Comparative analysis of data protection regulations in East African countries

Deo Shao, Fredrick Ishengoma, Anastasija Nikiforova and Mrisho Swetu

Abstract

Purpose – *Protection of personal data is integral to the digital economy, ensuring trust and privacy as its foundational elements. The purpose of this study is to analyze data protection laws in Tanzania, Kenya, Uganda and Rwanda to understand their legal frameworks and identify challenges hindering their effective implementation.*

Design/methodology/approach – *This study uses a comparative exploratory case study approach, analyzing legal frameworks of four East African (EA) countries through examination of legal documents, official reports and academic articles. The dimensions of analysis include registration, supervisory authority, data subject rights and cross-border data transfer regulations.*

Findings – *While all four EA countries are in the process of enacting data protection acts, they differ in scope, provisions and enforcement; more needs to be done to ensure mature data protection in these countries. The commonalities and distinctions in the legal frameworks are underscored, providing a mapping of data protection regulations in the EA region. Moreover, this study reports implementation constraints and areas for improvement.*

Practical implications – *The findings of this study provide valuable insights for policymakers, highlighting areas where data protection regulations can be improved. The results of this study can guide harmonizing regional data protection laws, ensuring consistent and effective enforcement. This study offers a foundation for future policy development and regional cooperation on data protection issues.*

Social implications – *The social implications of this research lie in its potential to shape public attitudes on data protection and privacy rights. By highlighting these concerns, this study may influence societal norms and values, encouraging a more informed and conscientious public discourse on inclusive policies that consider the diverse needs of different regional populations.*

Originality/value – *This study provides a pioneering comparative analysis of data protection regulations across four EA countries, offering unique insights into the regional variations and commonalities in legal frameworks. Its value lies in informing future policy development, enhancing regional cooperation and contributing to the harmonization of data protection practices in the selected EA countries, which remains an under-explored area in existing literature.*

Keywords *Data protection regulation, East Africa, Privacy, Cross-border data transfer, Personal data protection, Digital economy*

Paper type *Research paper*

(Information about the authors can be found at the end of this article.)

Received 13 June 2024
Revised 23 August 2024
Accepted 15 September 2024

1. Introduction

The rapid expansion of digital technologies, the commercialization of personal data and the highest dependence and reliance on data-driven activities over the recent decades (Macenaite, 2017; Rumbold and Pierscionek, 2017) are evidence of the global need for solid data protection regulations. Protecting personal data has become significant, as it is an integral part of the technological revolution of our digital age, the era of massive use of technology and the highest rate of growth for data-driven activities. In the Internet age, with the dominating use of online resources, accumulation of data and the highest level of dependence on digital technology, countries need to increase data protection regulations to avoid the invasion of individual privacy and protect people from the unjust treatment of personal data.

Data protection has emerged as a critical concern in both developed and developing countries (Hoofnagle *et al.*, 2019; Joo and Kwon, 2023; Ilori, 2020). Developed regions, exemplified by the European Union (EU), have made substantial progress in this area through frameworks such as the General Data Protection Regulation (GDPR). The GDPR has setup high standards for privacy protection, including principles. However, it is not a complete solution and must adapt to new challenges and technologies over time (Zaeem and Barber, 2020). In contrast, data protection in Africa remains in its formative stages, with regulatory frameworks still developing.

Efforts for data regulation are gaining momentum on a broader scale across the African continent. The African Union Data Policy Framework (AU, 2022) has been developed as a critical step toward the creation of a common data ecosystem and harmonized digital data governance regimes that will see the cross-border data exchange in Africa while upholding human rights, security and fair access to and sharing of the benefits.

Moreover, 37 of 55 African countries have adopted some form of regulation for protecting personal data (AU, 2022). Most data regulation efforts in Africa are concentrated on data protection, whose primary goal is to protect the privacy rights of Internet users (AU, 2022). Nevertheless, there are no benchmarks of "umbrella laws" that regulate every aspect of data, including data protection law, competition law, cyber security law, electronic communications and transactions law and intellectual property law, that are potentially conflicting in some cases and leave gaps in others (Adu, 2018).

The East African (EA) context presents distinctive challenges and opportunities in data protection. The diverse socioeconomic landscapes of countries heighten the complexity of data protection regulation, their unique legal traditions and varying levels of technological infrastructure, data maturity, digital readiness and regulatory environments across countries (Prinsloo and Kaliisa, 2022; Mganyizi, 2023).

The objective of this study is to fill the research gap in data protection regulations in EA countries, specifically Tanzania, Kenya, Uganda and Rwanda, by systematically exploring and comparing the existing data protection regulations in these countries in four dimensions – *registration requirement*; *supervisory authority*; *data subject rights*; and *cross-border data transfer*. The aim is to provide a comprehensive analysis of the legal frameworks, identify commonalities and variations and assess the strengths and challenges in implementing and enforcing these regulations.

As such, research questions (RQs) guiding this study are:

RQ1. How do the data protection regulations in Tanzania, Kenya, Uganda and Rwanda address the protection of data subject rights, data breach notification requirements and the establishment of regulatory bodies and cross-border data transfer?

RQ2. What are the similarities and differences in data protection regulations among East African Community (EAC) countries?

RQ3. What are the strengths and challenges in implementing data protection regulations in these EA countries?

This study contributes to both theory and practice. As a theoretical contribution, it addresses a research gap in data protection regulations within EA countries. It systematically analyses the legal frameworks in Tanzania, Kenya, Uganda and Rwanda. Identifying commonalities and variations in scope, provisions and enforcement mechanisms fills a prior void in research, shedding light on the less explored landscape of EA countries compared to other African countries. The definition of registration requirements, different supervisory structures and unique entitlements of data subjects highlights the complexity and nature of each country's approach to protecting personal data.

This study underscores the significance of international standards in guiding the development and implementation of domestic data protection regulations, advocating for globally coordinated mechanisms to address issues such as data exploitation and surveillance.

Additionally, it suggests avenues for future research to evaluate the practical implementation of these regulations and their impact on privacy rights and the digital economy. At a practical level, the findings serve as a roadmap for policymakers, by which they can inform and improve the existing data protection framework, as well as guide harmonization efforts (both regional and external) regarding personal privacy, consumer trust and business reputation in the digital space of EA. A harmonized data protection framework for EA (despite the non-binding nature of community-level regulations) can be instrumental in ensuring consistency across member states to simplify compliance and enhance cross-border data transfers, mitigating complexities and costs associated with varying national laws and fostering greater consumer trust and business efficiency. Additionally, aligning regional policies with international standards will strengthen the data protection infrastructure, facilitate regional cooperation and demonstrate a commitment to safeguarding personal data, thereby improving the region's global credibility and supporting effective policy development.

The rest of the paper is organized as follows: Section 2 provides a background on data protection regulations, Section 3 presents the research methodology, Section 4 presents results, Section 5 establishes the discussion and emphasizes the limitations of this study and the final section concludes the paper.

2. Background

2.1 Data protection. Key principles and provisions

Ensuring the protection of individuals' data is paramount, particularly in light of the regulations governing their processing by organizations. Consequently, data protection laws have been established to ensure the proper collection, use and disclosure of personal data, especially in the digital era (Zuiderveen Borgesius and Poort, 2017). This underscores the necessity for a robust legal framework that delineates the rights and responsibilities of both *data controllers* and *subjects* to ensure fair, transparent and secure processing of personal data (Hoofnagle *et al.*, 2019).

Data protection laws typically include essential principles and provisions designed to ensure that personal data is managed fairly, equitably and lawfully. These principles serve as the main guiding principles for organizations and establish the rights and protections afforded to individuals (Pearce and Platten, 1998). The fundamental principles of *lawfulness, fairness, equity, transparency and openness* play a key role in many data protection legislation.

Purpose limitation is another fundamental principle that limits organizations' use of individual data exclusively for legitimate and specific reasons made known to individuals when these data are collected (Rumbold and Pierscionek, 2017). The principle enshrined in Article 5(1)(b) of the GDPR, as well as Section 1798.100(b) of the California Consumer Privacy Act, prohibits the on-thread or excessive use of personal data, forcing organizations to have a lawful position to process the information (Cormack, 2016).

The principle of *data minimization* states that organizations should limit the amount of personal information they collect and store about individuals to the level necessary to achieve a specific purpose to prevent indiscriminate collection or retention (Quelle, 2017). Strictly related to this principle, the data accuracy provision requires companies to maintain the accuracy of the personal data they store in their information systems and implement ways to demonstrate compliance with privacy laws and regulations (Bélanger and Xu, 2015).

2.2 Data protection regulations in East Africa

The literature indicates that data protection across African continent is marked by the considerable complexity. Despite some progress, many regions, including EA, continue to face significant challenges (Ndemo *et al.*, 2023). This underscores the slow pace of

regulatory development and highlights the urgent need for more robust data governance structures tailored to local contexts. Similarly, in other African countries such as Nigeria, legislative gaps and practical challenges hinder the effective enforcement of data protection measures (Abdulrauf and Fombad, 2017). To address these issues, specific legal reforms are being proposed to update regulatory frameworks. These reforms are essential for mitigating the risks associated with data protection violations, particularly in nations experiencing rapid ICT advancements while struggling with inadequate regulatory mechanisms (Abdulrauf and Fombad, 2017).

EA countries are emphasizing the establishment of comprehensive data protection mechanisms and frameworks. The institutionalization of data protection regulations is increasing the focus on privacy and security. These regulations are designed to safeguard personal information while fostering investment and innovation (Martin *et al.*, 2019).

According to Greenleaf and Cottier (2022), EA countries have fundamentally lagged in the development of data protection regulations until 2019, when both Uganda and Kenya introduced data protection laws. Notably, these laws are heavily influenced by the GDPR. Rwanda followed suit by enacting its law in 2021, while Tanzania also has the specific Act for personal data protection. The EAC has required its member states to enact data protection legislation (Makulilo, 2015), whereas initiatives include the adoption of a *Bill of Rights for the EAC* in 2012. Unlike the African Charter on Human and Peoples' Rights, this Bill incorporates an explicit right to privacy. Its enforcement, however, awaits the approval of the EAC Heads of State.

The literature on data privacy in EA highlights several key challenges that shape the region's data protection landscape. EA countries have only recently begun implementing data protection frameworks, with existing regulations often lacking clarity in some areas. For instance, while Kenya's Data Protection Act is progressive, it falls short in providing detailed guidance on data anonymization and pseudonymization. Similarly, Tanzania's evolving regulations have gaps in defining and implementing standards for anonymization and pseudonymization, complicating compliance and enforcement (Staunton *et al.*, 2024).

Another challenge is the variability in data protection standards across the region. Differences in the scope and detail of data protection laws in countries like Kenya, Rwanda and Tanzania create a fragmented regulatory environment. For example, while Rwanda's Law Relating to the Protection of Personal Data and Privacy provides clearer definitions and regulations on pseudonymization, Kenya's approach remains less specific, leading to inconsistencies in data protection practices (Staunton *et al.*, 2024). This fragmentation hampers regional cooperation and complicates efforts to create a cohesive data protection framework.

3. Methodology

This research followed an exploratory case study approach, looking at four of six EAC countries. An exploratory case study approach is particularly suitable when new hypotheses and propositions are needed or when the problem at hand is a contemporary problem with little to no empirical information (Chopard and Przybylski, 2021). In this paper, the unit of analysis is the data protection laws for each EAC country – Uganda, Rwanda, Kenya and Tanzania. These four countries were selected because of their recent advancement in data protection frameworks, which provide a rich context for analysis and comparison. The selected countries are in different categories of the United Nation's e-Government Development Index [1]: Kenya and Rwanda are on the higher end (H2 and H3), and Uganda and Tanzania are on the medium end (M3 and M2). The heterogeneity in e-government maturity is a crucial element of this study. Thus, it allows for a detailed examination of data protection practices and challenges in EA, offering insights that could inform broader regional efforts.

Our approach includes several elements (Figure 1). First, extensive desk research was conducted to collect relevant information artefacts such as legal documents, official reports and academic articles related to data protection regulations in selected Eastern African countries. Following information artefact collection on selected countries, content analysis was conducted to better understand the data protection laws of Tanzania, Kenya, Rwanda and Uganda, structuring findings in four dimensions:

1. registration requirement;
2. supervisory authority;
3. data subject rights; and
4. cross-border data transfer.

These elements constitute fundamental components of regulatory laws governing data protection, playing a pivotal role in defining and overseeing the procedures through which organizations handle personal data.

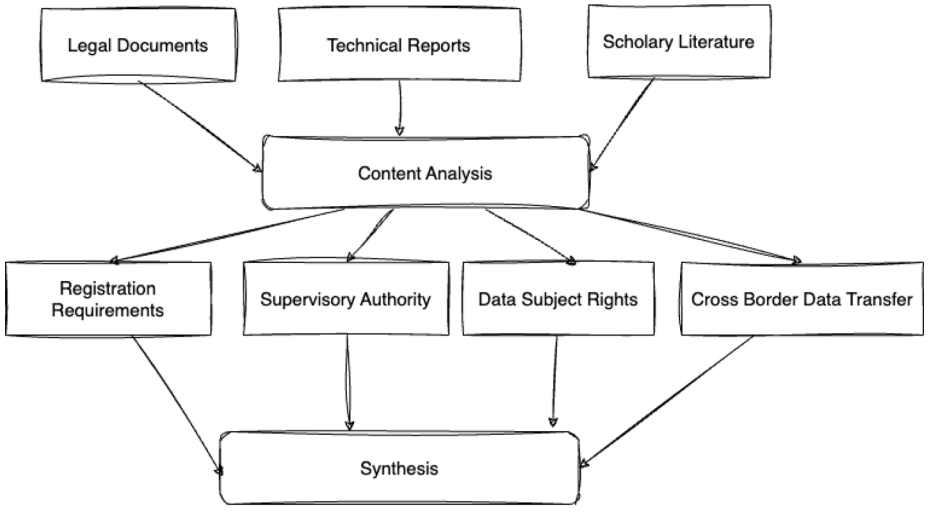
The scope and limitations of each legal framework (1), the provisions and instruments of each framework (2) and any other salient characteristics (3) were derived from the analyzed documents, thereby constituting a structured overview for selected countries. Afterwards, EA countries' regulations were compared to understand how similar or different they are, allowing for an analysis of this information and the data protection outcomes of the frameworks of EA countries.

4. Results

4.1 Data protection regulation landscape in the selected countries

4.1.1 Tanzania. The right to privacy is a constitutional right in Tanzania [2]. The motivation for the enactment of the Personal Data Protection Act (PDPA) and its regulations was the fact that the country has seen commercialization of personal data, technological development, use of personal data beyond the original purpose and compliance with the

Figure 1 Workflow of the methodological approach



Source: Authors own work

constitutional requirement, making personal data prone to misuse and unauthorized access to personal data.

The advancement and increased consumerization of Information and Communication Technology (ICT) in the country promoted the necessity for personal data governance. This then motivated the need to establish a specialized act to regulate personal data in the country. It was followed by the adoption of two Regulations – the Personal Data Protection Regulations, GN No 349 of 2023 and the guidelines for complaint handling.

The establishment of Tanzania's PDPA was a huge step in protecting individuals' privacy. The law outlines what constitutes personal data and sensitive personal data, data protection principles, registration of data controllers and processors, rules for collecting or processing sensitive personal data, cross-border data transfers and offences and penalties. On the other hand, the law establishes an institutional framework such as the Personal Data Protection Commission (PDPC) and a board responsible for overseeing the commission. The President appointed the board of the PDPC in January 2024, indicating the officiation of its operation.

In general, the PDPA applies to both data controllers and processors, legal or natural person, as well as the private and public sector in Tanzania.

4.1.2 Kenya. Recognizing the importance of individual privacy, the Government of Kenya is promoting the implementation of data protection law. The Data Protection Act in Kenya was enacted to establish a data protection framework classified as International Data Protection Standards.

Kenya's primary aspiration in enacting the Data Protection Act is to enhance the country's attractiveness to international investors, with a particular emphasis on investors in the ICT sector, by creating an environment that guarantees the protection of personal data. As a result of implementing this law, Kenya created the Office of the Data Protection Commission, an independent regulator responsible for enforcing data protection laws and resolving disputes arising from them.

4.1.3 Rwanda. The Rwanda Government Law on Protection of Personal Data (PPD) was enacted in 2021 to provide a legal framework of rights for the privacy of Rwandan citizens and articulate core guidelines on how the government and other public authorities process and use personal data. The core principles of the law specify the conditions relating to the collection, use, sharing and transfer of personal data in temporary or permanent storage (Mganyizi, 2023). The law serves as the gatekeeper of personal data, protects privacy rights and provides a framework for the safe use of data. The core principles of the law identify key roles that data controllers, data collectors and data processors (DCCPs) should take and maintain reasonable measures.

Moreover, the country's ambition to attract investments and foster innovation is one of the main drivers behind Rwanda's enactment and enforcement of data protection laws. Mutimukwe *et al.* (2019) argue that investors are becoming more demanding of compliance with data regulations. Rwanda has taken a big step in this by having data protection law and related rules as well as a protection authority that oversees and enforces these laws.

4.1.4 Uganda. Concern for personal rights and the general cyber landscape called upon the Government of Uganda to enact the Data Protection and Privacy Act, which stipulates the right to privacy and the right to confidentiality of personal data and provides guidelines for the processing of data in accordance with subsection (1) of a section of Data Protection and Privacy Act 2019. The law affords the rights of the individual whose data is processed (Muhangi, 2019). Among these rights are the "Right of an individual not to have personal data processed unless the consent on particulars of an individual is obtained," access to that information, to modify it, to rectify it, the right to erasure and many others, as provided therein. Notably, the law captures a data processor's obligation of mandated consent. The

Act makes a pertinent mention of the obligation of consent to be obtained by a data processor from the individuals being processed, as well as making such processing subject to information and the individual's free will.

The government has formed the National Information Technology Authority–Uganda (NITA-U) to address the implementation and application of data protection rights. The government's creation and sustenance of NITA-U shows its commitment to the positive implementation of data protection rights, as it assumes an institutionalized approach to implementing such rights. In particular, NITA-U is in charge of monitoring and enforcing data protection, covering all data processing activities carried out by all actors. The functions of the authority to regulate the data-protection space better and enhance digital services are intended to enable it to carry out its regulatory functions: coming up with policies, setting standards and guidelines and assessing ICT services and products against established and stipulated privacy and personal data protection rules and standards.

4.2 Comparative analysis of data protection regulations in East African countries

The study analysis was performed in Kenya, Uganda, Tanzania and Rwanda using four key areas, as described in the following subsections.

4.2.1 Registration requirement. In the Republic of Uganda, requirements necessary for registration are indicated in the Data Protection Regulations [3]. The regulation requires all DCCPs to be registered with the data protection office [4]. Moreover, the data protection office was given the power, in consultation with the board, to exempt DCCPs after a notice in a gazette. However, to date (2024), the office has not published any notice. This means that all DCCPs are required to be registered, regardless of their size. In Tanzania, DCCPs are required to be registered with the Personal Data Protection Commission (DPC) [5]. To put it simply, Tanzania's PDPA prohibits any person from collecting or processing personal data without being registered with the DPC [6]. Moreover, mandatory registration of DCCPs is regulated by the PDPA and its underlying regulations.

Meanwhile, Kenya has a mandatory registration of DCCPs [7]. However, registration of DCCPs in Kenya is subject to factors such as the nature of the industry, the volume of data processed, the sensitivity of data processed and any other criteria the commissioner may specify [8]. This means that there are DCCPs who are exempt from being registered with the Data Commissioner. Rwanda also has mandatory registration of DCCPs [9].

With regards to registration, all EA countries – Uganda, Rwanda, Tanzania and Kenya – require a compulsory registration of DCCPs. The only difference is that, in some countries, such as Kenya, there are categories of DCCPs who are exempted from registration with the ODPC. Table 1 provides a comparative summary of the registration requirements for DCCPs in selected EA countries.

4.2.2 Supervisory authority. The Supervisory Authority is the government regulatory body or institution tasked with monitoring compliance with the data protection laws.

The Data Protection and Privacy Act of Uganda establishes the Personal Data Protection Office (PDPO) and charges with the responsibility to oversee the implementation of the Data Protection and Privacy Act and the promotion of and respect for the right to privacy of individuals and their personal data. It is also expected to supervise, monitor and report on compliance with the right to privacy and personal data, as well as develop, implement and oversee programs to raise public awareness of the right to data protection. Furthermore, it shall be responsible for keeping and maintaining a register of data protection and privacy as well as any other function created by a law or organ deemed necessary to further, implement and enforce the Act. [10].

Moreover, the personal data protection office must be subordinate and report to the board. That is, there is the board that supervises the PDPO [11]. The NPDPD may be terminated by

Table 1 Comparison of data controller and processor registration requirements in selected East African countries

Criteria	*Uganda*	*Tanzania*	*Kenya*	*Rwanda*
Registration requirement	Mandatory for DCCPs	Mandatory for DCCPs	Mandatory for DCCPs	Mandatory for all intending to be a DCCP
Exemptions	Power to exempt after notice in gazette, but no published notices	No mention of explicit exemptions	Exemptions based on industry, data volume, nature of data and the sensitivity of data	No mention of explicit exemptions
Registration authority	Office of data protection	Commission for personal data protection	Commissioner for data protection	Supervisory authority of Rwanda
Publication of notices	No specific mention of published notices	No specific mention of published notices	No specific mention of published notices	No specific mention of published notices

Source: Authors' own work

the Minister after consultation with the board [12]. But the law does not prescribe by whom the board will be acquired and on what grounds they should be members. The independence of the PDPO and the qualifications of board members on matters relating to data protection in Uganda must, therefore, be questioned.

In Tanzania, the PDPC is accountable for all matters relating to data protection in Tanzania. The PDPC is mandated with the power to monitor compliance by DCCPs with the provisions of this Act, to register DCCPs, to receive, investigate and deal with complaints of alleged violations of personal data protection and privacy of individuals. It is also mandated to investigate and take action against any matter which appears to the commission to affect the PPD and violate the privacy of individuals, as well as to educate the public.

It is also mandated to establish cross-border cooperation mechanisms and advise the government on issues related to the implementation of the PDPA, as well as to perform other functions of the commission [13]. In this case, the commission is headed by the Director General, who is appointed by the president [14]. The Tanzania PDPA has established a Personal Data Protection Board, which is the governing body of the commission [15]. The chairman and vice-chairman are appointed by the president, while the remaining five members are appointed by the Minister of ICT [16]. The fact that the commission is established in this way raises questions about the independence of the Supervisory Authority, as there is no open space for competition among potential candidates for the positions. Merit-based appointment would require the position to be publicly open and advertised, and eligible people apply and be appointed if they meet respective requirements.

In Kenya, the Data Protection Act establishes a Supervisory Authority known as the DPC [17] where its recruitment process is initiated by the Public Service Commission [18]. At the end of the process, the Public Service Commission nominate three candidates who meet the requirements of the DPC [19]. The president is given the power to nominate and, with the approval of the National Assembly, to appoint the DPC [20].

In Rwanda, the data protection framework also recognizes and provides for the responsibilities of the Supervisory Authority [21]. The power of the Supervisory Authority includes issuing a certificate of registration to ensure that the processing of personal data complies with the provisions of the law and to ensure that the use of ICTs does not pose a threat to public freedoms and the privacy of an individual. It is also mandated to provide regulations regarding the application of the principal Act and to impose administrative sanctions in accordance with the provisions of the law [22]. Moreover, the Rwandan Supervisory Authority plays an important role in ensuring that DCCPs comply with the law. Table 2 compares supervisory authorities in EA countries.

Table 2 Comparison of data protection supervisory authorities in selected countries

Supervisory authority	*Uganda*	*Tanzania*	*Kenya*	*Rwanda*
Mandate	Oversees implementation, promotes protection of privacy rights, monitors, investigates and reports on observance of privacy rights	Monitors compliance by DCCPs, handles complaints and inquiries	Oversees implementation of the data protection act	Issues registration certificates, ensures data processing aligns with the law, regulates applications of the principal act and imposes administrative sanctions
Reporting structure	Reports to the board	Governing body is the personal data protection board, appointed by the president	Appointed by the president and reports to the national assembly	Appointed by the president
Leadership appointment	National personal data protection director appointed by the minister on the board's recommendation	Director general appointed by the president; chairman and vice chairman appointed by the president	DPC appointed by the president with national assembly approval	DPC appointed by the president

Source: Authors' own work

4.2.3 Data subject rights. Data subject rights constitute a crucial dimension of the comparative legal analysis of the existing legal frameworks on data protection in EA countries (Table 3).

In Uganda, *the Data protection and Privacy Act* recognizes the rights of data subjects, including the right to access personal data, the right to the processing of personal data, the right to prevent the processing of personal data for direct marketing, rights on automated decisions and the right to modification, blocking, removal and destruction of personal data [23].

In Kenya, *the Data Protection Act* recognizes the right to data portability, the right to access personal data, the right to automated decisions, the right to restriction of data processing, the right to the processing of personal data and the right to rectification and erasure [24].

The *Personal Data Protection Act of Tanzania* recognizes the rights of the data subject that are: the right to access personal data, rights related to automated decision-making, the right to prevent the processing of personal data that may affect the data subject, the right to prevent the processing of personal data for direct marketing purpose, the right to

Table 3 Data subject rights across the data regulations

Data subjects rights	*Tanzania*	*Uganda*	*Rwanda*	*Kenya*
The right to access personal data	X	X	X	X
The right to prevent the processing of personal data		X	X	X
The right to prevent the processing of personal data for direct marketing		X		
Rights in relation to automated decision	X	X	X	X
The right to rectification, blocking, erasure and destruction of personal data	X	X	X	X
The right to object			X	X
The right to portability of personal data			X	X
The right to erasure personal data			X	X
The right to designate an heir to personal data			X	X
The right to representation	X		X	X
The right to prevent processing of personal data that may affect the data subject	X			
The right to compensation	X			

Source: Authors' own work

compensation and the right to correction, blocking, deletion and destruction of personal data [25].

The *Data Protection Law of Rwanda* also stipulates several rights of data subjects, including rights to personal data, rights to object, rights to portability of personal data, rights not to be subject to a decision based on automated data processing, rights to restriction of the personal data, rights to erasure personal data, rights to rectification, rights to designate an heir to personal data and rights to representation [26].

4.2.4 Cross-borders data transfer. The transfer of data across borders significantly contributes to the social and economic development of EA countries.

In Uganda, the transmission of personal data outside Uganda or to an international organization is permissible only if adequate measures are in place to safeguard the personal data. These measures must provide at least the same level of protection as stipulated by the Ugandan law particularly concerning the consent of the data subject [27].

In Rwanda, the transfer of personal data overseas is permitted if the individual granted consent and the Supervisory Authority authorized the DCCPs on the basis of evidence of sufficient protection of the personal data, or it is required for the performance of the contract or the performance of public interest [28]. In Kenya, an individual can authorize the transfer of personal data overseas on the basis of a determination of adequacy decision, appropriate safeguard, consent and necessities.

Transfer of personal data outside Tanzania is permitted under the following circumstances:

- when the recipient country provides adequate data protection, subject to certain conditions;
- when the transfer to a country without data protection, under additional safeguards with explicit consent of the data subject; and
- under special circumstances, such as when required for the performance of a contract [29].

4.3 Identification of differences and unique aspects of data protection laws in East African countries

In emphasizing the significance of distinct characteristics, the data protection laws in EA countries diverge in their approaches. Notably, the Tanzanian PDPA provides comprehensive coverage for both public and private sectors, ensuring thorough PPD (*Personal Data Protection Act, Tanzania*). By contrast, Kenya has implemented distinct regulations for the public and private sectors, with the Data Protection Act applying to both entities (*Data Protection Act, Kenya*).

Substantial requirements for data localization are incorporated into the Rwanda Data Protection Act; Kenya has data localization requirement on sensitive data; Tanzania and Uganda do not have clear data localization rules.

The Uganda Data Protection Regulations include measures to protect biometric data and recognize the special privacy considerations associated with this type of information (*Data Protection and Privacy Act, Uganda*). The emphasis on biometric data sets Uganda from other countries in its approach to addressing emerging technological challenges.

4.4 Gaps and challenges in data protection regulations

The data protection regulatory landscape in EA countries have challenges that could compromise the overall effectiveness of the regulations. An illustrative example is Uganda, where a gap exists. Although the law mandates registration for all DCCPs, no exemption notices have been published in the gazettes. The lack of explicit standards for exemption

introduces ambiguity into the process, potentially impeding the efficient implementation of measures to safeguard data.

The analysis of the Ugandan regulation calls into question the ability of their Supervisory Authority to be independent self-sufficient and competent. The Act is silent on the constitution of the Personal Data Protection Office oversight board and the qualifications of its members. This raises questions about whether the body is independent and whether those involved have any knowledge of data protection issues. This issue may exist because of a lack of transparency, which could be then overcome by ensuring it.

Tanzania, in turn, has limited degree of transparency and openness in the selection of its supervisory body, called the Personal Data Protection Commission. This commission is vital for ensuring compliance, registering DCCPs and resolving disputes. The lack of an open vetting process may affect how independent or effective the regulatory authority is perceived to be.

A unique challenge mentioned for Rwanda is data localization, which means that personal data must be stored in a specific location and processed only there. This can be challenging for companies and organizations that operate across these borders, as in most cases, any data they provide is located outside the country.

Embracing these challenges proactively will foster the development of dynamic regulatory framework that will strike the balance between the protection of privacy and the enabling of data-driven activities that are essential for socioeconomic development.

5. Discussion and limitations

5.1 Discussion

The analysis of data protection laws highlights critical building blocks of effective frameworks, along with key areas that stand out as policy efforts. Although the enactment of data protection laws is a step in the right direction, variations point to the need for harmonization with international standards.

Supervisory authorities board members selection methods, their openness and transparency, are essential, as issues related to the creation of boards may raise doubts about their objectivity. Moreover, the private appointment of the Director General in Tanzania may also call into question the impartiality of the board in the eyes of the public. Therefore, there is a need to appoint these supervisory authorities through a transparent and competitive process. This, in turn, can guarantee more efficiency in their duties.

Moreover, in Uganda, the need to publish notification of exemptions implicates the issue of registration difficulty. When the conditions that guide the granting of exceptions are clear and publicly available, it will be possible to have a registration process that is more transparent (Matheus *et al.*, 2021). Added to that is the emphasis on data localization in Rwanda imposes huge constraints for entities outside the country. In the digital economy, however, it is necessary to find a balance between creating a measure of security and safety at the national borders and at the same time being able to relate with other nations. This ambivalence is another factor to capitalize on and exploit to be fully empowered to take advantage of the most powerful scavenger benefit of the movement of information across global boundaries (Larionova and Shelepov, 2021).

The analysis among the EA's data protection frameworks highlights commonalities. However, variations in exemptions, transparency in supervisory authority appointments and data subject rights reveal varying levels of maturity and effectiveness in the implementation of these frameworks. Understanding these nuances is essential for recognizing both the strengths and limitations of existing data protection efforts, which can guide reforms and facilitate regional cooperation to tackle shared challenges and align with international standards.

The analysis also indicates impact of current data protection frameworks on the privacy landscape. While progress has been made in establishing legal structures and regulatory bodies, the practical effects on data privacy vary across countries. For example, the effectiveness of enforcement mechanisms, public awareness of data rights and organizational compliance with data protection regulations differ. Although the presence of regulatory bodies and data protection laws are steps in the right direction, challenges such as unclear exemption processes, varying degrees of transparency and limited public engagement can undermine these frameworks' effectiveness. Further empirical research and case studies are, however, needed to fully assess how these regulations affect data protection practices and privacy outcomes.

Comparing EA's data protection frameworks with the EU's GDPR provides insights into their effectiveness. The GDPR is renowned for its comprehensive approach, including stringent requirements for transparency, accountability and data subject rights, setting a high standard for global data protection practices. In contrast, EA's frameworks, while progressing, often lack the GDPR' level of detail and robustness. For instance, GDPR emphasis on clear exemptions, robust enforcement mechanisms and detailed data subject rights provides a benchmark against which EA regulations can be measured. Highlighting these differences advocates for the enhancements of regional data protection laws to align with international best practices and underscores the need for continuously refinement to better safeguard privacy and foster regional and international cooperation.

A significant strength in EA's data protection governance is the establishment of legal frameworks that reflect an increasing awareness of privacy and data security. These frameworks provide a structure that enhances regulatory oversight and supports the protection of personal data addressing privacy concerns and fostering trust in the era of digital economy.

Overall, this study underscores the necessity for EA countries to align their data protection regulations more closely with international standards, such as the GDPR. This alignment would improve the effectiveness of individual frameworks, facilitate cross-border data exchanges and bolster international trade cooperation and the digital economy at large.

5.2 Limitations

While this study presents useful insights, it is important to contextualize the findings. The availability, quality and detail of the data recorded in each country, as well as the timing of the regulatory framework being adopted, may limit the comparability of some findings. The evolving nature of the digital space means there are likely to be rapid changes in the regulatory regime governing data protection that occur immediately after publication. Given that it is likely to be practically impossible to impose new post-publication constraints on regulatory functions that were in force before that period, this underscores the need for regular review.

Although this study generalizes the results to some extent to the entire EA region, it should be emphasized that the study considered four of the six EAC countries (Tanzania, Rwanda, Uganda, Kenya, South Sudan, Rwanda and Burundi) where South Sudan and Burundi were not included in the sample, which may prevent the study from drawing a definitive conclusion for the region because of this lack of representation. Future research may expand this research to include the remaining countries, whereas this study has deliberately limited the sample, given the affiliation with the selected countries in line with Lnenicka *et al.* (2024).

Another limitation is related to the reference source, which is secondary resources such as the legal documents, official reports and scholarly articles, which may not capture the practical implementation and impact of the regulations on privacy rights and the digital economy. However, this limitation of scope was deliberate, as the study intention was to

take this very first step toward understanding the current situation in data protection regulation in the selected countries, as well as to encourage further research. Considering this limitation, as well as the fact that sometimes we faced unavailability of data or difficulties in finding and accessing it, subsequent research would benefit from focusing on empirically assessing the effectiveness of these regulations in various domains, with a particular focus on accelerating of digital economy.

6. Conclusion

This research examines the state of data protection in EA countries – Kenya, Tanzania, Uganda and Rwanda – by comparing their laws, policies and enforcement frameworks. All four nations have established legal structures for data protection, demonstrating a foundational commitment to safeguarding personal privacy. However, notable differences in implementation and effectiveness are evident. Kenya and Uganda stand out for their robust regulatory structures, emphasizing transparency, whereas Tanzania's supervisory authority appointment process lacks transparency, potentially compromising its effectiveness. Rwanda's data localization measures, while intended to enhance security, could potentially hinder cross-border data flows, revealing a need to balance national security with international cooperation. Furthermore, inconsistencies in exemption processes and registration difficulties uncover gaps in the regulatory frameworks. These issues suggest areas where reforms could improve clarity and operational efficiency, contributing to more effective data protection across the region.

Moving forward with the development of data protection in EA will require concerted efforts between governments and other stakeholders within the data ecosystem. Further, as more countries in Africa develop similar laws, a comparative assessment of the fairness of the laws in the EA context to broader African contexts will be needed. Moreover, a comprehensive data protection strategy in EA should include the development and implementation of strong policies, enhancing data security and privacy frameworks, promoting awareness on data protection, enhancing collaboration with other jurisdictions and ensuring the application of agreed standards and best practices including those under the GDPR.

This study revealed the potential role of data protection and privacy. It calls policymakers and regulators, to develop specific-regional data protection regulations and ensure that the regulations of one region are interoperable with the other regions. Organizations operating in these nations are encouraged to invest in data security and privacy infrastructure to enable the enforcement of these existing regulations. For researchers, this provides a starting point to study the area of data protection in chosen EA countries, as this area of research is nascent. Moreover, this paper highlights the current evolution in the policy of data protection in these nations and as such emphasizes the need for further research to strengthen and harmonize the policies in this area.

This study addresses the gap between theoretical and practical aspects of data protection by systematically analyzing the legal frameworks of Tanzania, Kenya, Uganda and Rwanda. It identifies key similarities and differences in their data protection approaches, thereby filling significant research gap in EA, a region that has been less explored compared to others. By examining these frameworks, this study enhances our theoretical understanding of data protection practices and underscores the importance of international standards, such as the GDPR, as benchmarks for developing robust domestic regulations. It advocates for coordinated global efforts to enhance data protection and combat data exploitation. It offers actionable recommendations for policymakers, linking theoretical insights with practical implications.

The findings contribute to both academic discourse and practical policy development by highlighting the need for robust data protection laws and alignment with international standards. Finally, as a practical contribution, this study provides a roadmap for

policymakers to fine-tune existing data protection frameworks, advocating for regional and international harmonization.

Notes

1. Available at: https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf
2. Article 16 of the Constitution of the United Republic of Tanzania, 1977 [CAP 2 RE 2005] .
3. Regulation 15 of Data Protection Regulation 2021.
4. Ibid, regulation 15(1).
5. Section 7 of the Act, No. 11 of 2022 .
6. Section 14 of the Act, No. 11 of 2022
7. Section 18 of the Act, No. 24 of 2019 .
8. Section 18 (2) of the Act, No. 24 of 2019 .
9. Article 29 of the Data Protection and Privacy law 2021.
10. Section 5 of the Act.
11. Section 4 of the Act.
12. Ibid. Regulations 5.
13. Section 7 of the Act, No. 11 of 2022.
14. Section 11 of the Act, No. 11 of 2022.
15. Section 8 of the Act, No. 11 of 2022 .
16. Ibid.
17. Section 5 of the Act, No. 24 of 2019.
18. Section 6 of the Act, No. 24 of 2019.
19. Section 6(3) (e) of the Act, No. 24 of 2019.
20. Section 6(4) of the Act.
21. Article 28 a 29 of the Act.2nd.
22. Ibid Article 28 of the Act.
23. Part v of the Data Protection and Privacy Act, 2019.
24. Sections 34, 35, 36 a 38 of the Act, No. 24 of 2019 .2nd
25. Sections 33, 34, 35, 36, 37 a 38 of the Act, No. 11 of 2022.
26. Article 19, 20, 21, 22, 23, 24, 25 and 26 of Rwanda Data Protection Law, 2021.
27. Section 19 of Data Protection and Privacy Act, 2019.
28. Article 48 of Rwanda Data Protection law, 2021.
29. Section 31, 32, 33 a 34 of the Act, No. 11 of 2022.

References

Adu, K.K. (2018), "The paradox of the right to information law in Africa", *Government Information Quarterly*, Vol. 35 No. 4, pp. 669-674.

Abdulrauf, L.A. and Fombad, C.M. (2017), "Personal data protection in Nigeria: reflections on opportunities, options, and challenges to legal reforms", *Liverpool Law Review*, Vol. 38 No. 2, pp. 105-134, doi: 10.1007/s10991-016-9189-8.

African Union (2022), "AU data policy framework", available at: https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf

Bélanger, F. and Xu, H. (2015), "The role of information systems research in shaping the future of information privacy", *Information Systems Journal*, Vol. 25 No. 6, pp. 573-578.

Chopard, K. and Przybylski, R. (2021), "Methods brief: case studies", available at: www.jrsa.org/pubs/factsheets/jrsa-research-methods-brief-case-studies.pdf (accessed 28 January 2024).

Cormack, A.N. (2016), "Downstream consent: a better legal framework for big data", *Journal of Information Rights, Policy and Practice*, Vol. 1 No. 1.

Greenleaf, G. and Cottier, B. (2022), "International and regional commitments in African data privacy laws: a comparative analysis", *Computer Law & Security Review*, Vol. 44, p. 105638.

Hoofnagle, C.J., Van Der Sloot, B. and Borgesius, F.Z. (2019), "The European Union general data protection regulation: what it is and what it means", *Information & Communications Technology Law*, Vol. 28 No. 1, pp. 65-98.

Ilori, T. (2020), "Data protection in Africa and the COVID-19 pandemic: old problems, new challenges and multistakeholder solutions", Association for progressive communications, 15 June.

Joo, M.H. and Kwon, H.Y. (2023), "Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea", *Government Information Quarterly*, Vol. 40 No. 2, p. 101805.

Larionova, M. and Shelepov, A. (2021), "Emerging regulation for the digital economy: challenges and opportunities for multilateral global governance", *International Organisations Research Journal*, Vol. 16 No. 1, pp. 29-63.

Lnenicka, M., Nikiforova, A., Luterek, M., Milic, P., Rudmark, D., Neumaier, S., Santoro, C., Flores, C.C., Janssen, M. and Bolívar, M.P.R. (2024), "Identifying patterns and recommendations of and for sustainable open data initiatives: a benchmarking-driven analysis of open government data initiatives among European countries", *Government Information Quarterly*, Vol. 41 No. 1, p. 101898.

Macenaite, M. (2017), "The 'riskification' of European data protection law through a two-fold shift", *European Journal of Risk Regulation*, Vol. 8 No. 3, pp. 506-540.

Makulilo, A.B. (2015), "Myth and reality of harmonization of data privacy policies in Africa", *Computer Law & Security Review*, Vol. 31 No. 1, pp. 78-89.

Martin, N., Matt, C., Niebel, C. and Blind, K. (2019), "How data protection regulation affects startup innovation", *Information Systems Frontiers*, Vol. 21 No. 6, pp. 1307-1324.

Matheus, R., Janssen, M. and Janowski, T. (2021), "Design principles for creating digital transparency in government", *Government Information Quarterly*, Vol. 38 No. 1, p. 101550.

Mganyizi, D.D. (2023), "Assessment of independence of regulatory structures governing data protection and privacy in East Africa: a case study of Kenya and Tanzania", *International Journal of Law and Politics Studies*, Vol. 5 No. 6, pp. 10-17.

Muhangi, K. (2019), "Overview of the data protection regime in Uganda", *Journal of Data Protection & Privacy*, Vol. 3 No. 1, pp. 82-92.

Mutimukwe, C., Kolkowska, E. and Grönlund, Å. (2019), "Information privacy practices in e-government in an African least developing country, Rwanda", *The Electronic Journal of Information Systems in Developing Countries*, Vol. 85 No. 2, p. e12074.

Ndemo, B., Ndung'u, N., Odhiambo, S. and Shimeles, A. (Eds) (2023), *Data Governance and Policy in Africa*, Palgrave Macmillan, London, doi: 10.1007/978-3-031-24498-8.

Pearce, G. and Platten, N. (1998), "Achieving personal data protection in the European Union", *JCMS: Journal of Common Market Studies*, Vol. 36 No. 4, pp. 529-547.

Prinsloo, P. and Kaliisa, R. (2022), "Data privacy on the African continent: opportunities, challenges and implications for learning analytics", *British Journal of Educational Technology*, Vol. 53 No. 4, pp. 894-913, doi: 10.1111/bjet.13226.

Quelle, C. (2017), "The 'risk revolution' in EU data protection law: we can't have our cake and eat it, too", *Data Protection and Privacy: The Age of Intelligent Machines*, Vol. 10.

Rumbold, J.M.M. and Pierscionek, B. (2017), "The effect of the general data protection regulation on medical research", *Journal of Medical Internet Research*, Vol. 19 No. 2, p. e47.

Staunton, C., Edgcumbe, A., Abdulrauf, L., Gooden, A., Ogendi, P. and Thaldar, D. (2024), "Cross-border data sharing for research in Africa: an analysis of the data protection and research ethics requirements in 12 jurisdictions", *Research Square*, doi: 10.21203/rs.3.rs-4217849/v1.

Zaeem, R.N. and Barber, K.S. (2020), "The effect of the GDPR on privacy policies: recent progress and future promise", *ACM Transactions on Management Information Systems*), Vol. 12 No. 1, pp. 1-20.

Zuiderveen Borgesius, F. and Poort, J. (2017), "Online price discrimination and EU data privacy law", *Journal of Consumer Policy*, Vol. 40 No. 3, pp. 347-366.

Further reading

Purtova, N. (2015), "The illusion of personal data as no one's property", *Law, Innovation and Technology*, Vol. 7 No. 1, pp. 83-111.

Author affiliations

Deo Shao is based at the Johannesburg Business School, University of Johannesburg, Johannesburg, South Africa and Department of Information Systems, College of Informatics and Virtual Education, The University of Dodoma, Dodoma, United Republic of Tanzania.

Fredrick Ishengoma is based at the Department of Information Systems and Technology, College of Informatics and Virtual Education, The University of Dodoma, Dodoma, United Republic of Tanzania.

Anastasija Nikiforova is based at University of Tartu, Tartu, Estonia.

Mrisho Swetu is based at Digital Agenda for Tanzania Initiative, Dar es Salaam, United Republic of Tanzania.

Corresponding author

Deo Shao can be contacted at: deoshayo@gmail.com