



GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

SUBMISSION ON KENYA'S DRAFT GUIDANCE NOTE ON CROSS-BORDER DATA TRANSFERS TO THE OFFICE OF THE DATA PROTECTION COMMISSIONER (ODPC)

June 2026

The Global Data Alliance (GDA)¹ thanks the Office of the Data Protection Commissioner (ODPC) for the opportunity to provide feedback on Kenya's Draft Guidance Note on Cross-Border Data Transfer. The GDA welcomes the ODPC's commitment to operationalizing the Data Protection Act, 2019, and to providing clear, workable guidance on cross-border data transfers. We offer the following comments in a constructive spirit, with the shared goal of ensuring Kenya's data protection framework safeguards privacy while supporting the cross-border data flows on which Kenyan businesses, researchers, and citizens depend.

I. Introduction

The Global Data Alliance is a cross-industry coalition of companies headquartered across multiple regions of the world that are committed to high standards of data privacy, security, and responsible data use. GDA members share a long-standing commitment to supporting economic development, building trust in the digital economy, and protecting personal and non-personal data across jurisdictions, technologies, and business models. Alliance member companies rely on the ability to transfer data responsibly across borders in order to innovate, create jobs, and make industries more competitive both in their home markets and abroad. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors.

Kenya occupies an increasingly important position in the African digital economy. As digitalization accelerates across the continent, the ODPC's guidance on cross-border data transfers will shape not only how Kenyan companies engage with global markets, but will also serve as a model for the region. The GDA therefore welcomes this consultation as an important opportunity to advance a framework that is both privacy-protective and commercially workable.

Cross-border data transfers are a foundational enabler of Kenya's most important long-term economic and development strategies, including Kenya Vision 2030, the Digital Economy Blueprint, and Kenya's commitments under the African Continental Free Trade Area (AfCFTA), including the AfCFTA Digital Trade Protocol. They support growth across all sectors of the economy—from agriculture, fisheries, and

mining, to manufacturing and digitally enabled services—while enhancing productivity, safety, cybersecurity resilience, and environmental sustainability. These benefits are particularly important for micro, small, and medium-sized enterprises (MSMEs), which depend on affordable access to global digital infrastructure, cloud services, and analytical tools to scale beyond domestic markets.

At a time of rising geopolitical tensions and regulatory divergence, policies that unnecessarily restrict data flows risk fragmenting the global digital economy and limiting the ability of Kenyan firms to access regional and global markets. By contrast, data governance frameworks that enable data to move freely with trust help economies integrate into global value chains, support services exports, and advance shared prosperity.

II. Areas of Support

The GDA welcomes several constructive and forward-looking aspects of the Draft Guidance Note.

The Draft Guidance Note appropriately provides multiple transfer mechanisms—including adequacy decisions, reciprocal data protection agreements, and Binding Corporate Rules (BCRs), consistent with international best practices. A flexible, mechanism-based approach would be well-aligned with frameworks such as the EU General Data Protection Regulation and the Global Cross-Border Privacy Rules (CBPR) system, and will give organizations operating across multiple jurisdictions workable compliance pathways. The GDA also supports the Guidance Note's recognition of the Kenya Cloud Policy 2024 to the extent that this Policy acknowledges the importance of facilitating cross-border data transmission, fostering interoperability, and strengthening collaboration across nations. The Guidance Note should be interpreted consistently with these objectives.

III. Areas for Improvement and Clarification

Below we identify several areas for improvement and clarification in the draft Guidance.

A. Eliminate or Narrow Data Localization Proposals

Section 10 of the Draft Guidance Note interprets the “strategic interest of the state” data localization requirement under Section 50 of the Data Protection Act to encompass broad categories of activity, including all primary and secondary healthcare provision and all early childhood and basic education. As currently drafted, this interpretation would compel a wide cross-section of digital economy participants operating in Kenya—including hospitals, clinics, schools, and the cloud service providers they rely on—to store and process personal data in-country.

The GDA respectfully urges the ODPC to reconsider this expansive interpretation for several reasons.

First, the economic costs of broad data localization requirements are well-documented. Data localization mandates raise prices for consumers, reduce competitiveness, weaken cybersecurity outcomes, and deter foreign direct investment without producing measurable privacy or security gains. The GDA's Cross-Border Data Policy Index—which assesses the openness or restrictiveness of cross-border data policies across nearly 100 economies—consistently finds that more restrictive data transfer environments correlate with diminished digital transformation, reduced economic opportunity, and weaker data security outcomes. Restrictions on cross-border data transfers also prevent domestic companies, including MSMEs and large organizations such as hospitals and banks, from using world-leading cloud computing solutions that frequently provide best-in-class security capabilities.

Second, broad localization requirements are inconsistent with Kenya's own commitments under the AfCFTA Digital Trade Protocol, which promotes cross-border data flows and disciplines unjustified localization requirements among African Union Member States. They would also risk undermining Kenya's ongoing bilateral trade engagement with the United States, in which open cross-border data flows and the avoidance of forced localization are core digital trade priorities.

Third, the Draft Guidance Note's treatment of healthcare and education as per se "strategic interest" processing activities conflates sovereign governmental functions with routine commercial service delivery. Ordinary commercial healthcare and education provision—including cloud-hosted electronic medical records systems used by private hospitals or e-learning platforms—are not equivalent to core state functions such as administering civil registration, overseeing election systems, or managing public finances. The ODPC should clarify that data localization requirements apply only where processing directly and materially supports core sovereign governmental functions of the type envisaged in Regulation 26 of the General Regulations.

The GDA also encourages the ODPC to confirm that the "serving copy" obligation under Section 50(b) of the Act can be satisfied through interoperable cloud architectures and does not require duplicative on-premises or in-country infrastructure. Cloud-based architectures that maintain a logical copy of data accessible within Kenya, without requiring physical data center presence, represent a pragmatic and technically sound approach that serves the underlying policy objective without imposing unnecessary costs.

Recommendation:

- Clarify that data localization requirements under Section 50 apply only where processing directly supports core sovereign governmental functions, and that routine commercial healthcare and education service delivery is not, by default, processing for the "strategic interest of the state."
- Clarify in the Draft Guidance Note that the concept of "strategic interest of the state" should be interpreted narrowly and should apply only to processing that directly supports core sovereign governmental functions. It should not automatically extend to routine commercial or administrative activities, including ordinary healthcare administration, insurance administration, claims handling, member support, or education service delivery, merely because such activities involve sensitive or health related data.
- Confirm that the "serving copy" obligation can be satisfied through interoperable cloud architectures, without requiring duplicative on-premises or in-country physical infrastructure.

B. Recalibrate Onward Transfer Restrictions to Reflect Commercial Realities

Section 9 of the Draft Guidance Note would condition onward transfers on specific, prior, and written authorization from the transferring entity for the exact third party, location, data categories, and purpose involved. The Guidance Note also categorically prohibits onward transfers for the recipient's own purposes, including analytics, commercial exploitation, profiling, product improvement, or marketing.

As drafted, these restrictions would prevent routine and beneficial activities relied upon by Kenyan businesses every day. For example, a Kenyan company that transfers personal data to a cloud service provider operating outside Kenya under a valid transfer mechanism could not permit that provider to use standard sub-processors for security monitoring, fraud prevention, service reliability, or technical support—activities that actively protect data subjects. The categorical prohibition on processing for the

recipient's own purposes could similarly prevent legitimate contractual arrangements with sub-processors for product improvement or cybersecurity purposes. The draft could also expressly acknowledge routine onward transfers within corporate groups and operational ecosystems, including transfers to affiliates, shared service centers, and central analytics functions that support service quality, fraud prevention, product governance, or product improvement, provided these activities remain subject to appropriate safeguards, contractual controls, and purpose limitations.

These restrictions go significantly beyond international norms. Widely recognized frameworks, including the Global CBPR system and ISO/IEC 27701 (Privacy Information Management), permit onward transfers to contractually bound sub-processors on a category basis with appropriate notification and objection rights, without requiring case-by-case, purpose-specific pre-authorization. The EU's Standard Contractual Clauses similarly permit the use of sub-processors subject to prior general or specific authorization and appropriate safeguards, rather than requiring prior written authorization for each individual transfer.

The GDA also notes that the categorical prohibition on onward transfers for the recipient's "own purposes" is broader than necessary to give effect to the purpose limitation principle in Section 6.2 of the Guidance Note. A narrower restriction—prohibiting processing that is incompatible with the original purpose, consistent with established purpose limitation doctrine—would better align with international norms while still protecting data subjects.

Where organizations in Kenya process personal data relating to individuals who are not located in Kenya and who are not Kenyan nationals (e.g., in the context of regional or global service delivery hubs), the Draft Guidance Note should clarify that such processing and subsequent transfers are not subject to data residency or onward transfer restrictions intended to protect Kenyan data subjects.

In particular, the Guidance should confirm that personal data originating outside Kenya may be returned or re-transferred to the relevant jurisdiction, or further processed within global service delivery models, provided that appropriate safeguards are in place.

Such clarification is critical to ensure that Kenya can continue to position itself as a competitive destination for global and regional operations, including shared service centers, technology hubs, and data-driven industries that rely on the ability to process and transfer international data flows efficiently.

Recommendation:

- Recalibrate onward transfer restrictions to permit transfers to disclosed and contractually bound sub-processors, affiliates, shared service functions, cloud providers, and other operational counterparties, on a category basis, with appropriate notification and objection rights, consistent with the Global CBPR system and ISO/IEC 27701.
- Replace the categorical prohibition on onward transfers for the recipient's own purposes with a narrower restriction on processing that is incompatible with the original transfer purpose, consistent with the purpose limitation principle in Section 6.2.
- Clarify the treatment of international data and avoid unintended application of data residency or onward transfer restrictions to non-Kenyan data. Failure to provide this clarification risks discouraging international investment and undermining Kenya's ability to act as a regional digital hub, particularly for organizations operating global or multi-jurisdictional data processing models.

C. Adopt a Risk-Based, Proportionate Approach to Compliance Obligations

The Draft Guidance Note's compliance obligations—including requirements for Transfer Impact Assessments (TIAs), Data Protection Impact Assessments (DPIAs), detailed transfer documentation, and mandatory demonstration of safeguards prior to every transfer—will, in practice, apply to organizations of vastly different sizes, sophistication levels, and risk profiles. As currently drafted, these obligations do not scale to the volume and sensitivity of data processed, creating disproportionate burdens for MSMEs and data-intensive industries, without commensurate privacy or security benefits.

The GDA urges the ODPC to expressly endorse a risk-based and proportionate approach to compliance, so that the obligations imposed scale to the actual risk profile of the transfer in question. In particular, routine, low-risk transfers—such as those made under widely accepted international transfer mechanisms, or involving pseudonymized or encrypted data—should not require the same level of documentation and prior demonstration of safeguards as high-risk transfers involving sensitive personal data.

The ODPC should also consider aligning its compliance expectations with established international standards, including ISO/IEC 27701 (Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management) and the Global CBPR system. Alignment with such internationally recognized frameworks would allow organizations to leverage existing compliance investments, reduce duplicative burdens, and enhance cross-border regulatory interoperability—all without weakening the substantive protections available to Kenyan data subjects.

Recommendation:

- Explicitly endorse a risk-based and proportionate approach to compliance obligations, scaling requirements to the volume, sensitivity, and risk profile of the transfer in question.
- Recognize ISO/IEC 27701 certification and Global CBPR system participation as evidence of “appropriate safeguards” under Section 49(3) of the Act.
- Streamline documentation and prior demonstration requirements for low-risk transfers made under widely accepted international transfer mechanisms.

D. Expand Recognized Transfer Mechanisms and Promote Regional Interoperability

The GDA welcomes the Draft Guidance Note's recognition of multiple transfer mechanisms. To make these mechanisms operationally viable and to promote Kenya's integration into regional and global digital ecosystems, the ODPC should consider whether additional steps could help expand the range of recognized transfer tools.

For example, the ODPC could consider whether the Guidance Note might be updated to recognize the Global CBPR system or other international interoperability frameworks as a basis for finding “appropriate safeguards” under Section 49(3) of the Act. The GDA also encourages the ODPC to assess how to promote cross-border interoperability in a manner consistent with the AfCFTA Digital Trade Protocol. Kenya has an important opportunity to serve as a catalyst for regional data governance interoperability.

More broadly, the GDA encourages Kenya's continued engagement and consideration of formal participation in the Global CBPR Forum, through ongoing forums and workshops, as a means of deepening Kenya's integration into global data governance networks and reinforcing its position as a trusted and attractive hub for data-driven investment.

Recommendation:

- Recognize the Global CBPR system and ISO/IEC 27701 certification as bases for "appropriate safeguards" under Section 49(3) of the Act.

E. Ensure Consistency with Kenya's Cloud Policy and Trade Commitments

The Draft Guidance Note acknowledges the Kenya Cloud Policy 2024 as part of Kenya's legislative framework. The GDA supports this recognition. The Cloud Policy expressly endorses cross-border transmission, interoperability, and international collaboration, reflecting Kenya's commitment to an open digital economy.

The ODPC should ensure that the final Guidance Note is interpreted and applied in a manner fully consistent with these commitments. In particular, overly burdensome compliance requirements, broad data localization mandates, or restrictive onward transfer conditions that effectively deter use of global cloud services would undermine the objectives of the Cloud Policy and risk increasing compliance costs without commensurate privacy benefits.

The GDA also notes that data localization requirements that exceed the narrowly defined categories established in Regulation 26 of the General Regulations would create tensions with Kenya's trade objectives under the AfCFTA Digital Trade Protocol and Kenya's ongoing engagement with bilateral trade partners, including the United States. A final Guidance Note that interprets localization requirements narrowly, and that affirmatively supports the use of global cloud infrastructure for routine commercial activities, would better serve Kenya's dual objectives of privacy protection and economic competitiveness.

Recommendation:

- Ensure the final Guidance Note is interpreted consistently with Kenya's AfCFTA Digital Trade Protocol commitments as well as other Kenyan legal authorities that support cross-border data transfers and that discipline data localization requirements. Affirm that the use of global cloud services for routine commercial healthcare, education, finance, and other activities does not constitute processing for the "strategic interest of the state" and does not trigger localization requirements, and clarify that the involvement of health data does not by itself render ordinary administrative, operational, or support processing subject to localization.

IV. Conclusion

The ODPC's Draft Guidance Note on Cross-Border Data Transfer reflects a genuine commitment to protecting the privacy and dignity of Kenyan data subjects and to providing clear, actionable guidance for organizations engaged in cross-border data transfers. With targeted refinements—particularly around the scope of data localization requirements, onward transfer restrictions, the adoption of risk-based

compliance approaches, and the expansion of recognized transfer mechanisms—the final Guidance Note can serve as a regional model that protects data subjects while enabling cross-border data flows, digital economy growth, and Kenyan leadership.

Cross-border data flows are not merely a commercial convenience; they are essential infrastructure for Kenya's participation in the global economy. Robust, trusted, and workable cross-border data transfer rules will help position Kenya as an attractive destination for data-driven investment, a regional hub for digital innovation, and a model for Africa of how privacy protection and economic openness can reinforce rather than undermine each other.

The GDA appreciates the opportunity to provide these comments and stands ready to continue engaging with the ODPC on these important issues. Should you have any questions or comments, please feel free to contact Joseph Whitlock, Executive Director, Global Data Alliance, at josephw@bsa.org.

¹ The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. For more information, see <https://www.globaldataalliance.org>