



GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

ECONOMIC AND POLICY IMPLICATIONS OF KENYA'S GUIDANCE ON CROSS-BORDER DATA TRANSFERS

SUPPORTING KENYA'S DIGITAL SOVEREIGNTY & US-KENYA RELATIONS

October 2026

I. Executive Summary

The Global Data Alliance (GDA)¹ respects and supports objectives underlying Kenya's September 8 Guidance on Cross-Border Data Transfers (Guidance).² These objectives are well-served by policies that build domestic capability; preserve access to trusted global technologies; ensure redundancy, response, and recovery; and hold providers accountable for legal compliance and operational performance. The GDA is concerned that aspects of the Guidance may produce the opposite result: higher costs for Kenyan firms, fewer response and recovery options, and impediments to cybersecurity, safety, economic development, and regulatory compliance priorities.

The GDA understands digital sovereignty through four mutually reinforcing pillars: capability, collaboration, resilience, and trust. Geographic storage mandates, data transfer restrictions, and nationality-based digital sovereignty mandates weaken each of these pillars. Instead, we urge Kenyan authorities to undertake a risk- and performance-based evaluation of capability, collaboration, resilience, and trust.³

Three features of the Guidance warrant priority attention: (1) the application of the statutory local processing or local serving copy requirement to healthcare, education, and designated protected systems, even where private-sector services are involved; (2) imposing restrictive onward-transfer conditions that appear to conflict with transfer authorization provisions in the contractual annexes; and (3) uncertainty about compliance procedures for routine transfers involving offshore cloud infrastructure. Separately, the Guidance's cross-border data restrictions deserve particular scrutiny in the healthcare context, given the risks to human health that come from these undue access restrictions to cross-border medical services and treatments.

GDA urges Kenya to undertake a targeted, risk-based clarification or amendment that preserves Kenya's control, supervision, and safeguards while allowing trusted cross-border data processing and cross-border access to information and digital tools. The United States should place this issue on the agenda of bilateral discussions, offer technical engagement, and support Kenya's capacity to adopt performance-based security and privacy protections.

II. Core Concerns re Cross-Border Guidance

A. Concerns re Localization Mandates

Section 50 of the Data Protection Act, 2019 provides alternative compliance routes for data processed for the "strategic interests of the state": process it through a server and data center in Kenya, OR store at least one serving copy in a Kenyan data center. The Guidance incorporates Regulation 26's categories, including civil registration, elections, public finances, protected computer systems, early childhood and basic education, and primary and secondary healthcare. It does not expressly distinguish private commercial healthcare and education providers from core state functions. Reporting on the draft suggested possible coverage of transport platforms through the protected-system category; the extent of that coverage should be confirmed with the

WWW.GLOBALDATAALLIANCE.ORG

ODPC. While the local serving copy option does not itself prohibit overseas processing or storage, it creates a greater data- and cyber-security attack surface to defend.⁴

B. Concerns re Onward Transfer Restrictions

The main body of the Guidance requires cumulative conditions for onward transfers, including specific prior written authorization for the exact recipient, location, data categories, and purpose; assessments; contractual protections; records; and audit rights. It also prohibits onward transfers for a recipient's own purposes, listing analytics and product improvement among the examples. The Guidance is highly restrictive in a way that does not match broader international practice.

Furthermore, the Guidelines contain internal inconsistencies that further complicate compliance. For example, despite some of the prohibitions described above, the annexed controller-to-controller standard clauses (Clause 18.1(d)) allow onward transfers expressly permitted under specified contractual conditions, and the controller-to-processor clauses (Clause 18.2) permit prior general authorization by category of subprocessor, with notice and objection rights.

C. Concerns re Cloud-related Provisions

We have particular concerns on the provisions relating to cloud storage and processing and sensitive data.

On the one hand, we welcome the Guidance's express recognition of the compelling legitimate interests in overseas cloud hosting, as well as the inclusion of standard contractual clauses, binding corporate rules, and cloud security measures.

On the other hand, several requirements may prove impracticable if applied to routine cloud operations. First, the Guidance treats processing on offshore cloud servers as a cross-border transfer and requires transfer records and demonstration of safeguards to the Commissioner upon request. Second, it calls for data protection impact assessments where processing presents a high risk. Third, Section 49(1) of the Data Protection Act and the Guidance impose additional explicit-consent and safeguard requirements for cross-border transfers of sensitive personal data, including health, biometric, and genetic information.

Across these requirements, the central concern is the absence of sufficiently clear, systematic, and streamlined compliance pathways for repetitive, continuous, and appropriately protected cloud usage at scale. Modern cloud environments continuously perform thousands or millions of automated operations –including saving and refreshing files, synchronizing databases, replicating and backing up information, exchanging machine-to-machine data, routing requests between servers, balancing workloads, updating applications, generating security logs, and monitoring system performance – often across multiple jurisdictions without human intervention.

If every such operation must be separately identified, documented, assessed, or authorized, compliance would become technically and operationally unworkable. These activities are continuous and interconnected components of cloud services, not discrete transactions that can practicably be regulated one by one.

D. Concerns re Sensitive Personal Data Provisions

These difficulties are particularly acute for sensitive personal data. Hospitals, laboratories, insurers, connected medical devices, and healthcare platforms routinely exchange and update health, biometric, and genetic information for diagnosis, treatment, claims administration, patient monitoring, cybersecurity, and medical research. If the Guidance is interpreted to require separate explicit consent or individual transfer assessments for each automated exchange, it could impede essential healthcare operations, including activities necessary to protect patient safety. The Guidance should therefore clarify how ongoing consent, legally recognized transfer mechanisms, standing authorizations, and system-level assessments may support continuous, appropriately safeguarded processing. Where the explicit-consent requirement under Section 49(1) does not permit sufficient flexibility for necessary healthcare and safety functions, targeted legislative clarification or amendment may be warranted.

The cumulative effect of these requirements may be to discourage or effectively preclude cloud adoption by many Kenyan healthcare providers, particularly smaller hospitals, clinics, laboratories, and other organizations

unable to absorb the costs and legal uncertainties of compliance. Instead, such providers may be driven toward fragmented, on-premises systems that lack many of the advantages of modern, centrally managed cloud environments—including geographic redundancy, disaster recovery, continuous cybersecurity monitoring, automated security updates, scalable computing capacity, specialized technical support, and access to advanced analytical and AI tools. Fragmented systems can also impede the secure sharing and integration of medical information, limiting timely access to patient records, remote specialist consultations, telemedicine, coordinated treatment, clinical decision support, medical research, disease surveillance, and the early detection of adverse medical events.

The ultimate costs would be borne not merely by healthcare providers, but by Kenyan patients: delayed diagnoses and treatment, preventable medical errors, interrupted services, and missed opportunities to identify and respond to emerging health risks. If these restrictions materially reduce the availability, quality, or continuity of healthcare services, the resulting public-health consequences could be substantial and measurable, including through increased rates of avoidable illness, adverse clinical events, and other preventable patient harms. A regulatory framework intended to protect sensitive health information should not inadvertently deprive Kenyan patients and healthcare professionals of the technologies needed to deliver safe, timely, and effective care.

III. How Restrictive “Sovereignty” Rules Can Harm Kenya

A. Economic capacity, AI adoption, and services exports

Kenyan businesses need affordable cloud, cybersecurity, analytics and AI capabilities to compete in agriculture, logistics, manufacturing, financial services, healthcare and digital exports. Requirements to duplicate infrastructure, use a narrow range of in-country capacity (including on-premises infrastructure), or negotiate individual sub-processor permissions raise fixed costs. Smaller Kenyan enterprises are least able to absorb those costs, and Kenyan business-process and shared-service hubs may become less attractive if international data cannot reliably enter, be processed, and move onward under safeguards. These effects weaken Kenyan economic capability, not merely US technology exports.

Published economic modeling illustrates these effects in other parts of the world. A May 2026 Oxford Economics study modeled wider private-sector sovereign-AI and localization restrictions in Asia-Pacific economies and found material reductions in projected AI adoption and foregone 2035 GDP gains.⁵ The study offers a cautionary message: when a government imposes rules containing data or infrastructure localization mandates, case-by-case transfer restrictions, or unscalable one-off government notification and approval procedures, these types of rules deprive firms and citizens of the digital transformation benefits that the government is seeking to deliver.

Compulsory measures of the sort described above can deter investment – rather than encourage it – leading to the opposite of the intended result.

B. Operational resilience: response, recovery and continuity

The ability to recover from a cyberattack, natural disaster, electricity disruption or physical incident depends on redundancy, geographic separation, portable backups, tested restoration, and access to qualified responders. The Guidance's serving-copy alternative permits the possibility of internationally distributed processing and recovery; accordingly, it should not be characterized as categorically prohibiting offshore disaster recovery. Nevertheless, a required in-country copy can introduce extra repositories to secure, synchronization costs, and potential single-country operational dependencies if implemented rigidly. Its existence alone does not establish failover capability, recovery-time performance or backup integrity. The Guidance itself calls for backup, business-continuity and disaster-recovery measures.

Geographic redundancy must also be evaluated against common failure risks. Multiple data centers or availability zones within the same country may share dependencies on electricity grids, telecommunications networks, software infrastructure or physical facilities, leaving critical services exposed to correlated disruptions.

For Kenyan hospitals, schools, payments operators and essential infrastructure, the ODPC should explicitly recognize safeguarded cross-border replication, failover, forensic response and restoration under distributed and hybrid architectures. Objective criteria should address recovery-time and recovery-point objectives, verified restore tests, segregated backups, interoperability, access controls and assured lawful supervisory access. This would implement the Guidance's own emphasis on recoverability without mandating unnecessary infrastructure duplication for ordinary commercial workloads.

C. Cybersecurity and national-security effectiveness

Modern cyber defense relies on combining threat signals across jurisdictions, around-the-clock security operations, distributed incident-response specialists, and rapid deployment of protections. Uncertainty about which onward transfers require specific authorization—and about permissible secondary uses of operational data—may complicate security collaboration. The Guidance already supports logging, encryption, multifactor authentication and backups; the ODPC should make clear that safeguarded threat detection, malware analysis, security telemetry and incident response fit within its transfer and purpose-limitation framework. These are prospective operational concerns, not evidence of cyber incidents caused by the Guidance.

For national security, governments often have good reasons to impose more rigorous protections for narrowly defined classified information, military systems, election infrastructure and core government records. But extending security-driven location rules to routine commercial healthcare, education, and potentially transport may divert scarce supervisory resources away from truly high-risk systems. The better distinction is between risk categories and verifiable security controls, with tailored exceptions where a demonstrated sovereign need justifies physical custody or domestic processing.

D. Healthcare, research and public-health preparedness

Healthcare resilience is also a patient-safety and consumer-protection issue. Hospitals, insurers and other healthcare providers depend on timely access to accurate records for patient eligibility verification, treatment authorization, claims processing, provider payments and clinical case management. Interruptions to these functions can delay treatment and disrupt continuity of care. Kenya's regulatory framework should therefore assess whether critical health services remain available during cyber incidents, power disruptions and other emergencies—not merely whether health data is stored domestically.

As introduced in the cloud services discussion above, the explicit coverage of primary and secondary healthcare creates particular exposure for Kenyan patients and providers. Electronic health records, specialist referral, diagnostics, cloud support and continuity of clinical systems may depend on international services; clinical trials, pharmacovigilance and medical-device vigilance can require protected exchanges across jurisdictions. Beyond the serving-copy requirement, the Guidance repeats Section 49(1)'s requirement for explicit data-subject consent and confirmation of appropriate safeguards for transfers of sensitive personal data. The ODPC should clarify how those requirements operate for essential clinical continuity, safety monitoring, urgent care and properly authorized research, rather than implying that any transfer of health data is prohibited.

The Guidance recognizes transfers necessary to protect vital interests during exceptional emergencies, and proportionate, legally authorized public-interest transfers in circumstances such as pandemics and disease outbreaks. It should expressly explain how these bases interact with special requirements governing sensitive data. The US–Kenya Health Cooperation Framework has separately raised concerns over data safeguards. Bilateral initiatives should use legally valid, transparent data-sharing arrangements, with aggregation or de-identification where suitable, while ensuring continuity of care and appropriate patient protections.⁶

IV. A More Effective Kenyan Digital Sovereignty Framework

Kenya can achieve sovereign control through enforceable outcomes rather than general geographic exclusion. The GDA recommends five targeted changes, while preserving Kenya's ability to impose stricter requirements for genuinely high-risk sovereign functions:

1. **Narrow localization.** Amend Regulation 26 or issue legally sound clarification so that the “strategic interest” scope is confined to processing directly and materially supporting core sovereign functions, such as those relating

to military and other core national security data. We also recommend a narrowing of the scope of “strategic interest.” We respectfully submit that the Guidance may not promote Kenya’s “strategic interest” if it undermines – across healthcare, education, and finance – Kenya’s cross-border access to data and digital tools, thus impeding Kenya’s integration into knowledge and technology ecosystems.

2. **Reconcile onward transfer rules.** Clarify that the main text’s exact-recipient approval language is consistent with controller-to-controller Clause 18.1(d) and the controller-to-processor Clause 18.2 provision for category-based subprocessor authorization, including advance notice and objection rights. Clarify the distinction between onward transfers for a recipient’s own purposes and lawful processing by the initial recipient. Permit appropriately controlled cybersecurity, fraud prevention, reliability, product-safety and compatible improvement functions under enforceable contractual and technical safeguards. Relevant assurance criteria should include defined recovery-time and recovery-point objectives, independently tested restoration capabilities, immutable or offline backups, encryption and key-management safeguards, incident-response procedures, and demonstrable supervisory access to records and systems.
3. **Make compliance practicable and risk-proportionate.** Preserve the existing high-risk trigger for DPIAs and the Commissioner’s ability to request evidence of safeguards. Clarify how continuous or repeated low-risk cloud transfers may be documented and assessed at an appropriate system or contractual level without artificially treating each routine transmission as a separate regulatory exercise. Support reuse of adequate transfer mechanisms and existing verified safeguards. In particular, Kenya should consider whether necessary health-related transfers – including continuity of treatment, claims administration, medical-device safety monitoring and emergency response – can be authorized through clearly defined statutory grounds and appropriate safeguards without requiring repeated individual consent where consent is impracticable or inappropriate. Any such clarification or reform must be consistent with Section 49 of the Data Protection Act or accompanied by the necessary legislative amendment.
4. **Recognize verifiable technical and legal safeguards.** Accept robust encryption and customer key control, tested recovery plans, access controls, contractual remedies and recognized standards/certifications as relevant evidence—not automatic substitutes for statutory duties. Explore the Global CBPR System and ISO/IEC 27701 as interoperability and assurance tools.
5. **Protect essential health and safety functions.** Clarify how explicit consent and appropriate-safeguard requirements for sensitive personal data operate alongside recognized vital-interest and public-interest transfer bases, including urgent treatment, outbreak response, clinical research, pharmacovigilance and connected medical-device safety. Clarify conditions for transfer and re-transfer of foreign-origin data processed by Kenyan service hubs, without presuming such transfers are categorically exempt from applicable law.

VI. Conclusion

The GDA appreciates the opportunity to provide these comments. Should you have any questions, please feel free to contact Joseph Whitlock, Executive Director, Global Data Alliance, at jwhitlock@bsa.org.

¹ For more information, see www.globaldataalliance.org

² Kenya ODPC, Guidance Notes for Cross-border Data Transfers (2026), <https://www.odpc.go.ke/wp-content/uploads/2026/09/ODPC-%E2%80%93Guidance-Notes-for-Cross-border-Data-Transfers.pdf>; Kenya Data Protection Act 2019, §§49–50, https://www.odpc.go.ke/wp-content/uploads/2024/02/TheDataProtectionAct__No24of2019.pdf

³ See e.g., GDA, Promoting Digital Sovereignty: Building Capability, Collaboration, Resilience, and Trust into Digital Ecosystems (2026), at www.globaldataalliance.org; GDA, Cloud & AI Development Act: Preserving Cross-Border Digital Access Across All EU Sectors (2026), at www.globaldataalliance.org

⁴ See Kenya, Data Protection (General) Regulations 2021, reg. 26, <https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf>; ODPC Guidance, pp. 20–27; Techweez, Kenya Pushes Mandatory Local Data Storage for Ride-Hailing and Booking Apps (Apr. 17, 2026), <https://techweez.com/2026/04/17/odpc-transport-local-data-storage/>

⁵ Oxford Economics & AI Adoption Initiative, The Economics of Sovereign AI: Balancing Autonomy, Innovation, and Growth in the Asia-Pacific (May 2026), https://adopt-ai.org/wp-content/uploads/2026/05/Oxford-Economics-x-AIAI_Sovereign-AI.pdf

⁶ Capital FM, Appeal Court Temporarily Lifts High Court Orders Blocking Kenya–US Health Deal (May 12, 2026), <https://www.capitalfm.co.ke/news/2026/05/court-of-appeal-lifts-high-court-orders-kenya-us-health-deal-2026/>; JURIST, Kenya Dispatch (Dec. 30, 2025), <https://www.jurist.org/news/2025/12/kenya-dispatch-high-court-halts-kenya-us-health-deal-over-constitutional-concerns/>