Global Scientific JOURNALS

GSJ: Volume 13, Issue 6, June 2025, Online: ISSN 2320-9186
www.globalscientificjournal.com

Harmonizing Data Protection in East Africa: A Comparative Analysis and Policy Recommendations

Eng. Murenzi Daniel [1]

[1] Principal Information Technology Officer

East African Community HQ, Arusha

Received Date: Accepted Date: Published Date:

ABSTRACT

This paper provides a comprehensive comparative analysis of data protection frameworks within the East African Community (EAC). It examines the national data protection laws, enforcement mechanisms, and cross-border data flow mechanisms in each of the EAC Partner States, including Kenya, Uganda, Rwanda, Tanzania, Burundi, Somalia, the Democratic Republic of Congo (DRC), and South Sudan. The study identifies key gaps and challenges in the current legal landscape and proposes actionable recommendations for harmonizing data protection laws, strengthening regulatory institutions, and enhancing regional cooperation. The analysis also draws from international best practices, including the European Union's General Data Protection Regulation (GDPR) and the African Union's Malabo Convention, to provide insights into potential solutions for improving data governance in East Africa.

Key words: Data Protection, National Data Protection Laws, Enforcement Mechanisms, Cross-Border Data Flow, General Data Protection Regulation (GDPR) and Malabo Convention.

1. INTRODUCTION

Data protection and governance have become critical components of national and regional digital transformations, particularly in the context of East Africa. As the global digital landscape expands, ensuring the privacy, security and integrity of personal data has emerged as a pivotal issue for governments, businesses and individuals alike. In this rapidly evolving digital age, the East African Community (EAC) faces both unique challenges and opportunities in implementing robust data protection frameworks that are aligned with international standards while also catering to the regional context.

The digital economy has a profound impact on various sectors, ranging from health and education to trade and governance. However, with the increase in data generation and processing across borders, there is an inherent need for harmonized legal frameworks that can effectively protect the data of citizens while fostering economic growth and technological innovation. The challenges of cross-border data flows, privacy concerns, cybersecurity risks, and the lack of standardization in data protection practices across EAC partner states have underscored the importance of a cohesive and adaptive approach to data governance.

This paper explores the data protection and governance landscapes within the EAC, offering a detailed comparative analysis of the data protection frameworks in each member state. Additionally, the paper examines regional and international frameworks such as the African Union's Malabo Convention, the Common Market Protocol, and best practices from other regional bodies like the European Union (EU) and ASEAN. Through this comparative study, we aim to identify gaps, propose solutions, and provide recommendations for fostering regional cooperation and improving the protection of personal data in East Africa.

2. OVERVIEW OF THE DATA PROTECTION LAWS IN EAST AFRICA COMMUNITY.

In order to understand the status of data protection across the EAC, it is essential to examine the legal instruments governing data protection in the individual Partner states. These instruments are critical in ensuring compliance with regional and international standards, as well as in addressing challenges related to data privacy, security, and cross-border data flows.

Kenya

Kenya has made significant strides in data protection with the enactment of the **Data Protection Act, 2019**. This law provides a comprehensive framework for the protection of personal data, aligning with international best practices, particularly the EU's General Data Protection Regulation (GDPR). Key components of Kenya's data protection framework include regulations for data controllers, data processors, and the establishment of the Office of the Data Protection Commissioner (ODPC) to oversee compliance.

The regulations further elaborate on data registration, complaints handling, and specific guidance for sectors such as education, digital credit, and electoral processes. However, challenges remain in the enforcement of these regulations, as the operationalization of the ODPC is still ongoing.

Uganda

Uganda's **Data Protection and Privacy Act**, enacted in 2019, marks a significant milestone in the country's data protection journey. The law establishes a framework for the protection of personal data across both public and private sectors. Similar to Kenya, Uganda's law draws heavily from international frameworks like the GDPR, with provisions for data processing, cross-border data transfer, and the establishment of the **National Information Technology Authority - Uganda (NITA-U)** to enforce the regulations.

However, Uganda's framework faces challenges in terms of implementation and compliance, especially in sectors such as telecommunications and banking, where personal data is often processed without sufficient safeguards.

Rwanda

Rwanda's **Personal Data Protection and Privacy Law (2021)**, although relatively new, demonstrates the country's commitment to a strong data protection regime. Rwanda has established a robust legal framework that integrates with the country's broader digital transformation goals. The establishment of the **National Cyber Security Authority (NCSA)** and the Data Protection Department within it marks a forward-thinking approach to data protection.

Rwanda's data protection framework closely follows international standards, though there are concerns about the capacity of the regulatory bodies to enforce the law effectively in the absence of a fully operationalized data protection authority. Rwanda has acceded to the Budapest Convention on Cybercrime (ETS 185) and fully a state party to the Budapest Convention and bound by its provisions.

Tanzania

Tanzania's **Personal Data Protection Act (2022)**, which was preceded by several sectoral laws covering telecommunications and banking, finally brings personal data protection into a legal framework. The Act is accompanied by regulations that set out specific conditions for the collection, processing, and storage of personal data.

Despite the legislative advancements, Tanzania faces challenges related to data localization and cross-border data transfers, which could hinder the free flow of information essential for regional and global economic integration.

Burundi

Burundi does not yet have a comprehensive data protection law. While there are sectoral laws related to health, banking, and telecommunications that address aspects of personal data protection, there is no standalone data protection law in the country. This legal gap poses significant challenges to the country's ability to regulate and protect the personal data of its citizens, particularly in the digital age.

Somalia

Somalia passed its **Data Protection Law (2023)**, which represents an important step towards protecting the privacy and data rights of its citizens. However, operational guidelines and the necessary institutional framework to enforce this law are still in development, which presents challenges in terms of its effective implementation.

The Democratic Republic of the Congo (DRC)

In the DRC, the legal framework for data protection is still evolving. The **Digital Code (2023)** contains provisions related to the protection of personal data, but the country lacks a standalone law dedicated to data privacy. Furthermore, DRC's participation in the **Malabo Convention** could drive future developments in personal data protection, although much remains to be done in terms of enforcement and regulatory capacity.

South Sudan

South Sudan has yet to enact a formal data protection law. However, there have been discussions about the development of a **Data Protection Bill (2020)**, which would establish a legal foundation for data protection in the country. Currently, there is no established data protection authority, and the implementation of such a law would face significant capacity challenges.

Key Legal Instruments

1. **The Malabo Convention**: This Pan-African legal framework focuses on personal data protection, cybersecurity, and the regulation of electronic transactions and cybercrimes. While this Convention is widely adopted across the African Union (AU), only Rwanda and the Democratic Republic of the Congo (DRC) have ratified it within the EAC.
2. **The EAC Cyber-Laws Framework (2008)**: Initially intended to harmonize data protection laws, this framework has not yet resulted in unified legislation but has been instrumental in influencing national reforms in countries like Kenya, Uganda, and Rwanda.
3. **The Common Market Protocol (CMP)**: This EAC treaty provides for the free movement of goods, services, labor, and capital within the region. Although the Protocol does not directly address data protection, it mandates the alignment of national laws to facilitate regional integration, including policies on data protection.

Key Elements of the Policy Framework

Vision & Mission

The vision is to create a data-driven, equitable socio-economic community with improved livelihoods and protected digital rights. The mission centers around developing a secure data management ecosystem to support data-driven services and a sustainable digital economy in the region.

Strategic Objectives

- Harmonize data governance policies across EAC states.
- Enhance cross-border data flows to boost digital trade.
- Promote secure and privacy-respecting data management.
- Support the development of digital infrastructure and human capital to sustain the data-driven economy.

Key Findings from the Comparative Study

i. Diverse legal landscape

Across the EAC, data protection laws exhibit varying degrees of maturity. While countries like Kenya and Uganda have well-established frameworks, others like South Sudan and Burundi are still in early stages of developing these legal instruments. This fragmentation hampers regional cooperation and impedes the effective handling of cross-border data flows.

ii. Adoption of International Standards

The Malabo Convention on cybersecurity and data protection, ratified by only Rwanda and the DRC among EAC partner states, provides a continental framework for data governance. Its principles align with global standards, but full regional adoption is critical for fostering a unified approach to data protection.

iii. Operationalization of Data Protection Laws

Despite the establishment of data protection laws in some partner states, these laws are not yet fully operational. Challenges include limited capacity in Data Protection Authorities (DPAs), inconsistent enforcement, and a lack of standardized procedures for handling data breaches. The operationalization of these laws is vital for building public trust and encouraging cross-border trade.

iv. Cross-Border Data Flow Mechanisms

Cross-border data flows are essential for the digital economy. However, inconsistent legal frameworks and the lack of uniform standards for assessing data protection adequacy present obstacles to seamless data exchange.

Comparative Lessons: The EU and ASEAN Models

- The European Union's General Data Protection Regulation (GDPR) sets a high standard for personal data protection, focusing on transparency, consent, and individual rights. Its expansive territorial scope and substantial penalties for non-compliance serve as a model for the EAC. However, it may be challenging to replicate such stringent standards immediately across all EAC Partner States, given the varying levels of legal and institutional maturity.
- The ASEAN model, characterized by non-binding guidelines on data management and cross-border flows, provides a more flexible approach. It emphasizes the mutual intention of partner states to cooperate on data protection without imposing legally binding obligations. This approach may be more feasible for the EAC, allowing for a smoother, less complex adoption process while still promoting alignment and cooperation.

3. EAC DATA GOVERNANCE POLICY FRAMEWORK:

Strategic Pillars

The EAC Data Governance Policy Framework, aligned with international best practices, aims to enhance regional integration through the following strategic pillars:

1. ***Data Protection and Privacy****:*
   The framework emphasizes robust data protection principles, ensuring the privacy of individuals while fostering trust in the region's data handling practices. This is particularly important for safeguarding digital rights as the region pursues its Vision 2050 of a unified digital economy.
2. ***Cross-Border Data Flows****:*
   Promoting unrestricted yet secure data flows across EAC Partner States is pivotal. The framework advocates for harmonized data protection laws that respect national sovereignty while facilitating regional digital trade. The establishment of a *Common Data Categorization and Sharing Framework* is recommended to standardize data types and their corresponding privacy levels, further boosting cross-border data exchanges.
3. ***Digital Skills and Capacity Building****:*
   A critical component of the policy is the development of digital literacy and the enhancement of technical capacity across sectors. This includes empowering stakeholders to effectively manage data, from government agencies to private businesses.
4. ***Regulatory Frameworks and Compliance****:*
   To ensure compliance with data protection laws, the EAC proposes strengthening penalties for violations, aligning national data protection laws with international standards, and developing common guidelines for assessing data protection adequacy

Legal Gap Analysis

A key aspect of this study is identifying the legal gaps that exist in the data protection frameworks of the EAC partner states. These gaps can hinder the effective protection of personal data and the seamless flow of information across borders.

- ***Definition and Classification of Personal Data***

While most EAC countries have adopted definitions of personal data that align with international standards, there are variations in how sensitive data is classified. Some countries, such as Tanzania, have a broader definition of sensitive data, which includes financial information, trade union membership, and social security numbers. This broader

classification provides a higher level of protection and could serve as a model for other EAC partner states.

- ***Cross-border Data Transfers***

Most EAC countries allow for the transfer of personal data outside their borders only when certain conditions are met, such as ensuring that the recipient country offers an adequate level of protection for the data. However, the lack of a consistent approach to cross-border data flows across the region remains a significant challenge. Some countries, like Uganda and Tanzania, have stricter conditions, requiring that transfers be based on contractual agreements or government-approved adequacy findings. This lack of uniformity in data transfer protocols can create barriers to regional data exchange and economic integration.

- ***Enforcement Mechanisms***

Enforcement of data protection laws remains a challenge in many EAC countries. While some countries, such as Kenya, Rwanda and Uganda, have established regulatory bodies like the **Office of the Data Protection Commissioner (ODPC), National Cyber Security Authority (NCSA)** and **NITA-U**, others, such as Burundi and South Sudan, lack functional data protection authorities. Strengthening the capacity of these institutions is crucial for ensuring compliance, addressing data breaches, and promoting a culture of data protection within both the public and private sectors.

- ***Recommendations***

To address the legal gaps identified in the analysis, the following recommendations are proposed:

1. *Harmonization of Data Protection Laws*: EAC partner states should work towards aligning their data protection laws with international standards, particularly those outlined in the Malabo Convention and the GDPR. While full legal harmonization may not be immediately achievable, a convergence of basic principles and standards would facilitate greater coherence in the regional legal framework.
2. *Strengthening Regulatory Bodies*: To improve enforcement, EAC partner states should invest in the capacity building of their Data Protection Authorities (DPAs). This includes providing sufficient resources, training, and operational frameworks to ensure that these bodies can effectively monitor compliance and address data breaches.
3. *Establishing Guidelines for Cross-border Data Transfers*: EAC partner states should collaborate to develop a common set of guidelines for cross-border data transfers, ensuring that personal data is protected while facilitating free data flows for regional economic integration.

4. THE DATA GOVERNANCE STRUCTURE

The policy framework is structured around four critical pillars:

- **Data Management**: Including collection, classification, and governance practices.
- **Data Infrastructure**: Enabling the proper storage and processing of data.
- **Digital Skills & Human Capacity**: Empowering the workforce with necessary digital competencies.
- **Policy, Legal & Regulatory Frameworks**: Establishing rules to ensure compliance, privacy, and security in data handling.

5. IMPLEMENTATION STRATEGY

(I) Legal Framework and Context

Objective:

To create a robust and harmonized legal framework across the East African Community (EAC) Partner States in alignment with the EAC Treaty.

Action Steps:

- *Awareness and Understanding*: Ensure that all legal professionals, government officials, and policymakers in Partner States understand the EAC Treaty and its implications for regional integration and law supremacy.
- *Institutional Support*: Strengthen regional institutions responsible for implementing the EAC Treaty, such as the East African Court of Justice (EACJ), the EAC Secretariat, East Africa legislative Assembly(EALA) and national ministries or departments responsible for integration.

(II) Principle of Supremacy of Regional Law

Objective:

Establish the legal supremacy of regional laws over national laws in instances of conflict or inconsistency, ensuring uniformity across all Partner States.

Action Steps:

- *Amendment of National Laws*: Partner States must review and amend their national laws to align with EAC regional laws, treaties, regulations, and decisions.
- *Training and Capacity Building:* Organize workshops and training programs for legal and judicial bodies to ensure proper interpretation and application of regional laws.
- *Drafting of Protocols and Guidelines*: Develop clear protocols and guidelines outlining the hierarchy of laws, addressing when and how regional laws take precedence over national laws.

(III) Legal Basis for Supremacy

Objective:

Solidify the legal foundation for the supremacy of regional laws through the Treaty obligations of Partner States.

Action Steps:

- *Implementation of Article 7*: Promote awareness of the importance of cooperation and harmonization of laws, as specified in Article 7 of the EAC Treaty.
- *Legislative Reviews*: Partner States should carry out periodic reviews of their national laws and harmonize them in compliance with Article 76(2) of the Treaty.
- *Judicial Enforcement*: Encourage the EACJ to actively interpret and apply regional laws, providing definitive rulings when conflicts arise between regional and national laws.

(IV) Reasons for Supremacy

Objective:
Justify and promote the need for the supremacy of regional laws by highlighting the benefits and goals of EAC integration.

Action Steps:

- *Promote Economic Integration*: Advocate for uniform standards and regulations, especially in areas such as trade, customs, and transportation, to facilitate smoother cross-border operations and greater economic cooperation.
- *Political and Social Integration*: Develop common policies across Partner States that foster political and social cohesion within the EAC region, ensuring equal treatment for citizens across borders.
- *Consistency in Law Enforcement*: Establish uniform enforcement mechanisms to guarantee that regional standards and policies are consistently applied in all Partner States.

(V) Implementation and Enforcement

Objective:
Ensure effective enforcement of regional laws and ensure compliance with the supremacy of regional law over national legislation.

Action Steps:

- *Amendment of National Legislation*: Partner States must establish procedures for amending national laws and policies that conflict with regional laws, ensuring consistency with EAC legislation.
- *Establishment of Regional Enforcement Mechanisms*: Create a framework for monitoring and enforcing regional laws at both the national and regional levels, involving the EACJ and national courts.
- *Strengthening the EACJ*: Empower the East African Court of Justice to handle disputes regarding the supremacy of regional law and act as the final authority in conflicts between national and regional legislation.
- *Dispute Resolution Mechanisms*: Establish clear procedures for addressing disputes and legal conflicts between Partner States, ensuring that regional laws are upheld.

(VI) Monitoring and Evaluation

Objective:
Create an effective system for monitoring the implementation of the legal supremacy principle and evaluate the compliance of Partner States with regional laws.

Action Steps:

- *Annual Reporting and Auditing*: Develop an annual report on the progress of regional integration and the alignment of national laws with EAC laws. This should include an audit of legal frameworks in each Partner State.
- *Feedback Mechanism*: Implement a feedback system where Partner States can share challenges in complying with regional laws, allowing for continuous improvements to the implementation strategy.
- *Impact Assessment*: Conduct regular assessments to evaluate the impact of legal supremacy on regional integration goals, such as trade flow, political cohesion, and legal consistency.

(VII) Public Engagement and Advocacy

Objective:
Increase public understanding and support for the legal framework and the supremacy of regional laws.

Action Steps:

- *Public Awareness Campaigns*: Use media platforms and community outreach to raise awareness about the importance of regional integration and the role of regional laws in achieving this goal.
- *Engagement with Stakeholders*: Involve business, civil society, and other stakeholders in discussions about regional law supremacy, fostering a sense of collective responsibility toward the integration process.
- *Education Programs*: Integrate regional law education into academic curricula and professional training programs, ensuring future generations are equipped to navigate the legal complexities of the EAC.

Conclusion

The strategy outlined above provides a comprehensive and systematic approach to implementing the supremacy of regional law under the EAC Treaty. By aligning national

laws with regional laws, building capacity at all levels of government, and ensuring effective enforcement, the EAC can achieve its integration goals and maintain the legal unity essential for regional cooperation.

Challenges & Recommendations

The report emphasizes the importance of managing data across multiple jurisdictions, which can be complicated by differing legal frameworks. To overcome this, it recommends:

- Developing a harmonized policy and legal framework across the region.
- Establishing uniform standards for cross-border data flows.
- Creating a regional task force to focus on cybersecurity and data privacy.

Conclusion

The East African Community stands at a crossroads in its digital transformation journey. By addressing the legal fragmentation in data protection laws and fostering regional cooperation, the EAC can create a robust data governance ecosystem that supports economic growth, protects individual rights and enhances cross-border digital trade. However, achieving these goals requires sustained efforts, comprehensive policy reforms and a commitment to harmonization across the EAC Partner States. By drawing on international best practices and regional models, the EAC can pave the way for a unified, secure and inclusive digital economy in East Africa.

The successful implementation of the EAC Data Governance Policy Framework is also crucial for realizing the region's digital economy and enhancing regional integration. Stakeholder engagement and a robust legal framework are necessary to ensure the sustainability of the region's data infrastructure and its alignment with global data governance practices.

This framework is a step toward realizing a unified and secure data environment that fosters economic cooperation and digital transformation in East Africa.

REFERENCES

[1] Gstrein, O.J. & Zwitter, A.J., "Extraterritorial application of the GDPR: promoting European values or power? "Internet Policy Review, 2021, 10(3). Available at: https://policyreview.info/articles/analysis/extraterritorial-application-gdpr-promoting-european-values-or-power

[2] Svantesson, D. J. B. "Article 3. Territorial scope. In C. Kuner, L. A. Bygrave, & C. Docksey (Eds.), The EU General Data Protection Regulation (GDPR): A commentary," Oxford University Press, 2019, pp. 74–99.

[3] Sangeeta K & Voss W. G, "The Digital Single Market: Move from Traditional to Digital? in Handbook on The EU and International Trade 384, 389 (Sangeeta Khorana & María García, eds., 2018).

[4] Drysdale, P. 'ASEAN: The Experiment in Open Regionalism that Succeeded,' Available at: https://www.eria.org/5.1.ASEAN_50_Vol_5_

[5] Corrales C, Marcelo & Aboy, Mateo and Minssen, Timo, 'Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual