addition to regulating transfers, the Law imposes requirements relating to the storage of personal data. Article 50 requires data controllers and data processors to store personal data within Rwanda. The provision effectively establishes domestic storage as the default position and permits storage outside Rwanda only under specified conditions. Particularly, offshore storage is permitted where a data controller or data

processor possesses a valid registration certificate authorising the storage of personal data outside Rwanda. Such certificates are issued by the supervisory authority pursuant to Article 50. However, the legislation does not expressly specify the circumstances or criteria under which such certificates may be granted. As a result, the legal basis upon which offshore storage authorisations are issued remains largely dependent upon administrative determination by the supervisory authority.

At the operational level, Rwanda's cross-border transfer framework is implemented through the Standard Contractual Clauses (SCCs) issued in February 2024 by the Data Protection and Privacy Office operating under the NCSA.⁷ The SCCs constitute a binding transfer mechanism and operationalise Article 49 of Law No. 058/2021 through Clauses 1–12 and Annexes I and II. The instrument requires parties to execute written transfer agreements, implement technical and organisational safeguards, comply with breach-notification obligations relating to cross-border transfers, and observe data-minimisation and purpose-limitation requirements. In functional terms, the Rwanda SCCs perform a role broadly analogous to GDPR-style SCCs in facilitating and regulating international transfers of personal data.

The practical operation of the authorisation regime is further illustrated through the official application form for cross-border transfers issued under the Republic of Rwanda National Cyber Security Authority. The form identifies the Data Protection and Privacy Office as the responsible administrative office and requires the applicant, as data controller, to provide detailed information concerning the proposed transfer. Under Section 1 of the application form, the applicant must provide details relating to the data controller seeking authorisation. Section 2 requires disclosure of the categories of personal data to be transferred outside Rwanda, including the categories of data subjects concerned,

⁷National Cyber Security Authority (Data Protection and Privacy Office) February 2024). Standard Contractual Clauses

(SCCs).<https://dpo.gov.rw/fileadmin/DPO/ComplianceTools/Standard%20Contractual%20Clauses%20for%20Transfer>.

descriptions of the personal data involved, the purpose of the transfer, the dataset size or volume, and the legal ground relied upon for the transfer.

The application process further requires disclosure of the safeguards adopted to protect personal data during and after transfer. Applicants must indicate the format in which the data will be transferred, including whether the information will be encrypted, transferred as raw data, or transmitted in another form. Data controllers and data processors acting on behalf of controllers must also identify the safeguards, security measures, and protection mechanisms implemented prior to transfer, together with details concerning the intended recipient and the purpose of the transfer. In addition, applicants must specify the technical and organisational measures that will be implemented by the recipient to ensure the protection of personal data once it has been transferred outside Rwanda.

Notwithstanding the relative comprehensiveness of the statutory framework, certain aspects of Rwanda's transfer regime remain underdeveloped from a regulatory perspective. Although Law No. 058/2021 establishes the substantive legal basis governing cross-border transfers, Rwanda has not, at least publicly, adopted detailed subsidiary regulations comparable to Kenya's Data Protection (General) Regulations, 2021, which prescribe transfer assessment criteria, authorisation procedures, adequacy methodologies, a guidance notice on cross-border data transfers, and transfer impact assessment requirements. This regulatory gap is also reflected in the transfer application form, which does not expressly indicate the specific provision of the principal legislation or subsidiary regulations under which the application process is established. Consequently, while the framework provides substantive legal grounds for cross-border transfers and establishes institutional mechanisms for supervision and authorisation, aspects of its operational implementation remain dependent upon administrative discretion and practice. Concerns intersect with cross-border

data flows⁵. Operationalisation of Necessity, Proportionality, and Discretion

OPERATIONALISATION OF NECESSITY, PROPORTIONALITY, AND DISCRETION

Kenya: National Security, Public Interest, and Cross-Border Data Transfers

The Data Protection (General) Regulations, 2021 operationalise the cross-border transfer provisions contained in sections 48–50 of the Data Protection Act, 2019 by establishing four legal bases for international transfers: adequacy decisions, appropriate safeguards, necessity, and consent. Regulation 40 requires a transferring entity to demonstrate that any transfer of personal data outside Kenya is grounded in one of these recognised bases, thereby creating a structured framework for outbound data transfers. This approach reflects an attempt to balance data mobility with regulatory oversight while preserving room for public-interest and national-security considerations. However, the extent to which the framework constrains administrative discretion remains open to question.

A notable feature of the Regulations is the treatment of necessity as an independent legal basis for transfer. Regulation 45 permits transfers where they are “strictly necessary” for purposes contemplated under section 48(c) of the Act and further requires that no fundamental rights and freedoms of the data subject override the public interest necessitating the transfer. On its face, this provision incorporates elements of both necessity and proportionality by requiring a connection between the transfer and a legitimate objective while recognising competing rights interests. Nevertheless, neither the Act nor the Regulations define the circumstances under which public interest or national security considerations become sufficiently compelling to justify a transfer. The absence of statutory criteria creates uncertainty regarding the threshold for invoking these exceptions and leaves significant interpretive authority to regulators and transferring entities. As a result, necessity is recognised as a legal principle but is only partially operationalised through objective benchmarks.

The Regulations also reveal a strong reliance on administrative and private-sector assessments. Regulation 41 allows transfers based on “appropriate safeguards” where a controller concludes, after assessing the circumstances of the transfer, that adequate protection exists. While documentation requirements promote accountability, the provision does not prescribe a detailed methodology for determining adequacy or risk. This approach affords flexibility but simultaneously expands regulatory discretion by permitting substantial evaluative judgments without clearly articulated standards. Consequently, predictability may depend less on the text of the law and more on subsequent guidance issued by the Office of the Data Protection Commissioner (ODPC).

Public-interest exemptions under Regulations 55–57 further illustrate this tension. The Regulations identify several legitimate grounds, including the protection of public health, prevention of serious threats to life or safety, and action in response to suspected unlawful conduct. Although these provisions provide greater specificity than the Act itself, they remain broad and are not accompanied by explicit proportionality tests or procedural safeguards governing their invocation. Unlike some comparative regimes that require documented balancing exercises or independent authorisation for exceptional transfers, the Kenyan framework assumes that compliance with the stated grounds is sufficient. This creates the possibility that public-interest justifications may be interpreted expansively, particularly where national security concerns are implicated.

In the view of regulatory discretion, the framework exhibits a predominantly ex-post model of regulation. Data controllers and processors are authorised to proceed with transfers provided they can demonstrate ongoing compliance with the statutory bases. The Data Commissioner retains investigative and enforcement powers, but the Regulations do not establish a dedicated approval process for transfers invoking public-interest or national-security grounds. This distinguishes the Kenyan

model from systems that require prior regulatory authorisation and places considerable reliance on post-transfer review. While such an approach may facilitate innovation and data mobility, it also increases the importance of transparent enforcement practices and published guidance to ensure consistency in decision-making.

The availability of review and remedies provides an important, albeit incomplete, safeguard against arbitrary decision-making. Decisions of the Data Commissioner are generally subject to challenge through the statutory mechanisms established under the Data Protection Act and through judicial review before the courts. This contributes to transparency and legal conformity. However, the Regulations themselves provide limited procedural guidance on how national-security or public-interest determinations should be documented, reviewed, or challenged. Consequently, although remedies formally exist, the transparency and predictability of decision-making depend significantly on administrative practice rather than on detailed regulatory criteria.

Sections 51 and 52 of the Data Protection Act, 2019 provide the principal statutory foundation through which national security and public-interest considerations may influence the operation of Kenya’s cross-border data transfer regime. Although neither provision expressly regulates international transfers, both operate as limitation clauses that qualify the application of ordinary data protection obligations where overriding state interests arise. Section 51 exempts certain processing activities from aspects of the Act where such processing is undertaken for purposes relating to national security, defence, public security, or the prevention, detection, investigation, and prosecution of offences (Data Protection Act, 2019, s. 51). Read together with the Act’s transfer provisions under sections 48–50 and Regulations 40–49 of the Data Protection (General) Regulations, 2021, this exemption creates a direct statutory basis upon which cross-border transfers may be restricted, conditioned, or subjected to strict examination where security interests are involved.

Section 52 of the DPA extends this architecture by recognising broader public-interest grounds capable of limiting the exercise of data protection rights and obligations. While framed principally as an enforcement and exemption provision, it reinforces the legislative objective of ensuring that data protection does not undermine important governmental functions, including regulatory, judicial, and public-administration interests (Data Protection Act, 2019, s. 52). In practical terms, these provisions confer significant interpretive authority on the Office of the Data Protection Commissioner in determining the extent to which security or public-interest considerations justify departures from ordinary transfer safeguards. Such flexibility enables regulatory responsiveness to evolving security threats and public policy concerns. However, the breadth of the statutory language also creates potential for expansive administrative intervention, particularly because neither the Act nor the Regulations prescribe detailed criteria governing when national security or public-interest concerns become sufficiently compelling to justify limitations on cross-border data flows. The provisions therefore establish a legally recognisable basis for transfer restrictions while simultaneously positioning regulatory discretion as a central feature of Kenya's data transfer governance framework.

Overall, the Kenyan Regulations demonstrate partial adherence to the principles of necessity, proportionality, accountability, and reviewability. Necessity is expressly recognised, and proportionality is implicitly reflected through references to fundamental rights and public interest. However, the framework lacks detailed benchmarks for assessing national security and public-interest claims, resulting in a relatively broad sphere of regulatory and administrative discretion. The consequence is a transfer regime that is legally structured but not fully constrained by clear, objective, and consistently reviewable standards. This creates the potential for regulatory uncertainty, particularly where national security concerns intersect with cross-border data flows.

Rwanda: National Security, Public Interest, and Cross-Border Data Transfers

In Rwanda's cross-border data transfer regime under Law No. 058/2021, national security and data localisation operate as interlocking control mechanisms, both facilitated by the National Cyber Security Authority (NCSA) as the supervisory authority. At a structural level, data localisation (Article 50) creates a default expectation that personal data remains within Rwanda unless the NCSA authorises external storage or transfer. This gives the state a territorial baseline of control over data (data sovereignty). In parallel, national security and public interest clauses (especially Articles 48 and 52) function as broad justification grounds that allow restriction, retention, or conditioning of cross-border flows where state interests are implicated. The principles of necessity and proportionality are present in the statutory language (particularly through "necessity-based" transfer grounds and public interest limitations), but they are not operationalised through detailed statutory tests or structured balancing criteria. Instead, they are largely embedded as open-textured legal standards. This is where the role of the NCSA becomes decisive. The authority exercises high regulatory discretion in determining whether a transfer is justified under necessity or public interest grounds, whether safeguards are sufficient, whether localisation exceptions should be granted, and whether security concerns justify restriction or approval. The exercise of discretion is not predictable.

Because the law provides limited granular benchmarks, the application of necessity and proportionality is institutionally overseen rather than controlled or supervised by means of rules. In other words, these principles function more as decision-making language for the regulator than as strict legal tests that tightly structure outcomes. Criteria for outcomes are not stipulated. Consent operates as an independent legal basis for transfer, but its practical weight is moderated by the fact that consent can be bypassed or overridden through public interest and national security

justifications, and transfers often still require contractual safeguards or regulatory approval.

Consequently, the legal provisions on cross-border data transfer (Arts. 48-52) under Rwanda law do not comprehensively specify in the law or officially published regulation the type, nature or format of documents which must accompany an application for cross-border data transfer. The law is equally silent on how adequacy is evaluated because no adequacy benchmarks or criteria are provided in the law. If it concerns data security considerations, there are no clear benchmarks that must be established to have been fulfilled. There is no specific provision or publicly available regulation stipulating technical and organisational measures that are to be met to qualify as sufficient measures.

While data transfer may be decided based on national security concerns, the law does not provide benchmarks or granular criteria for evaluating grounds given as having met the criteria for national security consideration, much as the criteria are non-existent in any publicly available published law or regulations. While the principle of proportionality is a vital determinant of cross-border transfer, the law remains opaque on how proportionality should be evaluated as falling within the ambit of the data protection law. Data transfer has a purpose, mainly pegged to cross-border businesses and digital trading, which demand speed, precision, and predictable timelines for cross-border data transfer approvals. The time frame for data transfer is also not provided in the law, and no regulation has been published setting procedures, processes, timelines, and a feedback mechanism.

Incidentally, the applicant for cross-border data transfer (the data controller) determines the purposes, means of processing, and bears primary accountability for the transfer. The specific form of data transfer authorisation exists under the Republic of Rwanda National Cyber Security Authority portal but does not cite any law under

which the application form is made.⁸ The application form shows the sub-office as the data protection and privacy office. The application for cross-border transfer of data application form requires details of the Applicant (data controller) of personal data to be transferred outside Rwanda to be supplied for decision on authorisation to transfer personal data outside Rwanda (Section 1: Application Form). The application form must show details of the personal data to be transferred outside Rwanda category (Section 2: Application Form). These details are to be supplied under the categories of “data subjects”, “description of personal data to be transferred”, “purpose of transferring”, “dataset size/volume”, and “ground for transferring”.

In the section requiring details of protection for personal data to be transferred, the applicant (data controller) is required to indicate what is the format of personal data to be transferred, either encrypted, raw data, or other forms. The transfer form requires Data controllers or Data processors on behalf of data controllers to put in place clear safeguards, security measures, and mechanisms to implement the protection of personal data. This includes requiring the data controller applying for transfer of data to provide details to the entity (NCSA) deciding whether personal data should be transferred, to whom it will be transferred, and for what purpose. All these elements lack a legal foundational provision or regulation upon which they are based.

Regarding how the data controller plans to send/transfer personal data to recipients, the applicant for transfer of personal data outside Rwanda must supply to the data controller or Data processor clear details of what safeguards, security measures, and mechanisms have been implemented to protect personal data before sending the data outside Rwanda. Accordingly, the recipient must indicate clear technical and organisational measures in place to protect

⁸ National Cyber Security Authority, Data Protection & Privacy Office. (n.d.). Application form: Authorization to transfer personal data outside Rwanda. Republic of Rwanda.

<https://dpo.gov.rw/fileadmin/DPO/Services/application-form-for-external-transfer-authorization.pdf>.

personal data once it has been received abroad. (Section 5: Application Form).

The weakness in Rwanda's framework is that Law No. 058/2021 contains the substantive legal basis for cross-border transfers, but there are no publicly issued detailed subsidiary regulations comparable to Kenya's Data Protection (General) Regulations, 2021 that granularly prescribe the transfer assessment criteria, application procedures, adequacy methodology, or transfer impact assessment requirements. Even the Data transfer form does not state under which legal provisions of the Regulation or the principal law or subsidiary legislation it is made.

Further, there are no rules on appeal procedures specific to cross-border data transfer authorisations. This means that the framework provided under Articles 48–52 remains wanting in specific granular details. These gaps can well be filled in by the mandated authority issuing subsidiary legislation or ministerial orders; supervisory authority rules/regulatory authority guidelines, adequacy regulations, transfer authorisation guidelines, or any other framework that makes the implementation get out of regulatory opacity. This should also apply to national security, public interests, and the framework of discretionary exercise of powers under the principles of necessity and proportionality.

Overall, the framework is strong in state control and policy flexibility, but weaker in procedural precision and constraint of discretion. The interaction between localisation, security exceptions, and supervisory authority powers produces a system that is coherent in structure but highly regulator-dependent in operational uncertainty, with necessity and proportionality functioning more as guiding principles than enforceable constraints due to the absence of granular details on criteria justifying necessity and proportionality in deciding national interest or public interest considerations.

COMPARATIVE ASSESSMENT: CONVERGENCE OR DIVERGENCE?

The data presented in parts four and five above have shown that Kenya and Rwanda exhibit a significant degree of formal convergence in the regulation of cross-border personal data transfers. Both jurisdictions adopt a conditional transfer model grounded in the principles-based model that personal data may leave the national territory only where adequate protection or equivalent safeguards accompany the transfer. Kenya's framework, established under sections 48–50 of the Data Protection Act, 2019 and Regulations 40–49 of the Data Protection (General) Regulations, 2021, permits transfers based on adequacy, appropriate safeguards, consent, and necessity-based exceptions. Similarly, Rwanda's Law No. 058/2021 permits transfers where appropriate safeguards exist, where the data subject consents, or where specified necessity and public-interest grounds apply (arts. 48–49). In both systems, therefore, cross-border data transfers are neither prohibited nor unrestricted; they are conditioned upon legal mechanisms intended to ensure continuing protection of personal data beyond national borders. Both regimes further recognise consent as a lawful transfer basis and incorporate public-interest and necessity-related exceptions, reflecting a broadly comparable regulatory logic influenced by contemporary international data protection standards.

Underlying this formal convergence, in any case, notable substantive divergence emerges in three areas: security governance, localisation statutory scheme, and institutional discretion. First, Rwanda adopts a more security-centred transfer regime. National security and public-interest considerations are integrated directly into the transfer regime through Articles 48 and 52, while the National Cyber Security Authority (NCSA) exercises prior authorisation powers over transfers and offshore data storage. On the other hand, Kenya addresses national security primarily through exemption provisions under sections 51 and 52 of the Data Protection Act where national

security interests are at stake. Security considerations therefore operate more indirectly, as limitations on data protection obligations rather than as an embedded transfer-authorisation mechanism.

Second, the two jurisdictions diverge sharply on data localisation. Rwanda's Article 50 establishes a clear ex-ante territorial governance rule requiring all personal data to be stored in Rwanda unless the supervisory authority issues a valid registration certificate authorising cross-border data storage. Kenya contains no equivalent statutory localisation requirement. Instead, territorial control is pursued indirectly through adequacy assessments, safeguard obligations, and accountability requirements applicable to outbound transfers. Rwanda therefore adopts an explicit localisation model, whereas Kenya embraces a transfer-enablement model subject to protective conditions.

Third, institutional design reveals differing approaches to regulatory discretion. Rwanda employs an ex-ante model in which the NCSA functions as a cross-border data transfer gatekeeper with authority to authorise, condition, or prohibit transfers before they occur. Kenya relies predominantly on an ex-post compliance model administered by the Office of the Data Protection Commissioner through oversight, investigations, and enforcement powers. Consequently, discretion in Rwanda is concentrated at the authorisation stage, whereas in Kenya it is exercised primarily through supervision and enforcement.

Accordingly, the evidence suggests substantial formal convergence on principles but significantly operational divergence. While both jurisdictions embrace adequacy-oriented transfer frameworks and common safeguard mechanisms, they diverge in the intensity of security governance, the extent of localisation requirements, and the institutional allocation of regulatory discretion. The result is not convergence in regulatory outcomes but rather two distinct approaches to balancing data

mobility, state sovereignty, and national security within cross-border data transfer governance.

CONCLUSION

The findings suggest that while East African data protection regimes exhibit convergence at the level of transfer authorisation mechanisms, national security exceptions and localisation-oriented controls remain significant sources of regulatory divergence. The comparative analysis of Kenya and Rwanda legal regimes therefore demonstrates that convergence in transfer frameworks does not necessarily translate into convergence in regulatory outcomes. Although both Kenya and Rwanda adopt adequacy-oriented and safeguard-based frameworks for cross-border data transfers, their treatment of national security, public interest, data localisation, and regulatory discretion differs in practice.

This divergence raises broader questions about the prospects for regional digital integration and harmonised data governance in East Africa and the spirit of the African Union Protocol on Digital Trade to the Agreement Establishing the African Continental Free Trade Area (2024), providing for cross-Border data Transfers.

It is recommended that, to enhance legal certainty and accountability, both jurisdictions should develop clearer statutory and regulatory criteria governing the invocation of national security and public-interest exceptions in cross-border data transfer regimes. Also, greater specificity should be devised to employ in the application of necessity and proportionality standards. This should include evidentiary thresholds for justifying restrictions, and the circumstances under which cross-border transfers may be conditioned, suspended, or prohibited.

Such reforms would not undermine legitimate security interests but would ensure that limitations on cross-border data flow are predictable, transparent, and subject to meaningful regulation. In Kenya, this may require more structured guidance on the exercise of regulatory discretion under sections 51 and 52 of the Data Protection Act, while in Rwanda it may necessitate further

administrative instruction or subsidiarity legislation providing clarity of authorisation and localisation decisions administered by the National Cyber Security Authority. At its core, the central challenge is not whether national security may justify restrictions on cross-border data transfers, but how such restrictions can be exercised within a framework that preserves both effective data protection and legal certainty.

REFERENCES

- Abdulrauf, L. A. (2024). African approach(es) to data protection law. In R. Atuguba Akongburo, P. Boshe, S. A. Dei-Tutu, & M. Hennemann (Eds.), *African data protection laws: Regulation, policy, and practice* (pp. 31–54). De Gruyter. <https://doi.org/10.1515/9783110797909-005>.
- African Union. (2020). Digital transformation strategy for Africa (2020–2030). African Union Commission.
- African Union. (2024). Protocol on digital trade to the Agreement Establishing the African Continental Free Trade Area. <https://au.int/en/treaties/protocol-digital-trade-afcfta>
- Arnold, S. (2022). Drivers and barriers of digital market integration in East Africa: A case study of Rwanda and Tanzania. *Politics and Governance*, 10(2), 75–85. <https://doi.org/10.17645/pag.v10i2.4922>.
- Belli, L., Gaspar, W. B., & Singh Jaswant, S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review*, 54, Article 106017. <https://doi.org/10.1016/j.clsr.2024.106017>.
- Black, J. (2008). Forms and paradoxes of principles-based regulation. *Capital Markets Law Journal*, 1(4), 425–457. <https://doi.org/10.1093/cmlj/kmn026>.
- Bygrave, L. A. (2014). Data privacy law: An international perspective. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199675555.001.0001>.
- Charter of Fundamental Rights of the European Union, art. 52(1). (2012). 2012/C 326/02.
- Coche, E., Kolk, A., & Ocelík, V. (2024). Unravelling cross-country regulatory intricacies of data governance: The relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, 7, 112–127. <https://doi.org/10.1057/s42214-023-00172-1>.
- Council of Europe. (2018). Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+).
- European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- Gao, R. (2023). A battle of the big three? Competing conceptualizations of personal data shaping transnational data flows. *Chinese Journal of International Law*, 22(4). <https://doi.org/10.1093/chinesejil/jmad040>.
- Greenleaf, G. (2021). Global convergence of data privacy standards and limits of the EU model. *Computer Law & Security Review*, 41, 105561. <https://doi.org/10.1016/j.clsr.2021.105561>.
- Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, 169, 3–5. <https://doi.org/10.2139/ssrn.3836348>.
- ion and digital sovereignty post-Brexit* (pp. 147–162). Hart Publishing.

- <https://doi.org/10.5040/9781509966516.ch-008>.
- Kenya. (2010). The Constitution of Kenya, 2010. National Council for Law Reporting. <https://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ConstitutionofKenya2010.pdf>
- Khasanova, L., & Tai, K. (2024). Shades of authoritarian digital sovereignty: Divergences in Russian and Chinese data localisation regimes. *Journal of Cyber Policy*, 9(1), 70–94. <https://doi.org/10.1080/23738871.2024.2413938>.
- Kuner, C. (2011). Regulation of transborder data flows under data protection and privacy law: Past, present and future. OECD Publishing. <https://doi.org/10.1787/5kg0s2fk315f-en>.
- Kuner, C. (2013). Transborder data flows and data privacy law. Oxford University Press.
- Kuner, C. (2020). The Internet and the global reach of EU law: The role of the GDPR. *International Data Privacy Law*, 10(3), 160–165. <https://doi.org/10.1093/idpl/ipaa009>.
- Makulilo, A. B. (2016). The context of data privacy in Africa. In A. B. Makulilo (Ed.), *African Data Privacy Laws* (pp. 3–23). Springer. https://doi.org/10.1007/978-3-319-47317-8_1.
- Organisation for Economic Co-operation and Development. (2013). The OECD privacy framework. OECD Publishing. https://www.oecd.org/sti/ieconomy/oecd_privacy4_framework.pdf.
- Sangwa, S., & Mutabazi, P. (2025). Assessing the effectiveness of e-governance in public service delivery: A comparative study of digitization efforts in Rwanda, Kenya, and Ghana. *Open Journal of Stewardship Economics & Ethical Innovation*, 1(1). <https://doi.org/10.65655/srd9cj85>.
- Sekalala, S., & Lake, S. J. (2025). Stakeholder perceptions on institutional design of digital health regulatory frameworks: Insights from Kenya, Rwanda, and Uganda. *Oxford Open Digital Health*, 3, oqaf010. <https://doi.org/10.1093/oodh/oqaf010>.
- Sucker, F., & Beyleveld, A. (2024). African rules on cross-border data flows: The significance of regulatory convergence and the AfCFTA Digital Trade Protocol's potential contribution. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4741632>.
- Svantesson, D. J. B. (2014). International data transfers and data localisation requirements: A policy debate in need of clarification. *International Data Privacy Law*, 5(1), 1–5. <https://doi.org/10.1093/idpl/ipu034>.
- Tan, W. (2024). National security as the trump card: Assessing China's legal regime on cross-border data transfer. *Information & Communications Technology Law*, 33(3), 368–383. <https://doi.org/10.1080/13600834.2024.2375125>.
- Tranberg, C. B. (2011). Proportionality and data protection in the case law of the European Court of Justice. *International Data Privacy Law*, 1(4), 239–248. <https://doi.org/10.1093/idpl/ipr015>.
- Tranberg, C. B. (2011). Proportionality and data protection in the case law of the European Court of Justice. *International Data Privacy Law*, 1(4), 239–248. <https://doi.org/10.1093/idpl/ipr015>.

Cases

- Bundesverfassungsgericht. (1958). Apothekenurteil (Pharmacy Case), BVerfGE 7, 377 (1 BvR 596/56).
- Bundesverfassungsgericht (BVerfG). (1994). Beschluss des Bundesverfassungsgerichts, BVerfGE 91, 145 (173).
- Samuel Kerosi Ondieki v. National Hospital Insurance Fund Board of Management & Another [2012] KEHC 1594 (KLR).
- Steyn v. Ruscone (Application No. 4 of 2012) [2013] KESC 11 (KLR) (23 May 2013).

Legislation

Data Protection (General) Regulations, 2021,
Legal Notice No. 263 of 2021 (Kenya).

Data Protection Act, No. 24 of 2019 (Kenya).

Law No. 058/2021 on the Protection of Personal
Data and Privacy (Rwanda).

Law No. 26/2017 of 31 May 2017 Establishing the
National Cyber Security Authority and
Determining its Mission, Organisation and
Functioning (Rwanda).