

AMCHAM
KENYA

UNLOCKING THE ECONOMIC VALUE OF CROSS-BORDER DATA FLOWS IN THE EAST AFRICAN COMMUNITY (EAC)

10TH SEPTEMBER 2026



This report is a rapid, high-level outline of how cross-border data flows create economic value, how fragmentation in relevant laws across the EAC is preventing that economic value from being realised, and how harmonisation could be achieved to solve this barrier to economic growth.

IN PARTNERSHIP WITH



Eastern Africa
Regional
Digital Integration
Project

G:ENESIS
UNLOCKING VALUE

TABLE OF CONTENTS

ACRONYMS	4
USEFUL DEFINITIONS	5
EXECUTIVE SUMMARY	6
01 INTRODUCTION	9
1.1 CONTEXT & WHY NOW	9
1.2 APPROACH AND METHODOLOGY	11
02 THE ECONOMIC VALUE OF CROSS-BORDER DATA FLOWS	13
03 BARRIERS TO REALISING ECONOMIC VALUE FROM CROSS-BORDER DATA FLOWS	22
3.1 CURRENT STATE OF REGULATORY FRAGMENTATION	22
3.2 ANTICIPATED ELEMENTS OF THE EMERGING EAC FRAMEWORK	27
3.3 HOW FRAGMENTATION COSTS EAST AFRICAN BUSINESSES (MICRO IMPACT)	30
04 REMOVING BARRIERS: CONSIDERATIONS FOR THE PROPOSED EAC FRAMEWORK	34
4.1 TRANSFER RULES, NATIONAL PROCEDURES AND THE COST OF TRADING REGIONALLY	35
4.2 COMPLIANCE COSTS, INSTITUTIONAL CAPACITY AND SMALLER FIRMS	37
4.3 BALANCING OPENNESS WITH TRUST	39
05 WAY FORWARD	41

LIST OF FIGURES, TABLES & BOXES

Figure 1: Contribution of data-exposed, traded sectors to Kenya's GDP	17
Figure 2: Growth in digitally delivered services by region (2015-2024)	18
Table 1: Data governance regimes across the EAC's eight partner states	24
Figure 3: Anticipated key elements of the emerging EAC framework	29

ACRONYMS

AfCFTA	African Continental Free Trade Area	IT	Information Technology
AI	Artificial Intelligence	KCB	Kenya Commercial Bank
AML	Anti-Money Laundering	KII	Key Informant Interview(s)
CFT	Countering the Financing of Terrorism	KYC	Know-Your-Customer
AmCham	American Chamber of Commerce	MoU	Memorandum / Memoranda of Understanding
ARCT	Agence de Régulation et de Contrôle des Télécommunications	MSMEs	Micro, Small and Medium-Sized Enterprises
ARPTC	Autorité de Régulation de Poste et de Télécommunication	NCSA	National Cyber Security Authority
AU	African Union	ODPC	Office of the Data Protection Commissioner
BCRs	Binding Corporate Rules	OECD	Organisation for Economic Co-operation and Development
CBPR	Cross-Border Privacy Rules	PDPA	Personal Data Protection Act
DRC	Democratic Republic of the Congo	PDPC	Personal Data Protection Commission
EAC	East African Community	PDPO	Personal Data Protection Office
EEA	European Economic Area	PSP	Payment service provider
EU	European Union	RECs	Regional Economic Communities
FATF	Financial Action Task Force	RURA	Rwanda Utilities Regulatory Authority
GDP	Gross Domestic Product	SCCs	Standard Contractual Clauses
GDPR	General Data Protection Regulation	SMEs	Small and Medium Enterprises
HR	Human Resources	TWG	Technical Working Group
ICT	Information and Communications Technology	WTO	World Trade Organisation
IoT	Internet of Things		

USEFUL DEFINITIONS

TERM	DEFINITION
Adequacy	Recognition that a destination, sector, organisation or data-protection regime provides sufficient protection to permit transfers under an adequacy pathway.
Binding Corporate Rules	A cross-border transfer mechanism based on binding internal data protection rules for transfers within a corporate group, subject to applicable legal requirements.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Cross-Border Data Flow	The movement or availability of data between jurisdictions that enables regional business operations, digital services, payments, trade and related economic activity.
Data Classification Framework	A system for defining categories of data, such as high-risk or national-security data, so that different regulatory requirements can be applied predictably.
Data Localisation	A requirement, or practical regulatory pressure, to store or process specified data within a particular jurisdiction rather than using offshore or regional infrastructure.
Derogation	A limited exception to the normal transfer requirements, permitting a transfer on specified grounds, including explicit informed consent, contractual necessity, vital interests, important public interest or legal claims.
EAC Cross-Border Data Flows Framework	Refers to the proposed EAC Cross-Border Data Flows Framework which was presented for review and validation at the June 2026 EAC Technical Working Group meeting.
Mirroring rules	Requirements for a domestic copy of data to be maintained even where the data may also be stored or processed elsewhere.
Personal Data	Information relating to an identified or identifiable individual.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Standard Contractual Clauses	Pre-approved contract clauses which a regulatory authority has authorised for use as a recognised and lawful cross-border transfer mechanism.
Variable Geometry	Phased implementation in which Partner States that meet the required conditions can proceed before all EAC states are ready.

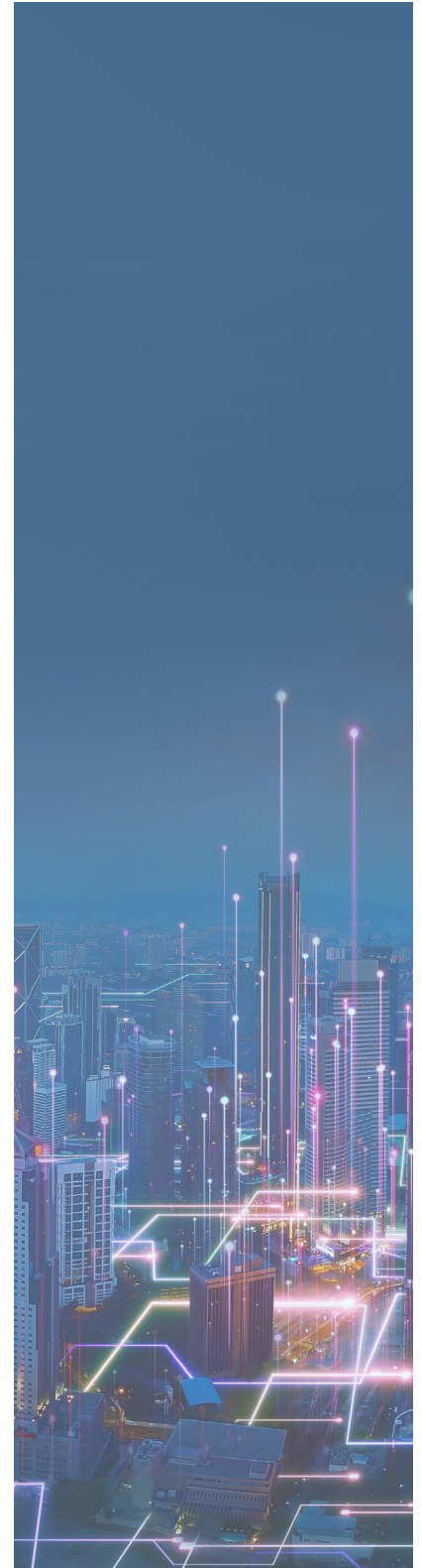
EXECUTIVE SUMMARY

The East African Community (EAC) is at an important point in the development of a regional approach to governing cross-border data flows. In June 2026, representatives of all eight Partner States met in Dar es Salaam, through the EAC Technical Working Group on Data Protection and Cybersecurity Harmonised Frameworks, to review and validate a proposed Cross-Border Data Flows Framework (the "Framework"). The Framework is intended to support secure data flows, protect privacy and facilitate digital trade. The likely next step is consideration of the framework by the relevant EAC Sectoral Council, including approval to commence legislative drafting. This creates a timely opportunity to shape the eventual regional legal instrument and its implementation.

This rapid assessment, commissioned by the American Chamber of Commerce, Kenya, examines how cross-border data flows create economic value in the EAC, how regulatory fragmentation constrains that value, and what the evidence implies for the design and implementation of the proposed Framework.

There is a clear economic case for getting cross-border data flows right. Reducing unnecessary barriers to the movement of data can lower the cost of operating across the EAC and support trade, investment and the scaling of digital services. Cross-border data flows increasingly form part of the infrastructure through which firms coordinate regional supply chains, settle payments, use cloud and enterprise services, analyse operational data and serve customers across multiple markets without duplicating systems in each country.

At the macroeconomic level, they support digitally delivered services, payments, merchandise trade and investment in shared digital infrastructure. Based on calculations conducted for this report, it is estimated that EAC digitally delivered services exports increased from around US\$1.9 billion in 2015 to US\$2.8 billion in 2024, although growth has lagged global and wider African comparators. Intra-EAC merchandise trade reached US\$19.3 billion in 2025, illustrating the scale of regional activity increasingly supported by interoperable customs, logistics, banking and other data systems.¹





The economic gains from regional integration can, however, be weakened where data must navigate fragmented or duplicative regulatory processes. Partner States currently apply different transfer models and administrative requirements, including differing approaches to authorisation, localisation and regulatory oversight. For firms operating across several EAC markets, this can mean repeating registrations, contractual arrangements, approvals, legal reviews and technical adaptations rather than relying on a single predictable regional framework. Interviews conducted for this rapid assessment illustrate the practical costs. One business reported repeating the same administrative process roughly 11 times across jurisdictions, while some firms estimated that regulatory back-and-forth over regional transfers can delay product launches by three to six months. Evidence reviewed for the assessment also indicates that forced localisation can increase local IT infrastructure costs.

Facilitating data flows without adequate safeguards would carry its own economic costs. Cross-border processing can increase exposure to cybersecurity incidents, unauthorised access, misuse of personal data and uncertainty over accountability where several jurisdictions and service providers are involved. INTERPOL reports that cybercrime accounts for more than 30% of all reported crime in Eastern and Western Africa, and 86% of surveyed African countries said their international cooperation capacity for cybercrime needs improvement.² The policy objective is therefore not simply to maximise the volume of data moving across the region. It is to enable trusted data flows, supported by effective privacy, cybersecurity, accountability and regulatory cooperation.

The economic case for harmonisation therefore rests on achieving both objectives at the same time. The EAC needs sufficiently common and interoperable rules to reduce duplication, approvals and uncertainty, while maintaining safeguards strong enough to protect individuals, businesses and public institutions. Harmonisation creates economic value where it makes lawful cross-border activity more predictable and less costly without weakening protection. Conversely, convergence around a highly duplicative or administratively burdensome model would leave much of the economic rationale for regional harmonisation unrealised.

This has direct implications for the development of the proposed EAC Framework.

National filing, approval and due-diligence procedures could be streamlined, while maintaining Partner States' national supervisory and enforcement authority. Requirements should be risk-based and proportionate so that routine, lower-risk transfers are not subject to the same burden as higher-risk activity. Data localisation should be treated as an exception where justified and should not undermine regional integration objectives or legitimate data flows supporting trade, health, e-commerce and digital services. Implementation capacity will also be critical: without stronger and more even regulatory capability across Partner States, harmonisation could formalise existing differences rather than resolve them.

The EAC has an opportunity to generate practical implementation lessons while the emerging framework is developed.

An interim arrangement between participating national regulators could test more consistent approaches to demonstrating and verifying compliance with data protection requirements, within existing national mandates and where legally feasible. This could include aligning the evidence businesses provide on transfer safeguards, allowing equivalent compliance information to be reused across jurisdictions and applying scrutiny proportionate to the risks of each transfer. Testing these approaches with regulators and businesses could establish whether they reduce repeated filings and due diligence without weakening protection, identify remaining incompatibilities between national requirements and inform future regional implementation.

EAC DIGITALLY
DELIVERED SERVICES
EXPORTS INCREASED
FROM AROUND

US\$1.9B

IN 2015 TO AROUND

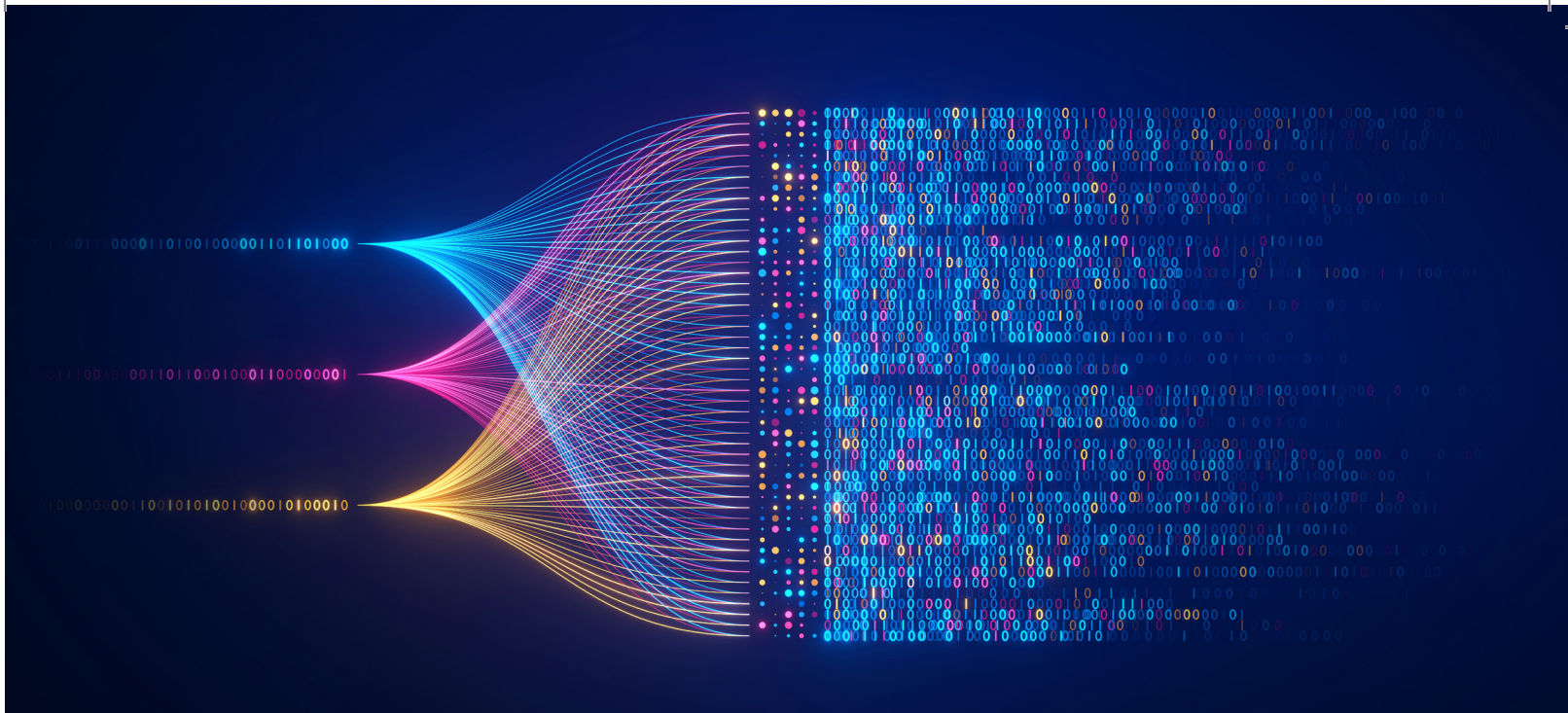
US\$2.8B

IN 2024



¹ East African Community. (2026). EAC Quarterly Statistics Bulletin: October-December 2025 (Issue 11). Available: <https://www.eac.int/documents/category/statistics>; East African Community. (2025, August 4). EAC launches Regional Customs Bond to unlock trade efficiency. Available: <https://www.eac.int/press-releases/3401-eac-launches-regional-customs-bond-to-unlock-trade-efficiency>.

² International Criminal Police Organisation. (2025). New INTERPOL report warns of a sharp rise in cybercrime in Africa. Available: <https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa>.



01. INTRODUCTION

1.1 CONTEXT & WHY NOW



Cross-border data flows are increasingly part of the infrastructure through which the EAC economy operates. They allow firms to coordinate regional supply chains, process payments, use cloud-based services, manage customers and operations, and deliver services across markets. They also support trade in goods through the movement of logistics, customs and other operational data. As the region becomes more digital and service-oriented, the ability to move data securely and predictably across borders is therefore becoming more important to trade, investment and firm productivity.



As cross-border data flows have expanded, so too have concerns about how data is protected once it moves beyond national borders. Greater volumes of personal, financial and other sensitive data moving between jurisdictions have heightened concerns around privacy, cybersecurity, regulatory oversight and the ability of individuals to seek redress when data is misused. Governments have responded by strengthening data-protection and transfer rules. Across the EAC, however, these rules have developed largely at national level and in different ways, producing a fragmented regulatory landscape that businesses must navigate when operating across the region. The policy challenge is therefore not whether cross-border data flows should be regulated, but how to provide credible protection without creating unnecessary barriers to legitimate regional data movement.



Momentum on this question is building at continental level, but it falls to Regional Economic Communities (RECs) to convert that momentum into interoperable rules on the ground. Both the African Union's Data Policy Framework and the African Union Commission's Digital Transformation Strategy treat the alignment of national transfer rules as a priority, on the reasoning that a continental digital market cannot operate on 55 separate and mutually incompatible data regimes.^{3,4} That position has since been carried into trade law: through the Digital Trade Protocol to the African Continental Free Trade Area (AfCFTA) agreement, African states have committed in principle to open data transfers.⁵ The East African Community (EAC), as one of the continent's RECs, is where this commitment must be given operational form for its eight Partner States (Burundi, the Democratic Republic of the Congo (DRC), Kenya, Rwanda, Somalia, South Sudan, Tanzania and Uganda), through the development and implementation of a harmonised regional framework.



Globally, cross-border data transfer systems take fundamentally different approaches to privacy and regulation. The Global Cross-Border Privacy Rules (CBPR) system, which can be classified as an open transfer model, seeks to facilitate trusted cross-border data flows through organisational accountability and voluntary certification against common privacy requirements by recognised third-party Accountability Agents. Its approach combines certification with enforceable requirements and cross-border regulatory cooperation to support interoperability between different national privacy laws. In contrast, conditional transfer models, such as the European Union's (EU) General Data Protection Regulation (GDPR), permit transfers only once a defined safeguard is in place, such as adequacy finding, standard contractual clauses, binding corporate rules, certification, or consent. **At the regional level, however, data governance across the EAC remains highly fragmented.** The eight Partner States operate across distinct models of cross-border data governance, ranging from open, conditional and controlled data transfer regimes, with some requiring case-by-case regulatory authorisation and others with no operative framework at all. **Businesses operating across more than one Partner State must navigate different legal, regulatory and compliance requirements, which raises the cost of doing business regionally and limits the extent to which firms can treat the EAC as a single, integrated market.**

³ African Union (2022). AU Data Policy Framework. African Union Commission. Available: <https://au.int/en/documents/20220728/au-data-policy-framework>

⁴ African Union (2020). The Digital Transformation Strategy for Africa (2020–2030). African Union Commission. Available: <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>

⁵ African Continental Free Trade Area. Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade. Available: <https://au.int/en/treaties/protocol-agreement-establishing-african-continental-free-trade-area-digital-trade>



The EAC has made significant progress on advancing a coherent and interoperable regional approach to data protection and cross-border data flows. At a meeting of the Technical Working Group (TWG) on Data Protection and Cybersecurity Harmonised Frameworks, held in Dar es Salaam in June 2026, representatives of all eight Partner States met to review and validate a proposed Cross-Border Data Flows Framework⁶. The proposed Framework is intended to support secure data flows, protect privacy and facilitate digital trade.



The timing of this report reflects a narrow but important window for input into the direction of the regional framework. While the framework is already substantively developed, a major challenge remains: aligning individual Partner States' national processes with the regional framework so they complement one another, rather than creating duplicative compliance burdens for businesses.

1.2 APPROACH AND METHODOLOGY

This report is a rapid, high-level outline of how cross-border data flows create economic value, how current fragmentation in relevant laws across the EAC is preventing that economic value from being realised, and how the proposed Framework could help solve this barrier to economic growth. This report draws on:

1. Existing literature, international and regional benchmarks, trade and investment data, and EAC and national policy and regulatory documents; and
2. Key Informant Interviews (KIIs) conducted with seven digitally enabled businesses operating across EAC Partner States, spanning the technology, banking, payments, fintech and asset-finance sectors. The analysis also incorporated two written submissions from AmCham members.

Quantitative evidence in this report comprises official statistics, author calculations, published study estimates and survey findings, respondent-reported experiences, and illustrative case studies. These evidence types are identified alongside the relevant claims. Interviews with seven businesses, excluding SMEs, provide illustrative accounts of operational frictions; figures reported by respondents are not representative EAC averages. Findings concerning SMEs draw on the reviewed literature and the report's analysis, rather than direct SME interviews. Estimates from studies covering Africa or the global economy should not be interpreted as estimates of the effects of EAC harmonisation.

HOW TO READ THIS REPORT

This report examines the economic case for cross-border data flows in the context of the EAC's ongoing work towards a regional harmonisation framework. The EAC's public communication of 25 June 2026 describes a proposed Framework under review, intended to facilitate secure data flows, safeguard privacy and support digital trade. Throughout this report, the emerging EAC harmonisation framework, or the framework, refers to this developing regional approach.

Our analysis draws on published research, economic data and business consultations to consider the framework's anticipated elements, their potential economic implications and priorities for its development.

WHAT YOU MAY WANT TO USE THIS REPORT FOR

1. **Understanding the policy direction:** the publicly stated objectives of regional harmonisation and the high-level elements our research suggests could support them.
2. **Understanding the economic and business implications:** how cross-border data flows create value, and how the design and implementation of a regional framework could affect firms operating across the EAC.
3. **Identifying implementation priorities:** where regulatory fragmentation, national procedures, institutional capacity or other practical issues could limit the benefits of harmonisation.
4. **Informing policy and advocacy:** identifying design choices and complementary measures that could support trusted and effective cross-border data flows as the framework develops.

Discussion of anticipated framework elements and possible implementation arrangements reflects our analysis and recommendations, rather than confirmation of agreed provisions, formal adoption or operational status.

⁶ East African Community. (2026, June 25). EAC advances development of regional framework for secure cross-border data flows to power East Africa's digital economy [Press release]. <https://www.eac.int/eadrip-news-updates/eadrip-press-releases/3554-eac-advances-development-of-regional-framework-for-secure-cross-border-data-flows-to-power-east-africa-s-digital-economy>.



02. THE ECONOMIC VALUE OF CROSS-BORDER DATA FLOWS

The economic value of cross-border data flows ultimately depends on how businesses use data to operate, trade and expand across markets. In practice, businesses leverage cross-border data through several distinct operational mechanisms:



SUPPLY CHAIN, LOGISTICS, AND TRADE DATA

Businesses operating regional value chains (agribusiness, manufacturing, distribution) use cross-border data flows to coordinate inventory, customs declarations, and logistics across the EAC's Common Market.

Economic value is generated primarily through lower transaction and coordination costs, and higher productivity. Real-time or near-real-time sharing of orders, inventory, shipment, customs, and demand data allows firms to optimise stocks, reduce delays and waste, improve asset utilisation, and coordinate production across multiple countries. Better data also makes it easier for firms to participate in regional value chains by reducing the information costs associated with finding suppliers, managing cross-border shipments, and meeting regulatory requirements.

CLOUD, ENTERPRISE, AND INFORMATION TECHNOLOGY (IT) DATA

Firms across sectors increasingly run core operations, such as analytics, Human Resources (HR), customer relationship management, and Artificial Intelligence (AI), on cloud infrastructure located outside their home country. UNCTAD reports that Africa hosts less than 1% of global data centre capacity.⁷

Economic value is generated through productivity gains, lower IT costs, and access to capabilities that would otherwise be unavailable or prohibitively expensive. Cross-border data transfers allow firms to use cloud computing, data analytics, AI, cybersecurity, and enterprise software without having to build equivalent infrastructure domestically. This enables firms to scale computing capacity on demand, reduce upfront capital expenditure, automate business processes, improve decision-making, and develop new digital products and services. The ability to access global cloud infrastructure can therefore increase the productivity and competitiveness of firms, particularly SMEs and startups that could not economically maintain their own data infrastructure.

A 2025 survey, reported by CIO Africa, of organisations across Sub-Saharan Africa found cloud computing was the leading digital priority, with 61% adoption, ahead of AI (55%) and analytics/cybersecurity (44% each) - meaning a majority of surveyed firms already depend on cross-border data transfer as an operational backbone.⁸ Notably, over 80% of African tech startups rely on foreign-owned cloud infrastructure providers, underscoring how dependent even domestically-focused digital firms are on data leaving the continent and returning as a processed service.⁹

⁷ United Nations Conference on Trade and Development (2024). Digital economy report 2024. Available: https://unctad.org/system/files/official-document/der2024_en.pdf

FINANCIAL AND TRANSACTIONAL DATA (MOBILE MONEY, PAYMENTS, DIGITAL BANKING)

Mobile network operators, fintechs, and banks depend on the ability to transmit transaction, identity, and credit-scoring data across borders to run interoperable payment systems, detect fraud, and extend credit.

Economic value is generated through several channels: cross-border financial data enables faster and lower-cost payments, expands the pool of customers that financial institutions can serve, improves credit assessment and reduces lending risk, and allows firms to detect fraud more effectively. Interoperability also increases the volume and frequency of transactions that platforms can process, generating fee and transaction revenues while enabling businesses and households to participate more easily in regional and international commerce.



GSMA industry figures identify East Africa as the global epicentre of this activity: the region was the leading driver of new mobile money account growth in 2024, contributing 32% of new accounts worldwide, and mobile money agent growth in East Africa outpaced every other region at 53% year-on-year in 2025.¹⁰ The same report puts Sub-Saharan Africa's mobile money ecosystem at US\$1.1 trillion in transaction value in 2024 (65% of the global total) and contributed an estimated US\$190 billion to regional GDP in 2023, up from US\$150 billion the year before.¹¹

A study of fintech adoption across Sub-Saharan Africa demonstrate that integrating digital payments and remittance corridors reduces average transaction costs from 9.0% to just 3.8% (a 57.78% reduction) and accelerates transaction times from 2 to 5 days to under 24 hours, with 65% of users achieving real-time transactions.¹²

Firms in this category, such as telecom-linked mobile money providers (e.g., M-Pesa-type platforms), digital lenders, and payment aggregators, rely on cross-border data transfer to interoperate across East Africa and to connect with international remittance and card networks.

⁸ CIO Africa (2025). CIO100 Megatrends Report Highlights Africa's Top 25 Tech Trends. Available: <https://cioafrica.co/cio100-mega-trends-report-highlights-africas-top-2025-tech-trends/>

⁹ Partech Partners (2024). 2024 Africa Tech Venture Capital. Available: <https://partechpartners.com/africa-reports/2024-africa-tech-venture-capital-report>

¹⁰ GSMA (2025). The State of the Industry Report on Mobile Money 2026. Available: <https://www.gsma.com/sotir/>

¹¹ *Ibid.*

¹² Abubakar, A. N., Iro, H. N., Akawu, U. H. and Ahmad, S. S. (2026). Empowering Small Businesses Through Fintech Adoption in Cross Border Payments in Africa. Journal of Community Service, 2(4). Available: <https://doi.org/10.62569/jics.v2i4.242>



BIOMETRIC AND IDENTITY DATA

Digital identity verification firms use biometric data - often shared across jurisdictions - to power know-your-customer (KYC) checks, reduce fraud, and enable financial inclusion.

Economic value is generated by reducing the cost and time of customer onboarding, lowering fraud and compliance costs, and enabling firms to serve customers who would otherwise be difficult or expensive to verify. Cross-border access to identity data can also allow individuals and businesses to establish trusted credentials across markets, expanding their ability to access financial services, employment, telecommunications, and other digital services. For providers, this translates into lower customer-acquisition and verification costs, reduced losses from fraud, and a larger addressable customer base.



E-COMMERCE AND PLATFORM DATA

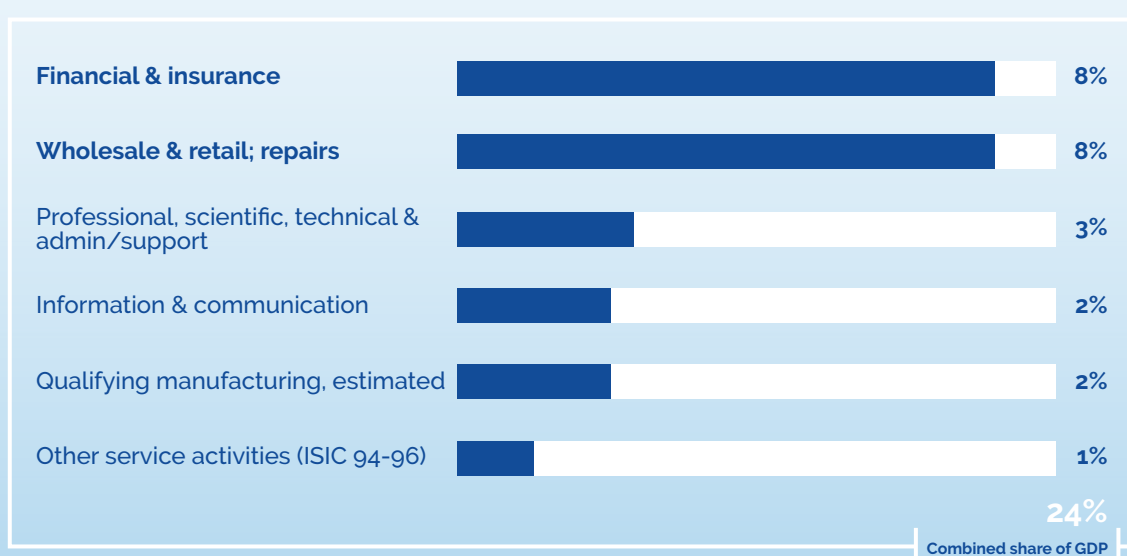
Small and medium enterprises (SMEs) trading through cross-border e-commerce platforms rely on data flows for payments, customer data, and marketing.

Economic value is generated by expanding market access and reducing the fixed costs of selling across borders. Cross-border data allows platforms to match buyers and sellers, process payments, personalise marketing, manage customer relationships, verify transactions, and coordinate fulfilment. This enables SMEs to reach customers outside their home market without establishing a physical presence in each country, increasing potential sales while lowering customer-acquisition, transaction, and distribution costs. At the platform level, greater volumes of transactions and users can generate additional revenues from commissions, advertising, payments, and other digital services.

When firm-level benefits are multiplied across businesses and sectors, the microeconomic gains from cross-border data flows can translate into broader macroeconomic benefits. One of the main channels through which restrictions on cross-border data flows affect the economy is trade, particularly trade in services and other data-reliant activities.¹³ **This channel is becoming increasingly important for the EAC as services take on a larger role in regional economies.** Since 1990, the shares of employment and real value added accounted for by services in East Africa have grown more rapidly than those of manufacturing.¹⁴ At the same time, services are becoming increasingly digital and tradable across borders. As regional economic integration and digitisation deepen, a growing share of economically significant activity therefore depends on data being able to move securely, predictably and efficiently between Partner States.

Understanding the economic significance of data-exposed sectors in the EAC is the first step to understanding the role of data flows in the macroeconomy. In the absence of EAC-wide sector data, the report uses Kenya as an illustration. Applying the sector classification drawn from Frontier Economics to Kenya National Bureau of Statistics data, the report estimates that data-reliant and traded industries generated around 24% of Kenya's Gross Domestic Product (GDP) in 2025, as shown in Figure 1.^{15,16} While Kenya's economy is not representative of other EAC states, it is a useful example of what the economic footprint of data-reliant industries can look like in a relatively large, services-oriented and diversified EAC economy.

Figure 1: Contribution of data-exposed, traded sectors to Kenya's GDP



Author estimate using Kenya National Bureau of Statistics data and the sector classification drawn from Frontier Economics (2021). Illustrative of Kenya, not an EAC-wide estimate.¹⁷

¹³ Frontier Economics (2021). The value of cross-border data flows to Europe: Risks and opportunities. DIGITALEUROPE. Available: https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf

¹⁴ Hamilton, C., Mensah, E., Sennoga, E. 2026. Services-led structural transformation in East Africa, Journal of African Economies, Volume 35, Issue 4, 2026, ejag013, <https://doi.org/10.1093/jae/ejag013>

¹⁵ Frontier Economics (2021). The value of cross-border data flows to Europe: Risks and opportunities. DIGITALEUROPE. Available: https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf

¹⁶ The list of data-reliant and traded sectors is borrowed from Frontier Economics. (2021). The value of cross-border data flows to Europe: Risks and opportunities. DIGITALEUROPE. Available: <https://www.digitaleurope.org/resources/the-value-of-cross-border-data-flows-to-europe-risks-and-opportunities/>

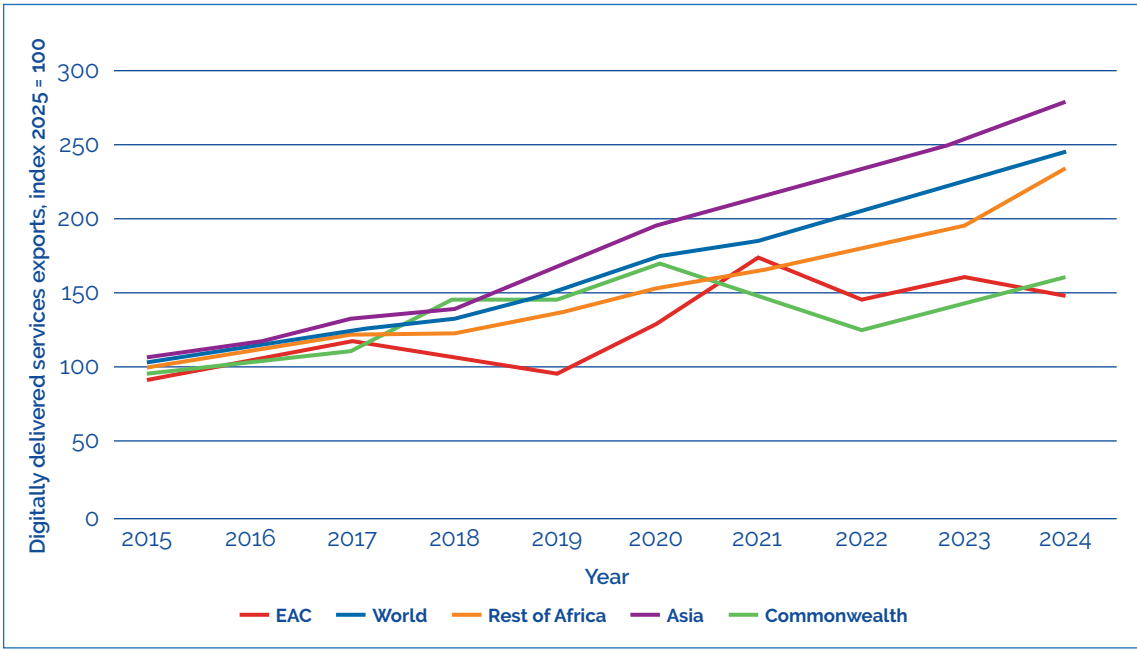
¹⁷ GDP statistics taken from Kenya National Bureau of Statistics. (2018). Census of industrial production and construction report 2018. Kenya National Data Archive. <https://statistics.knbs.or.ke/nada/index.php/catalog/126>, Kenya National Bureau of Statistics. (2026a). 2026 economic survey. <https://www.knbs.or.ke/reports/2026-economic-survey/>, Kenya National Bureau of Statistics. (2026b). Quarterly gross domestic product: First quarter 2026. <https://www.knbs.or.ke/reports/quarterly-gross-domestic-product-first-quarter-2026/>

The macroeconomic value of cross-border data flows can broadly be seen through the following trade and investment channels:

Digitally delivered services provide the clearest macroeconomic channel through which cross-border data flows support exports. Digital trade encompasses international trade that is digitally ordered and/or digitally delivered. For digitally delivered services, including financial, telecommunications, professional and cloud-enabled services, cross-border data transmission is the mechanism through which the service reaches the customer and the export transaction takes place. **The EAC is performing below its potential in digitally delivered services growth.** The following comparison uses author calculations from the digitally delivered services trade dataset cited below. The EAC aggregate covers seven Partner States; Somalia is not reported in the dataset and is not treated as zero. Since 2015, EAC digitally delivered services exports have increased from about US\$1.9 billion to US\$2.8 billion in 2024, an increase of around 50%. This is substantially weaker than elsewhere: over the same period, digitally delivered services exports grew by around 144% globally, 134% in the rest of Africa and 178% in Asia.

Figure 2 compares these growth trajectories by setting each region's 2015 export value equal to 100, allowing differences in growth to be compared despite large differences in the absolute size of their exports. It shows that the EAC briefly accelerated in 2021-22, when exports reached about US\$3.2 billion, but this momentum was not sustained. By 2024, EAC exports had fallen back to US\$2.8 billion, while exports in the comparator regions continued to expand.¹⁸

Figure 2: Growth in digitally delivered services by region (2015-2024)



Source: Author calculations from the digitally delivered services trade dataset. Values are in current US dollars and indexed to 2015 = 100. The EAC aggregate excludes Somalia because its data are not reported.¹⁹

¹⁸ WTO. 2025. Digitally Delivered Services Trade Dataset. Available: https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm

¹⁹ World Bank Digitally Delivered Services Trade dataset; author calculations. Export values are in current US dollars and indexed to 2015 = 100. EAC comprises Burundi, DRC, Kenya, Rwanda, South Sudan, Tanzania and Uganda; Somalia is not reported in the dataset and is not treated as zero. Rest of Africa comprises observed African countries excluding these EAC members. Asia and CIS use the dataset's regional aggregates. Dataset available: https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm

These figures demonstrate the untapped potential for EAC digital trade flows. By better enabling these services to be supplied regionally and internationally, data mobility can support foreign exchange earnings and export diversification, while access to imported digital services can provide productive inputs to domestic firms.



CROSS-BORDER PAYMENT DATA UNDERPIN THE SETTLEMENT INFRASTRUCTURE FOR REGIONAL TRADE, REMITTANCES AND FINANCIAL FLOWS.

Cross-border payment data are macroeconomically significant because payment systems provide the settlement infrastructure for regional trade, remittances and financial flows. According to World Bank data, recorded personal remittances alone exceeded US\$10 billion across Kenya, the DRC, Uganda, Tanzania, Rwanda and Burundi in 2024, before accounting for the much larger universe of payments associated with merchandise trade, services and investment²⁰

The macroeconomic significance is enabling rather than additive: payment data do not themselves constitute output, but they are necessary for cross-border transactions to be settled. The EAC's Cross-Border Payment System Masterplan treats regional payment connectivity, including interoperable instant payments, real-time gross settlement and cross-border mobile money, as part of the infrastructure required for deeper economic integration. More efficient cross-border payment data flows can therefore lower settlement frictions and make it easier for firms and households to transact across EAC markets, making data mobility part of the financial infrastructure underpinning regional economic integration.²¹

²⁰ World Bank. World Development Indicators: Personal remittances, received (current US\$), indicator BX.TRF.PWKR.CD.DT. IMF balance-of-payments data and World Bank staff estimates. Author calculation summing 2024 values for Kenya, the Democratic Republic of the Congo, Uganda, Tanzania, Rwanda and Burundi. Available: <https://data.worldbank.org/indicator/BX.TRF.PWKR.CD.DT>. Accessed 3 September 2026.

²¹ *Ibid.*



CROSS-BORDER DATA FLOWS SUPPORT MERCHANDISE TRADE BY REDUCING THE INFORMATION AND COORDINATION COSTS OF MOVING GOODS ACROSS BORDERS.

Customs declarations, transit guarantees, cargo-tracking information, payment instructions and logistics data increasingly move between jurisdictions before or alongside the physical shipment. **Intra-EAC merchandise trade reached US\$19.3 billion in 2025 - up 28% from US\$15.1 billion in 2024** - while total EAC merchandise trade with the world reached US\$156.6 billion.

As the EAC seeks to increase intra-regional trade, interoperable systems linking customs, logistics, banking, insurance and ports can reduce delays and administrative frictions across this substantial trade base. Cross-border data mobility is therefore part of the trade-facilitation infrastructure that allows goods to move more efficiently through the regional market.²²



A MORE INTEGRATED REGIONAL DATA MARKET CAN STRENGTHEN THE ECONOMICS OF INVESTMENT IN DIGITAL INFRASTRUCTURE.

Data centres, cloud infrastructure and shared digital services involve substantial fixed costs, making investment harder to justify where demand is fragmented across small national markets. The World Bank's Eastern Africa Regional Digital Integration Project identifies regional integration as a means of generating economies of scale and lowering the cost of digital infrastructure.²³ By allowing firms to serve demand across several EAC markets through shared systems, more interoperable data governance can increase infrastructure utilisation and improve the commercial case for investment. The macroeconomic channel is therefore indirect but important: regional scale can support greater capital investment in the digital infrastructure on which wider productivity and digitalisation depend.

²² East African Community. (2026). EAC Quarterly Statistics Bulletin: October–December 2025 (Issue 11). Available: <https://www.eac.int/documents/category/statistics>; East African Community. (2025, August 4). EAC launches Regional Customs Bond to unlock trade efficiency. Available: <https://www.eac.int/press-releases/3401-eac-launches-regional-customs-bond-to-unlock-trade-efficiency>.

²³ World Bank (2021). Eastern Africa Regional Digital Integration Project (P176181): Concept Project Information Document (Report No. PIDC31823). Available: <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/823091633534271893>.



TRUSTED DATA FLOWS ARE THE ENABLING INFRASTRUCTURE FOR DIGITAL TRANSFORMATION.

Trusted data flows allow data to be securely shared, governed and reused across systems and borders. They underpin AI development and deployment, strengthen global threat intelligence and cybersecurity, and enable research collaboration by connecting data, expertise and computing resources. They also support reliable digital public services and operational resilience, including disaster recovery, by allowing critical information to move between organisations when needed. **At a regional level, trusted and interoperable data exchange is a core component of digital public infrastructure (DPI), alongside digital identity and payments, enabling governments to deliver joined-up services at scale.**²⁴ In short, trusted data flows turn fragmented digital capabilities into connected, resilient systems.

Taken together, the macroeconomic significance of cross-border data flows lies in their horizontal role across several large and growing parts of the EAC economy. They enable digitally delivered services exports, underpin cross-border payments, support the information and coordination systems required for merchandise trade, and can strengthen the economics of regional digital infrastructure investment. As the EAC becomes more service-oriented, digitally connected and regionally integrated, a growing share of economic activity depends on information moving securely and efficiently across borders. Cross-border data governance is therefore increasingly part of the economic infrastructure underpinning the EAC Common Market.

INTRA-EAC
MERCHANDISE
TRADE REACHED

\$19.3B

IN 2025, UP

28%

FROM

\$15.1B

IN 2024.

²⁴ OECD (2026). Digital Government Outlook 2026: From Foundations to Transformational Impact. Available: <https://doi.org/10.1787/0496b2bc-en>.



03. BARRIERS TO REALISING ECONOMIC VALUE FROM CROSS-BORDER DATA FLOWS

3.1 CURRENT STATE OF REGULATORY FRAGMENTATION

While there are economic benefits for enabling cross-border data flows within the EAC, this connectivity is not without its challenges. The same movement of information that supports digitally delivered exports, payment settlement and regional value chains also carries real risks where it is poorly governed. Personal data may end up in jurisdictions offering weaker protection and no practical route to redress for the individual concerned. The financial, biometric and identity records that underpin mobile money and KYC systems are precisely the categories most valuable to fraudsters and most damaging when exposed. Regulators can lose visibility over where data is held, who is accountable when it is compromised, and which authority is competent to act.

As a result of these legitimate concerns, governments across the continent have ramped up their efforts to regulate cross-border data flows. Every EAC Partner State now regulates personal data in some form, but in varying ways, and with no State treating another as an automatically trusted destination for data. Seven of the eight Partner States have enacted a dedicated data protection law: Kenya (2019), Uganda (2019), Rwanda (2021), Tanzania (2022), the Democratic Republic of Congo (2023, via its Digital Code), Somalia (2023), and Burundi (2026). South Sudan remains the outlier, with no civil data protection law and only a security-focused cybercrime statute in force. Institutional capacity lags legislation further still: of the eight Partner States, only five (Kenya, Rwanda, Somalia, Tanzania and Uganda) have a functioning, dedicated data protection authority.²⁵ This asymmetry between countries creates a number of challenges for businesses operating across the EAC, as will be discussed in the next section, and explains why the EAC's Cross-Border Data Flows Framework is being pursued as a matter of priority.²⁶

Table 1 maps the national rules and regulations across the four elements that also anchor the emerging EAC Framework:

1. Lawful transfer mechanisms

Meaning the legal routes through which a business may move personal data out of the jurisdiction. Every regime permits transfers in principle; what differs is what a firm must do, and who must agree, before the data moves. The eight Partner States are classified into three models. These categories describe the intensity and timing of regulatory requirements for cross-border transfers of personal data, including whether firms must satisfy specified conditions or obtain prior regulatory authorisation. They do not rank national regimes or assess the quality of national privacy protection.

A **Open: South Sudan.** Transfers may proceed without any prior condition, with protection resting on general legal accountability after the fact. South Sudan falls into this category by default rather than by design: the position is open because no comprehensive data protection regime has been enacted, not because the country has deliberately adopted an accountability-based model of the kind found in the CBPR system, which pairs open transfers with certification against common privacy standards. For businesses, the practical result is permissive but not predictable, since a Data Protection Bill under validation could change the position materially and at short notice.

B **Conditional: Kenya, Uganda, Somalia and Burundi.** This means that transfers are permitted, but only once a defined condition is satisfied in advance: adequacy of the destination, standard contractual clauses, binding corporate rules, certification, codes of conduct or data subject consent. The controller generally assesses for itself whether the condition is met, so transfers do not require case-by-case sign-off, but the firm carries the burden of documenting and defending that assessment.

C Controlled: Rwanda, Tanzania and DRC. This means that transfers require case-by-case authorisation from the regulator, and may be subject to local storage or processing mandates, infrastructure requirements or prior security assessment. Data cannot lawfully move until the regulator has approved it, placing the timing of a transfer outside the firm's control.

²⁶ East African Community. (2026, 25 June). EAC advances development of Regional Framework for Secure Cross-Border Data Flows to power East Africa's digital economy [Press release]. Available: <https://www.eac.int/eardip-news- updates/eardip-press-releases/3554-eac-advances-development-of-regional-framework-for-secure-cross-border-data-flows-to-power-east-africa-s-digital-economy?highlight=WyJwb2ludHMiLCBjZCZkaWwNlcyslnNdydisIndvcmtzAGwIiwiaG9ic2VobzXklxwiczVdmdVslwicicj-RhdGl zdGliYcslsiFzdClsmFmzmFnbnMjLCBjZy7YTYSJldXum>. Source: chatgpt.com.

²⁶ East African Community (2026) EAC Technical Working Group on Data Protection and Cybersecurity Harmonised Frameworks, Fourth Meeting, Dar es Salaam, 23-27 June 2026 (validation of the Cross-Border Data Flows Framework; noting that only five of eight Partner States had established dedicated data protection authorities). Available: <https://www.eac.int/press-releases/3287-eac-readies-to-accelerate-regional-digital-integration-with-cross-border-data-flow-framework>.

2. Data localisation requirements

Meaning rules obliging firms to keep certain categories of data, or a copy of them, on servers inside the country. These range from explicit statutory mandates to sectoral rules in finance and telecommunications, through to de facto localisation, where no rule formally requires domestic storage but the evidentiary or authorisation burden on transfers is heavy enough that firms localise anyway.

Table 1: Data governance regimes across the EAC's eight Partner States

Jurisdiction	Core legal instrument	Supervisory authority	Data model for transfer mechanisms	Data localisation
SOUTH SUDAN	No civil data protection law; governed by the Cybercrime and Computer Misuse Act, 2026 (signed 18 February 2026). ^{27,28}	None. No dedicated data protection authority	Open (by default) South Sudan does not have a comprehensive enacted data-protection regime but a dedicated Data Protection Bill has been drafted and was undergoing validation in May 2026. ²⁹	No explicit mandate
KENYA	Data Protection Act, 2019 (ss.48-50) ³⁰	Office of the Data Protection Commissioner (ODPC), active, enforcing ³¹	Conditional Kenya's Office of the Data Protection Commissioner has not issued any adequacy decisions to date and closed a public consultation on more detailed cross-border transfer guidance in May 2026. ³²	Sectoral (finance, telecoms); as well as data concerning strategic state interests
UGANDA	Data Protection and Privacy Act, 2019 (s.19) ³³	Personal Data Protection Office (PDPO), active, enforcing ^{34,35}	Conditional Uganda's statute does not recognise "legitimate interest" as a standalone lawful basis for processing, instead it starts from the principle of consent and lists specific exceptions. ³⁶ Uganda's Personal Data Protection Office has also shown a clear willingness to assert jurisdiction over offshore processors regardless of local presence.	No explicit mandate; defensive localisation common

²⁷ Data Protection Africa. South Sudan Fact Sheet (no dedicated data protection legislation). Available: [https://dataprotection.africa/south-sudan/Radio Tamazuj \(2025\). South Sudan to get data protection bill in 2026, says minister. Available: https://www.radiotamazuj.org/en/news/article/south-sudan-to-get-data-protection-bill-in-2026-says-minister](https://dataprotection.africa/south-sudan/Radio Tamazuj (2025). South Sudan to get data protection bill in 2026, says minister. Available: https://www.radiotamazuj.org/en/news/article/south-sudan-to-get-data-protection-bill-in-2026-says-minister)

²⁸ Committee to Protect Journalists (2026). South Sudan's new cybercrime law ramps up threat of jail for journalists. Available: <https://cpj.org/2026/04/south-sudans-new-cybercrime-law-ramps-up-threat-of-jail-for-journalists/>

Jurisdiction	Core legal instrument	Supervisory authority	Data model for transfer mechanisms	Data localisation
SOMALIA	Data Protection Act, 2023 (Law No. 005) ³⁷	Data Protection Authority, transitioning; established 2023	Conditional Permits transfers on an adequacy-or-safeguard basis broadly consistent with international norms.	No general mandate identified
BURUNDI	Loi n°1/03 du 10 mars 2026 ³⁸	Independent authority created in law; composition and powers pending implementing decree	Conditional Burundi's newly enacted law serves as a basis for transfer of data as of March 2026. ³⁹ Permits transfers on the basis of sufficient protection in the destination country or, for countries outside the ministerial list, adequate safeguards adopted by the recipient and approved by Burundi's data protection authority.	No general mandate identified
TANZANIA	Personal Data Protection Act, 2022 (Act No. 11) ⁴⁰	Personal Data Protection Commission (PDPC), transitioning; enforcing registration only from April 2026	Controlled Focuses on pre-authorisation or permit-based authorisation that requires regulatory sign-off before a transfer can proceed. ⁴¹	No blanket mandate; high evidentiary burden drives de facto localisation

²⁹ Data Protection Africa. South Sudan Fact Sheet (no dedicated data protection legislation). Available: <https://dataprotection.africa/south-sudan/>; Committee to Protect Journalists. (2026, April). South Sudan's new cybercrime law ramps up threat of jail for journalists (Cybercrimes and Computer Misuse Act, 2026, signed 18 February 2026). Available: <https://cpj.org/2026/04/south-sudans-new-cybercrime-law-ramps-up-threat-of-jail-for-journalists/>; Radio Tamazuj. (2025, December). South Sudan to get data protection bill in 2026, says minister. Available: <https://www.radiotamazuj.org/en/news/article/south-sudan-to-get-data-protection-bill-in-2026-says-minister>

³⁰ Republic of Kenya, Data Protection Act, No. 24 of 2019, ss.48–50; Office of the Data Protection Commissioner (2026). Guidance Note on Cross-Border Data Transfers. Available: <https://www.odpc.go.ke/wp-content/uploads/2026/04/Guidance-Note-on-Cross-border-Data-Transfers.pdf>

³¹ ODPC (2025). Pre-Conference Breakfast Meeting with Journalists in Eldoret Ahead of Data Privacy Day 2025

³² Republic of Kenya, Data Protection Act, No. 24 of 2019, ss.48–50; Office of the Data Protection Commissioner. (2026, April). Guidance Note on Cross-Border Data Transfers (draft, consultation closed 15 May 2026). Available: <https://www.odpc.go.ke/wp-content/uploads/2026/04/Guidance-Note-on-Cross-border-Data-Transfers.pdf>; Global Data Alliance. (2026, June 23). Submission on Kenya's Draft Guidance Note on Cross-Border Data Transfers. Available: <https://globaldataalliance.org/wp-content/uploads/2026/06/06232026gdakenyadatransfer.pdf>

³³ Republic of Uganda, Data Protection and Privacy Act, 2019, s.19

³⁴ Cliffe Dekker Hofmeyr (2025). To register or not to register: The Ugandan Personal Data Protection Office's decision on the registration of data controllers. Available: <https://www.cliffedekkerhofmeyr.com/en/news/publications/2025/Sectors/Technology-Communications/technology-and-communications-alert-13-august-to-register-or-not-to-register-the-ugandan-personal-data-protection-offices-decision-on-the-registration-of-data-controllers>

³⁵ Uganda Registration Services Bureau (2025). Uganda's Data Protection Office Finds Google in Breach of Privacy, 12 August. Available: <https://ursb.go.ug/2025/08/12/ugandas-data-protection-office-finds-google-in-breach-of-privacy/>

³⁶ Republic of Uganda, Data Protection and Privacy Act, 2019, s.19; Cliffe Dekker Hofmeyr. (2025, August 13). To register or not to register: The Ugandan Personal Data Protection Office's decision on the registration of data controllers. Available: <https://www.cliffedekkerhofmeyr.com/en/news/publications/2025/Sectors/Technology-Communications/technology-and-communications-alert-13-august-to-register-or-not-to-register-the-ugandan-personal-data-protection-offices-decision-on-the-registration-of-data-controllers>

Jurisdiction	Core legal instrument	Supervisory authority	Data model for transfer mechanisms	Data localisation
RWANDA	Law No. 058/2021 (Arts. 48, 50) ⁴²	National Cyber Security Authority (NCSA), active, enforcing	Controlled Focuses on pre-authorisation or permit-based authorisation that requires regulatory sign-off before a transfer can proceed. ⁴³	Mandatory unless NCSA authorises offshore storage
DRC	Digital Code, Ordinance-Law No. 23/010 of 13 March 2023 (Title III, Art. 187) ⁴⁴	DRC's Data Protection Authority (APD) created in law but not yet constituted; Autorité de Régulation de Poste et de Télécommunication (ARPTC - the regulatory authority of the post and telecommunications) exercises interim functions ⁴⁵	Controlled DRC's Digital Code established an authorisation requirement that operates through an online compliance facility through which organisations can submit declarations and applications for authorisation, including foreign transfers. ⁴⁶	Mandatory data localisation under the Digital Code

³⁷ Federal Republic of Somalia, Data Protection Act, 2023 (Law No. 005), assented 21 March 2023, effective 23 March 2023.

³⁸ République du Burundi. Loi n°1/03 du 10 mars 2026 portant protection des données à caractère personnel. Agence de Régulation et de Contrôle des Télécommunications (ARCT). Available: <https://arct.gov.bi/2026/03/18/loi-n1-03-du-10-mars-2026-portant-protection-des-donnees-a-caractere-personnel/>

³⁹ République du Burundi. (2026). Loi n°1/03 du 10 mars 2026 portant protection des données à caractère personnel. Published by the Agence de Régulation et de Contrôle des Télécommunications. Available: <https://arct.gov.bi/2026/03/18/loi-n1-03-du-10-mars-2026-portant-protection-des-donnees-a-caractere-personnel/>. Press release regarding the launch of the digital platform for managing import and operating authorizations for electronic communications equipment. (March 2026). Available: <https://arct.gov.bi/2026/03/18/loi-n1-03-du-10-mars-2026-portant-protection-des-donnees-a-caractere-personnel/>

⁴⁰ United Republic of Tanzania, Personal Data Protection Act, 2022 (Act No. 11 of 2022); Personal Data Protection Commission. Cross-Border Data Transfer Permit. Available: <https://pdpc.go.tz/services/cross-border-data-transfer-permit/>

⁴¹ Personal Data Protection Commission, Cross-Border Data Transfer Permit, Section 31 and Section 32 of the Act (No. 11 of 2022) Available: <https://pdpc.go.tz/services/cross-border-data-transfer-permit/>

⁴² Republic of Rwanda, Law No. 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy, Arts. 43, 48 and 50. Available: <https://rwandalii.org/akn/rw/act/law/2021/58/eng@2021-10-15>

⁴³ Data Protection Office in Rwanda, Application form for external transfer authorization. Available: <https://dpo.gov.rw/services/authorization-to-transfer-outside-rwanda>

⁴⁴ Democratic Republic of the Congo, Ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique, Title III, Art. 187

⁴⁵ Democratic Republic of the Congo, Ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique, Title III, Art. 187; Law Lab Africa. Data Protection in Democratic Republic of the Congo: Law, Regulator, Enforcement. Available: <https://research.lawlab.africa/democratic-republic-of-the-congo/>

⁴⁶ Democratic Republic of the Congo, Ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique, Title III, Art. 187; Law Lab Africa. Data Protection in Democratic Republic of the Congo: Law, Regulator, Enforcement. Available: <https://research.lawlab.africa/democratic-republic-of-the-congo/>

3.2 ANTICIPATED ELEMENTS OF THE EMERGING EAC FRAMEWORK

The EAC is developing a regional framework to address regulatory fragmentation and support secure cross-border data flows. Its public communication identifies common standards, interoperable tools, coordinated oversight and cooperation among Partner States as intended features of the proposed approach. Based on research conducted for this report, it is anticipated that an emerging harmonisation framework will include common data protection safeguards and complementary lawful transfer pathways. Mutual recognition could help make transfers within the EAC more predictable, while interoperability with arrangements beyond the region will be important for maintaining access to international markets and digital services.

It is important to note that the EAC's June 2026 communication describes a workshop to review and validate the proposed Framework and identify implementation priorities ahead of finalisation. It does not confirm completed validation, formal adoption or an agreed implementation sequence. Figure 3 summarises the high-level elements we anticipate to be included in the proposed framework based on our research.

The key anticipated elements of the framework include the following:

A **Data in scope:** the Framework will likely focus primarily on personal data transferred within the EAC and to destinations outside the Community. This could encompass cross-border access and processing through cloud services and other digital platforms. Sensitive personal data is expected to attract stronger protection.

B **Default position on cross-border transfers:** For intra-EAC transfers, the anticipated approach is to facilitate data movement subject to adequate protection, potentially through recognition of comparable protections across Partner States. For extra-EAC transfers, the framework is expected to emphasise continuity of protection through safeguards in receiving jurisdictions or those adopted by the organisations involved.

C **Transfer pathways:** The emerging framework will likely seek to accommodate several lawful transfer pathways, including contractual safeguards and recognition of comparable protection. Their design should provide businesses with practical options while maintaining effective safeguards.

D **Safeguards and accountability:** The framework is expected to combine common data protection safeguards with responsibilities for organisations transferring and receiving personal data. This may include transparency, security, protection of individuals' rights and demonstration of compliance. Safeguards would reflect transfer risks, while cooperation among authorities could support responses to cross-border complaints and security incidents.

E **Localisation and national discretion:** The Framework will likely look to limit localisation to legitimate and clearly defined public interest, including national security or essential public policy, provided the measure is necessary, proportionate and does not undue barriers to regional data flows. Given the EAC's focus on national authority, this is likely to remain material. Partner States will retain flexibility over consistent national procedures relating to language, format, accessibility, timing, institutional processing and approval procedures, as well as relevant sector-specific requirements permitted under the regional framework.

F **Institutional architecture:** National competent authorities are likely to remain the principal supervisory and enforcement bodies, with the framework encouraging cooperation among those authorities, supported by regional coordination. Cooperation would be focused on information exchange and supervisory cooperation and support for consistent interpretation of transfer requirements.

G **Comparability to other global models:** The above elements signal the combining of features of the GDPR's approach to legal safeguards and recognised transfer pathways with the Global CBPR system's emphasis on organisational accountability and interoperability across different national privacy laws. This would mean common requirements for protecting transferred data, supported by contractual or certification mechanisms, while allowing Partner States to maintain their own legal systems and supervisory authorities.

Figure 3: Anticipated Key Elements of the Emerging EAC Cross-Border Data Flows Framework



3.3 HOW FRAGMENTATION COSTS EAST AFRICAN BUSINESSES (MICRO IMPACT)

The effective implementation of the proposed EAC Framework would have significant benefits for businesses operating within the EAC who face multiple operational frictions as a result of the prevailing regulatory fragmentation across countries. When EAC Partner States enact mismatched, country-specific data laws, businesses then need to navigate a complex labyrinth of divergent compliance regimes. At the microeconomic level, this digital fragmentation penalises firms through several distinct cost channels:

01

Because EAC Partner States each set their own data rules, companies cannot use one legal framework across the region, resulting in higher legal and compliance costs.

Instead, companies hire local lawyers, register separately, and rewrite contracts in every market. Consulted organisations listed having to repeat compliance paperwork market by market, with one representative stating they sometimes repeat a single administrative task roughly 11 times across different jurisdictions. To counteract this, some organisations apply group-wide privacy standards informed by internationally recognised frameworks, including the NPTR, to support consistent compliance across jurisdictions.

The Cisco 2026 Data and Privacy Benchmark Study found that 85% of their 5,200 respondents (IT, tech & security professionals across 12 markets) reported data localisation adding cost, complexity, and risk to cross-border service delivery.

02

Standard data localisation or mirroring rules compel firms to store or process certain categories of data domestically, preventing firms from using one shared cloud system, and requiring them to build separate data centres and security systems in each market instead.

The Cisco 2026 Data and Privacy Benchmark Study, for instance, found that 85% of their 5,200 respondents (IT, tech & security professionals across 12 markets) reported data localisation adding cost, complexity, and risk to cross-border service delivery.⁴⁷ Even profitable multinational corporations may struggle to economically justify building separate data centres in every small market they serve, sometimes leading them to either exit or entirely avoid smaller economies.⁴⁸



Case study from published literature: The cost of localisation

JUMO is a fintech platform that uses centralised cloud infrastructure to run machine learning engines that predict consumer creditworthiness based on mobile network usage data. JUMO operates in three East African markets: Uganda, Kenya and Tanzania. In 2018, the regulatory burdens imposed by Rwanda's data protection framework de facto required local storage. Because JUMO's low-overhead model depends entirely on cloud scalability, setting up a dedicated, physical data service just for Rwanda's small market was mathematically uneconomical, *forcing the firm to shut down its partnership with a local telecommunications provider and exit the market.*⁴⁹

03

Moving data between countries requires extra contracts, consent processes, and regulatory approvals, which slow transactions and raise costs.

For instance, a digital payments company consulted for this study that had faced repeated delays from an East African central bank when adding new mobile money partners had to build an entirely new technical system routing payments through a licenced commercial bank in order to work around this and keep transactions moving. An empirical study covering 31 African countries estimates that local storage requirements and laws requiring partner countries to have similar privacy laws are associated with a 12% to 20% reduction in bilateral digital services imports.⁵⁰ In contrast, African nations that implement a comprehensive data protection framework enjoy a 14% increase in digital services exports to developed markets like the Organisation for Economic Co-operation and Development (OECD), as it allows them to satisfy the adequacy conditions demanded by high-income trading partners.⁵¹

⁴⁷ Cisco (2026). Cisco 2026 Data and Privacy Benchmark Study. Available: <https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html> Leviathan Security Group (2024).

⁴⁸ Lee-Makiyama, H. and Lacey, S. (2021). Cross-Border Data Flows: The impact of data localisation on IoT. Available: <https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2021/01/Cross-border-data-flows-the-impact-of-data-localisation-on-IoT-Full-Report.pdf>

⁴⁹ Medine, D. (2023). Data Localization: A "Tax" on the Poor. Centre for Global Development. Available: <https://www.cgdev.org/sites/default/files/data-localization-tax-poor.pdf>

⁵⁰ Van der Marel, E. (2024). Data Regulation and Digital Services Trade in Africa. Journal of African Trade, 11(1). Available: <https://doi.org/10.59624/2214-8523.1140>

⁵¹ Ibid.

04

Because rules differ by country, digital firms must rebuild their products, back-end systems, and privacy notices market by market instead of launching one version regionally, resulting in slower product launches and regional expansion.

The EAC itself has flagged this as a major non-tariff barrier to its Common Market, particularly hurting startups and small businesses. Organisations consulted for this study cited clear examples of product launch delays, with some representatives estimating that regulatory back-and-forth and approvals around regional data transfers cause delays of three to six months to regional product launches.

Consulted businesses report that regulatory back-and-forth and approvals around regional data transfers add a stalling delay of three to six months to regional product launches

05

Pooling customer data lets companies centralise things like fraud detection and analytics, lowering the cost per customer. Fragmented rules block this, preventing firms from using a single, efficient regional data architecture.

This burden falls hardest on smaller companies without spare resources to duplicate the work. For example, Rwanda requires banks to maintain their primary data within Rwanda, while Uganda's National Payment Systems Act requires electronic-money issuers to maintain their primary data centre in Uganda. For a financial company operating across those markets, requirements like these can prevent it from simply operating one regional data architecture. Instead, it may need country-specific storage, compliance procedures and potentially duplicated infrastructure, which could delay the rapid combination of cross-border transaction and identity data needed by fraud systems to identify patterns.

06

Without one shared data authority across the EAC, national regulators interpret similar rules differently, and companies must prepare for sudden investigations, new compliance demands, or heavy fines.

The MTN Rwanda case study below highlights the extent of fines associated with not complying with changing, and often costly, local data protection laws.



Illustrative case study from published literature: Heavy fines for non-compliance with changing laws. MTN Rwanda, Rwanda's largest telecommunications company, was fined roughly US\$8.2 million (FRw 7.03 billion) in 2017 by the Rwandan telecommunications regulator, Rwanda Utilities Regulatory Authority (RURA), for breaching Rwanda's 2016 telecommunications security regulations, which required that subscriber data - voice, SMS, call records, and billing information - stay within Rwanda's borders. The penalty was based on ICT law provisions allowing daily fines of US\$499-US\$14,960 for non-compliance with a regulatory directive, on top of powers to impose extra license conditions, suspend a license, or revoke it outright. MTN and others at the time argued that moving its data centre from Uganda to Rwanda would be complex, costly, and disruptive to the efficient way the MTN Group managed its resources regionally.⁵²

07

Finally, the biggest cost of fragmentation may be the business that never happens at all - deals, market entries, and services that companies simply avoid because the legal and technical friction is too high.

For example, organisations consulted for this study noted that without regulatory certainty, it is sometimes "next to impossible" to justify the business case for building major infrastructure in East Africa, and that in some cases, fragmented rules have limited what services companies can offer there, thereby cutting local businesses and households from more advanced service offerings.

⁵² Collaboration on International ICT Policy for East and Southern Africa (CIPESA) (2022). Which Way for Data Localisation in Africa? Available: https://cipesa.org/wp-content/files/briefs/Which_Way_for_Data_Localisation_in_Africa_Brief.pdf



04. REMOVING BARRIERS: CONSIDERATIONS FOR THE PROPOSED EAC FRAMEWORK

In light of the costs associated with fragmented and restrictive cross-border data flow regulation, this section considers how the design of regional cross-border data governance could reduce these frictions while preserving credible safeguards, and what this implies for EAC policymakers as the emerging harmonisation framework develops .

It brings together two strands of evidence. First, it draws on the macroeconomic literature to identify the regulatory approaches associated with stronger economic outcomes, particularly the balance between openness, safeguards and administrative burden. Second, it relates these findings to the practical issues raised through KIIs with seven digitally enabled businesses operating in the EAC and AmCham member submissions. The aim is to assess the economic significance of these stakeholder concerns and identify the design and implementation choices that warrant particular attention as the framework develops.

4.1 TRANSFER RULES, NATIONAL PROCEDURES AND THE COST OF TRADING REGIONALLY

Transfer rules and the national procedures that accompany them serve a legitimate public-policy objective: they ensure that personal data leaving a jurisdiction remains subject to adequate safeguards and that authorities can protect data subjects. The implementation challenge is that, across the EAC, these rules currently take the form of divergent national requirements for authorisation, filing, due diligence and local storage, applied in parallel rather than as a single predictable regional regime.

Restrictive transfer requirements can raise trade costs, while credible domestic data protection can also support exports. Evidence from 31 African countries finds that local storage requirements and rules requiring partner countries to have similar privacy protections are associated with lower digital services imports⁵³. At the same time, privacy requirements imposed by trading partners are associated with around 14% higher digital services exports from African countries with comprehensive data protection frameworks, most likely because those frameworks help firms meet the standards required in destination markets.⁵⁴ The distinction is important for the EAC: strong privacy protection and restrictive transfer procedures are not the same policy choice. The economic objective is therefore to maintain credible protection while reducing transfer requirements that unnecessarily increase the cost of supplying or purchasing digital services across borders.

The design of harmonisation matters more than harmonisation alone. A 2025 study of African data-transfer regimes found no significant trade effect from countries simply sharing the same regulatory model; rather, economic outcomes depend heavily on how these models are implemented. While open transfer models have shown positive associations with intra-African digital services trade, conditional models, which rely on ex-ante mechanisms such as adequacy, standard contractual clauses and binding corporate rules, can inadvertently restrict trade if they are burdened with heavy administrative friction or rigid pre-approval requirements. The authors estimated that implementing smoother, less restrictive, open dataflow commitments across Africa could increase intra-regional digital services trade by up to 10.3%, or approximately US\$125 million relative to the 2021 trade base. The takeaway from this evidence is that regional convergence creates economic value only if common rules actually reduce duplication, approvals and uncertainty rather than harmonising around a high-friction process.⁵⁵

⁵³ Van der Marel, E. (2024). Data regulation and digital services trade in Africa. *Journal of African Trade*, 11(1), 65–79. Available: <https://doi.org/10.59624/2214-8523.1140>

⁵⁴ *Ibid.*

⁵⁵ Ferracane, M. F., González Ugarte, S., & van der Marel, E. (2025). The Brussels effect in Africa: Is it beneficial for intra-regional trade in digital services? *Journal of International Economic Law*, 28(1), 1–22. <https://doi.org/10.1093/jiel/jgae059>

Recognising both the legitimacy of these policy objectives and the costs of the current approach, businesses consulted for this study recommended that the Framework could address this through the following three avenues:



1) STREAMLINING NATIONAL FILING, APPROVAL AND DUE DILIGENCE PROCEDURES.

Consulted businesses generally agreed that the Framework should accommodate multiple transfer mechanisms, including SCCs and BCRs. The greater concern was the national licensing, filing, approval and due diligence procedures that may accompany their use. The literature does not isolate these administrative processes as the source of weaker trade outcomes, but it does find that conditional transfer regimes relying on ex ante mechanisms are associated with weaker intra-African digital services trade than more open models. The stakeholder evidence helps identify how some of that friction may arise in practice. As Partner States are expected to retain discretion over national procedures, the regional instrument can seek to ensure that these are as simple and low-burden as possible, so that convergence on recognised transfer mechanisms is not undermined by divergent national processes.



2) APPLYING RISK-BASED, PROPORTIONATE SUPERVISION AND LIMITING DELAYS IN TRANSFER PROCEDURES.

The framework should provide for safeguards to be calibrated to the sensitivity, volume, purpose and destination risk of a transfer. That principle can also shape how national procedures are implemented. Routine, lower-risk transfers should not face the same documentation and approval requirements as higher-risk transfers, and reporting obligations should be proportionate to the seriousness of the underlying risk. Where prior review or approval is required, clear and predictable timelines would help prevent the process itself from becoming a barrier to regional operations. This matters in practice: consulted firms reported that regulatory back-and-forth over regional data transfers can delay product launches by three to six months. A risk-based approach would allow regulators to focus supervisory resources on higher-risk transfers while reducing unnecessary delays for routine cross-border activity.



3) ENABLING MUTUAL RECOGNITION OF COMPLIANCE INFORMATION ACROSS AUTHORITIES.

Consulted businesses also highlighted the cost of submitting substantively similar information to multiple national regulators. The regional framework could reduce this duplication by allowing information already provided to a recognised authority to satisfy equivalent requirements elsewhere, where it meets the relevant standard. This would require a lawful basis for cooperation and clear arrangements between participating authorities for assessing and accepting equivalent compliance information. In practice, such an approach could reduce repeated documentation without weakening the underlying compliance requirement.

Interoperability beyond the EAC should be a design principle for these transfer pathways.

Their development and implementation should support the objectives of the AfCFTA Digital Trade Protocol, the AU Data Policy Framework and the Digital Transformation Strategy for Africa, while promoting interoperability with international transfer mechanisms. The aim should be to facilitate trusted transfers both within and beyond the EAC, subject to applicable legal requirements and adequate protection, so that regional harmonisation supports access to global digital services and international markets without creating a regional data silo.

4.2 COMPLIANCE COSTS, INSTITUTIONAL CAPACITY AND SMALLER FIRMS

Comprehensive data protection is critical for fulfilling individuals entitlement to consistent protection, regardless of the size or location of the firm processing their data.

The implementation challenge is that the cost of demonstrating compliance is largely fixed, while legal, compliance and institutional resources are unevenly distributed across firms and Partner States.

The economic consequences are distributional: compliance-intensive regimes can weigh more heavily on lower-income economies and smaller firms. The literature finds that comprehensive data protection laws are negatively associated with intra-regional digital services trade, with the effect concentrated in lower-income economies; this is linked to the fixed cost of compliance in smaller and less productive markets.⁵⁶ This highlights a distributional risk for the EAC: where compliance requirements are complex or administratively intensive, their costs are likely to be harder for SMEs and firms in lower-capacity Partner States to absorb. Proportionate obligations, simplified mechanisms for lower-risk transfers and targeted technical assistance are therefore part of the economic design of harmonisation, not only implementation considerations.⁵⁷

⁵⁶ Ferracane, M. F., González Ugarte, S., & van der Marel, E. (2025). The Brussels effect in Africa: Is it beneficial for intra-regional trade in digital services? *Journal of International Economic Law*, 28(1), 1–22. <https://doi.org/10.1093/jiel/jgae059>

⁵⁷ *Ibid.*

Consulted businesses for this study recommended addressing this through the following two avenues



1) MAKING COMPLIANCE REQUIREMENTS PROPORTIONATE FOR SMALLER FIRMS.

The cost of complying with the proposed framework is likely to fall unevenly across firms. Most large organisations consulted already apply group-wide data protection standards, often aligned with the GDPR, so harmonisation may change their compliance processes more than the substantive standard they follow. Smaller firms and start-ups have fewer legal and compliance resources and may therefore face a proportionately greater burden. The framework could account for this by simplifying documentation and procedures for lower-risk transfers and ensuring that SMEs participate in any pilot initiatives, so that harmonisation lowers barriers to regional participation rather than raising them.



2) PRIORITISING CAPACITY-BUILDING IN PARTNER STATES WITH WEAKER IMPLEMENTATION CAPACITY.

Differences in regulatory capacity were one of the most frequently cited implementation risks in consultations. Businesses emphasised that uneven implementation may reflect limited technical and institutional capacity rather than unwillingness to comply with regional rules. Recognition of comparable protection would depend partly on the capacity of participating authorities to supervise and enforce relevant requirements. Future implementation planning should therefore assess capacity needs, identify sustainable financing and support cooperation and learning among regulators. Without this support, the framework risks formalising existing differences in institutional capacity rather than reducing them.

4.3 BALANCING OPENNESS WITH TRUST

Data localisation mandates are often pursued in response to **legitimate concerns about privacy, security, human rights and economic competitiveness**. The proposed framework needs to take these objectives seriously rather than treating localisation solely as a barrier to trade; the question for the EAC is how to respect them while avoiding unnecessary economic cost.

The importance of this balance is reflected in the economic evidence. Economic effects of cross-border data regulation depend not only on how restrictive a regime is, but also on whether it provides credible safeguards that support trust. OECD-WTO modelling illustrates this non-linear relationship. A scenario in which all economies fully restrict data flows is projected to reduce global GDP by 4.5% and exports by 8.5%. Yet eliminating data-flow regulation altogether also produces a negative result, with global GDP falling by nearly 1% as the modelled loss of trust outweighs lower trade costs.



By contrast, convergence towards regimes combining relatively open flows with open or pre-authorised safeguards is projected to increase global exports by 3.6% and global GDP by 1.77%. The modelled GDP gains are largest for low- and lower-middle-income economies, at approximately 5% and 4.3% respectively. These global scenarios reinforce the central policy trade-off: safeguards can have economic value through trust, while excessive restrictions impose trade costs.⁵⁸

It is therefore recommended that the proposed framework define localisation clearly and establish a test for justified exceptions. The key question for the EAC is therefore when localisation is justified and how tightly any exceptions should be defined.

⁵⁸ OECD & World Trade Organization. (2025). Economic implications of data regulation: Balancing openness and trust. OECD Publishing. <https://doi.org/10.1787/aa285504-en>

The risk is that a principle expressed only as a general limitation on localisation will not be effective.

Consulted firms raised three specific questions that the emerging Framework should answer:

- **What a localisation requirement is:** the definition should capture de facto localisation, where a permit, authorisation or evidentiary burden makes local storage the path of least resistance, and not only explicit statutory mandates;
- **What makes a requirement justified:** the instrument should set out a necessity and proportionality test, a requirement that measures be published and specific to defined data categories, and a prohibition on open-ended designations. Consulted businesses were clear that the absence of a data classification framework is itself the problem, and that a government statement of what constitutes high-risk or national-security data would give firms the certainty they need to invest, whereas a blanket mandate does the opposite; and
- **Who adjudicates:** firms asked directly who checks compliance with the anti-localisation principle and how it is enforced, and noted that national security exceptions will need to be drafted tightly enough that they are not used to reopen the general rule.

Taken together, the evidence suggests that harmonisation will only deliver economic benefits if it reduces the practical frictions associated with moving data across borders.

The literature points towards better trade outcomes under relatively open regimes, while also showing that credible data protection can support trust and access to external markets. For the EAC, the priority is therefore to avoid harmonising around restrictive or administratively burdensome processes, and instead ensure that the framework's final design enables data to move more easily while maintaining appropriate safeguards.



05. WAY FORWARD

Maintaining momentum in the development of the emerging framework will be important. The priority should be to identify practical opportunities to reduce fragmentation and support trusted cross-border data flows, while allowing sufficient scope for consultation, policy development and any necessary legal reform.

There is a risk that implementation loses momentum while the legal instrument is developed. Policy development and legal reform can take time. Carefully designed testing could help assess the practicality and economic implications of possible approaches as the framework develops, subject to applicable law and agreement among participating authorities.

An interim cooperation mechanism could provide an opportunity to test practical approaches to cross-border data governance as the regional framework develops. Subject to national law and the agreement of participating authorities, such an arrangement could bring regulators and businesses together to assess how more consistent compliance and supervisory practices might work across jurisdictions.

This could help address the implementation challenges identified above. Potential areas for testing include greater alignment in the information businesses provide to demonstrate compliance, scrutiny proportionate to transfer risks and reuse of equivalent compliance information across authorities where legally feasible. These approaches could help address duplicative national procedures and disproportionate compliance burdens while preserving national supervisory responsibilities.

The design and testing of any interim mechanism should include structured business participation and wider stakeholder consultation. Participants should include MSMEs, firms operating across multiple EAC markets, data protection authorities and sector regulators, reflecting differences in institutional capacity, sector risk and business models. Testing should assess whether the arrangement reduces repeated filing and due diligence, provides predictable compliance expectations and maintains effective protection without adding procedural layers. Findings could inform the development and implementation of the regional framework.

RESEARCH GAPS AND AREAS FOR FUTURE WORK

This report is a rapid assessment based on desktop research and a limited number of private-sector interviews, rather than a comprehensive economic impact study. The analysis draws on existing literature, trade and economic data, regional and national policy documents, and interviews with seven businesses operating in the EAC. The interview sample was necessarily limited and did not include SMEs. As a result, the findings may not fully capture the particular costs faced by smaller firms, which are likely to have fewer legal, compliance and technical resources with which to manage divergent national requirements. The study also did not undertake scenario modelling using trade or other economic data to estimate the potential effects of alternative regulatory approaches. These limitations should be taken into account when interpreting the firm-level and macroeconomic findings presented in this report.

Once the design of the proposed EAC Cross-Border Data Flows Framework is clearer, future research should include a full regulatory impact assessment of its key provisions. This should identify the principal regulatory options available to the EAC, assess the likely costs and benefits of each option, and consider how these effects may differ across sectors, firm sizes and Partner States. Such an assessment could examine, for example, alternative approaches to mutual recognition, transfer mechanisms, localisation, regulatory approvals and compliance requirements. This would provide policymakers with a stronger evidence base for determining how the Framework can achieve its objectives of protecting data and building trust while minimising unnecessary costs to regional trade, investment and business activity.

