



COMPARATIVE STUDY OF DATA PROTECTION LEGISLATION FRAMEWORKS ACROSS THE EAST AFRICAN COMMUNITY

March 2024

Authors: Allan Mukuki ; Alex Assenga

This publication was co-funded by the European Union, Belgium, Estonia, Finland, France and Germany under the EU Global Gateway Strategy. Its contents are the sole responsibility of Strathmore University and do not necessarily reflect the views of the Commissioners.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
1 INTRODUCTION	3
1.1 Objectives of the Study	4
2 OVERVIEW OF DATA PROTECTION LAWS IN EAST AFRICA.....	5
2.1 Kenya	5
2.2 Uganda	6
2.3 Rwanda	6
2.4 Tanzania.....	8
2.5 Burundi	8
2.6 Somalia.....	9
2.7 South Sudan.....	10
2.8 The Democratic Republic of the Congo (DRC).....	10
2.9 EAC Legal Framework for Cyber Laws 2008.....	11
2.10 The Malabo Convention.....	12
2.11 The Common Market Protocol.....	13
3 LEGAL GAP ANALYSIS	15
3.1 Definition and Classification of Personal Data	15
3.2 Cross-border Transfer of Data	15
3.3 Lawful Processing of Personal Data.....	22
3.4 Investigations.....	23
4 BEST PRACTICES FROM OTHER REGIONAL BODIES	25
4.1 The European Union General Data Protection Regulations (GDPR).....	25
4.2 Association of South-East Asian Nations (ASEAN)	27
5 RECOMMENDATIONS.....	30
5.1 Preliminary Recommendations for Short-Term Measures.....	30
5.2 Preliminary Recommendations for Long-Term Measures.....	32
6 BIBLIOGRAPHY	35

EXECUTIVE SUMMARY

The study maps legislation, distinguishing differences in the existing and proposed data protection laws and trade laws within the East African Community. As part of the project's broader initiatives, the study makes a comparative analysis of data protection legislation across EAC partner states to identify legal gaps and make informed recommendations. It offers a comprehensive overview of data protection laws in EAC countries, delving into specific provisions for Kenya, Uganda, Rwanda, Tanzania, Burundi, Somalia, the Democratic Republic of the Congo, and South Sudan. Additionally, it explores relevant international agreements such as the EAC Legal Framework for Cyber Laws 2008, the Malabo Convention and the Common Market Protocol. It investigates primary gaps in the legislation and examines the approaches other regional bodies like the EU and ASEAN have approached the differences in the data protection laws of partner states and provides preliminary recommendations for short and long-term measures to strengthen regional trade, cross-border data flows and cooperation.

This analysis reveals a diverse landscape of data protection laws across EAC partner states with varying levels of implementation and enforcement. While some partner states have made significant strides, others are still in the process of developing data protection and privacy frameworks. The operationalization of these laws is critical for instilling trust among citizens and businesses, mitigating data breach risks and fostering economic growth. The ratification of the Malabo Convention emerges as a crucial aspect, with only two of the EAC partner states having done so. The Convention mandates states to ensure that domestic laws align with international standards on data protection. Capacity building for Data Protection Authorities is also essential for effectively addressing data breaches and preserving privacy rights. Strengthening DPAs' efforts will not only enhance their ability to respond to breaches but also foster a culture of compliance and trust.

In the short term, it is proposed to support DPAs in accelerating the operationalization of data protection laws and the ratification of the Malabo Convention. Other proposed measures include having capacity-building initiatives for DPAs, collaborating in investigating data breaches and promoting cross-border data flows. Looking ahead, it is recommended to ensure the development of common guidelines for assessing adequacy levels of personal data protection along with the establishment of a working group on data protection to facilitate the alignment of legislation and policies on the protection of personal data in the EAC. Additionally, translating data protection

Comparative study of the data protection legislation frameworks across the East African Community

laws into local languages and strengthening penalties for violations is crucial for promoting widespread compliance and accountability.

The recommendations emphasize the importance of collaborative efforts, stakeholder engagement, and a balanced approach to regulatory frameworks. By implementing these measures, the EAC can foster a robust data protection ecosystem, promote trust, and empower individuals with greater control over personal data. The preliminary recommendations for short-term and long-term measures are aimed at improving regional trade, cooperation, and potential harmonisation. This study is launched based on insights from the East Africa Exchange on Data Protection series stands as a collaborative effort to fortify regional cooperation on data protection in the East African Community.

I INTRODUCTION

The [African Union European Union Digital for Development Hub](#) (AU-EU D4D Hub) project aims to support African government agencies to identify and seize digitalisation opportunities for inclusive and sustainable development. The project covers three key activities, namely, technical assistance to national and regional institutions to develop or operationalise digital transformation plans and support the implementation of digital projects, the exchange of knowledge between African and European stakeholders which includes experiences, skills, and expertise and dialogues between governments, civil society, private sector and academia in Africa and Europe to promote collaborative policy-making and foster new partnerships. The AU - EU D4D Hub Project aspires to facilitate strategic partnerships and boost joint investments in digital for development between the EU and the AU to contribute to the reduction of the social and geographic digital divides, ensuring a human rights-based approach and leveraging digital innovation for inclusive and green sustainable development.

The Data Governance in Africa Initiative aims to promote an inclusive data-based economy and society. The project is an initiative resulting from the cooperation of the EU and its member countries' Digital Development Hub (D4D Hub). The initiative aims to strengthen comprehensive and unified policies and rules regarding personal and other information, promote cross-border data communication to create business opportunities and experiment with regional regulatory environments and promote partnerships for the development of green and secure data infrastructure.

The East Africa Exchange on Data Protection Activity follows from the above projects and advocates for fostering peer-to-peer learning and experience sharing among East African Data Protection Authorities. It aims to facilitate knowledge exchange, encourage cross-border collaboration, and emphasize the importance of exchanging insights and engaging with a diverse array of stakeholders, including civil society, academia, private sector entities and other stakeholders in the digital economy. The activity aims to improve compliance and service delivery by sharing resources, coordinating with development partners and leveraging on the existing networks.

This legal study was launched based on recommendations from the knowledge exchange activity that took place after a physical engagement of Data Protection Authorities from Kenya, Uganda,

Tanzania, and Rwanda as well as key regional stakeholders in data protection, the local private sector and civil society. The activity was aimed at improving collaboration and cooperation between East African countries on Data Protection and several opportunities for collaboration were identified on regional cooperation on Data Protection. The study makes recommendations that were presented at the second workshop in the series in March 2024 in Kampala, Uganda. Based on this study, delegates from all East African Community partner states including key stakeholders were able to discuss short-term and long-term measures to strengthen regional cooperation on data protection.

I.1 Objectives of the Study

The objectives of the study were:

- i. To develop a comparative study on data protection legislation across the East African Community, aiming to identify legal gaps, make recommendations, and cite areas for further research.
- ii. To map legal instruments and identify the nuanced differences in existing and drafted Data Protection Laws and the Trade Laws among the East African Community countries.
- iii. To investigate the primary gaps in the Data Protection Laws and the Trade Laws across East African Community countries.
- iv. To examine practices that EAC partner states can adopt from other regional communities, such as the EU and ASEAN.
- v. To provide some preliminary recommendations for short-term and long-term measures to improve regional trade and cooperation, and possibly harmonisation.

2 OVERVIEW OF DATA PROTECTION LAWS IN EAST AFRICA

This section provides an overview of the legal frameworks pertaining to data protection and privacy laws in the East African Community. It specifically highlights the status of implementation of data protection laws across the EAC partner states, covering the data protection laws including regulations and guidelines. It aims to identify variations in approaches, both in existing and proposed data protection and trade Laws in the EAC countries.

2.1 Kenya

Data Protection Laws	Enforcement Agency
The Data Protection Act (DPA), 2019 came into force on November 25, 2019. Regulations The regulations came into effect at different times and include: + The Data Protection (General) Regulations, 2021 which came into effect in February 2022. + The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 which came into effect in July 2022. + The Data Protection (Complaints Handling and Enforcement) Regulations, 2021 which came into effect in February 2022. + The Data Protection (Civil Registration) Regulations, 2020 which came into effect in October 2020. Guidance Notes + Guidance Note on Registration of Data Controllers and Data Processors + Guidance Note for Electoral Purposes + ODPC Guidance Note on Data Protection Impact Assessment + Guidance Note on Consent + Guidance Note For Digital Credit Providers + Guidance Note for the Education Sector + Guidance Note for the Communication Sector Other frameworks include: + The ODPC Complaints Management Manual	The Office of the Data Protection Commissioner (ODPC) is the independent agency in charge of the protection of personal data and privacy in Kenya.

Data Protection Laws	Enforcement Agency
+ Alternative Dispute Resolution (ADR) Framework/ Guidelines	

2.2 Uganda

Data Protection Laws	Enforcement Agency
Data Protection and Privacy Act (DPPA) No.9 of 2019 Assented to on 25 February 2019 and came into effect on 3 May 2019. Regulations + Data Protection and Privacy Regulations 2021 Guidance Notes + Guidance note on lodging complaints + Guidance note on registration and renewal of registration + Guidance note completion of the annual compliance report Sector Specific laws + The Access to Information Act, 2005 + The Regulation of Interception of Communications Act, 2010 + The Computer Misuse Act, 2011 (as amended) + The Registration of Persons Act, 2015	The Personal Data Protection Office (PDPO) is an independent Office that has been established under the National Information Technology Authority – Uganda (NITA –U). The PDPO reports to the board of the NITA –U. ¹

2.3 Rwanda

Data Protection Laws	Enforcement Agency
Law Relating to the Protection of Personal Data Protection and Privacy Law (DPL) 2021² Guidelines + Registration guide or Data Controllers and Data Processors + Guidance on Personal Data Inventory and Readiness Checklist Tools	Rwanda's Data Protection Office was established under the NCSA (National Cyber Security Authority) on 31 March 2022. The Data Protection Department is a department under the NCSA.

¹ Regulation 3 of the Data Protection and Privacy Regulations, 2021 of Uganda.

² Personal Data Protection and Privacy Law (DPL) 2021, (N° 058/2021) entered into force on 13 October 2021.

Data Protection Laws	Enforcement Agency
+ Guidance on the designation of a Data Protection Officer + Data Protection Impact Assessment Guide + Guidance note on complaint lodging for data subjects Sector specific Laws and Instructions + Law N° 017/2021 du 03/03/2021 relating to financial service consumers. + Law N° 73/2018 of 31/08/2018 governing credit reporting system. + Law N° 029/2023 of 14/06/2023 governing population registration in the national single digital identity system. + Law N°24/2016 of 18/06/2016 governing information and communication technologies + Law No. 60/2013 of 22 August 2013 Regulating the interception of Communications. + Law N° 04/2013 of 08/02/2013 relating to access to information. + Law N° 60/2018 of 22/8/2018 on prevention and punishment of cybercrimes. + Ministerial instructions N° 001/MINICT/2024 of 22/03/2024 on child online protection. International Conventions Rwanda has ratified the following Conventions; + Malabo Convention on Cybersecurity and Personal data protection. + Budapest Convention on Cybercrime. National Policies + National Data Revolution Policy of 2017 + National Cybersecurity Policy of 2015 + Child Online Policy of 2019 + National AI Policy	

2.4 Tanzania

Data Protection Laws	Enforcement Agency
The Personal Data Protection Act, 2022³ Regulations⁴ + The Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023, GN No. 349 of 2023.⁵ + The Data Protection (Complaints Handling Procedure) Regulations, GN No 350 of 2023.	The Personal Information Protection Commission is an independent office governed by the Board of Personal Data Protection Commission. The Chairman and the Vice-Chairman are appointed by the President while the other five members of the board are appointed by the Minister responsible for Communication.

2.5 Burundi

Data Protection Laws	Enforcement Agency
Burundi does not have a law that specifically regulates personal data protection. However, there are a number of related laws in the field of cyberspace, as well as sectoral laws in health, finance, banking, and telecommunication. Sectoral laws and regulations + Law no. 1/16 of 16 March 2022 on Prevention and Punishment of acts of Cyber-criminality in Burundi.⁶ + Law no. 1/012 of May 30, 2018, on the Code of Health Care and	There is no national data protection authority in Burundi.

³ The Personal Data Protection Act, 2022, [Government Notice No. 395b Published on 13/6/2023, the United Republic Of Tanzania Chapter 44 English Version](#). The Act is available in both English in Swahili.

⁴ The Ministry of Information, Communication and Information Technology published the Personal Data Protection Regulations (the Regulations) on the 12th of May 2023. You can see the [summary of the regulations](#) here.

⁵ The Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 provides for the procedure of registration of Data Controllers and Data Processors as well as the prescribed forms for registration, and the procedure of enforcing rights of a data subject.

⁶ Loi No. 1/16 du 16 mars 2022 portant prévention et répression de la cybercriminalité au Burundi.

Data Protection Laws	Enforcement Agency
Health Services Provision in Burundi, healthcare institutions are required to maintain the confidentiality of patient information, unless confidentiality is waived in cases provided for by law. + Law No. 1/17 of August 22, 2017, governing banking activities + Law n° 1/10ndu March 16, 2022 on the prevention and repression of cybercrime in Burundi: This law comes up of the cybercrime issues, and use of personal data in Burundi. It aims to protect individuals' privacy and ensure responsible handling of personal information by organizations. + Ministerial Orders in the telecommunications sector.⁷ + As of March 2024, a Draft Decree that creates the “National Commission for ICT, protection of personal data and control processing body” is under the process of development.	

2.6 Somalia

Data Protection Laws	Enforcement Agency
Somali Data Protection Act⁸: The Somali Data Protection Law (DPL) 2023 was approved by Somalia’s cabinet on 9th February 2023, passed by both Houses of Somali Federal Parliament and signed into law by the President of the Federal Republic of Somalia on 20th March 2023. However, the majority of the operational guidelines of the Act are yet to be developed.⁹ Regulations & Guidelines + DPA Somalia implementation Regulations + Data Protection Authority Guidelines	The Somali Data Protection Authority is governed by a board where 3 of the members are appointed by the Minister of Communications and Technology and the board members appoints a chairperson from among themselves.

⁷ Legislative Decree No. 100/153 of June 17, 2013 on the Regulation of the Control and Taxation System for International Telephone Communications entering Burundi; Decree-Law No. 100/112 of April 5, 2012 on the Reorganisation and Operation of the Telecommunications Regulatory and Control Agency 'ARCT'; Ministerial Ordinance No. 730/1056 of November 7, 2007 to protect the privacy of and restrict access to and interception of the contents of communications.

⁸ Law No. 005 of 2023

⁹ International Monetary Fund (IMF) library - Somalia

<https://www.elibrary.imf.org/downloadpdf/journals/002/2023/187/article-A001-en.pdf> pg. 41

+ Alternative Dispute Resolution Procedure	The Somali Data Protection Authority was launched on 28th January 2024.
--	---

2.7 South Sudan

Data Protection Laws	Enforcement Agency
The South Sudan Data Protection Bill, 2020* The draft bill establishes a data protection authority as well committees and councils under the authority. The members of the Board are to be appointed by the President in consultation with the Minister of Information. *This draft bill, developed by Civil Society Organisations and Academia, has not yet received approval from the Government of South Sudan.	A Data Protection Authority in South Sudan has not been established; however, the process is currently spearheaded by the National Communications Authority (NCA).

2.8 The Democratic Republic of the Congo (DRC)

Data Protection Laws	Enforcement Agency
There is no specific Act on data protection in DRC but they have several Acts in the field of telecommunication that have captured the protection of personal data. For example, Ordinance-law No. 23/010 of 13 March 2023 on the Digital Code has a dedicated chapter on the protection of personal data¹⁰ and the law on telecommunications, information, and communication technology N° 20/017 of 2020. On 2 December 2022 the Council of Ministers adopted a bill authorising the ratification of the Malabo Convention. The status of this bill remains unknown. In addition, a bill on the establishment of a Digital Code was adopted by the Council of Ministers on 14 October 2022. No draft is publicly available yet.¹¹	The DPA has yet to be created by Decree following the adoption of the Ordinance-law No. 23/010.

¹⁰ Available in French: <https://www.numerique.gouv.cd/code-numerique>

¹¹ https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/function_s/handbook.pdf?country-I=CD, accessed on 20th January 2024

Data Protection Laws	Enforcement Agency
Sector specific laws. + Law No. 013/2002 of 16 October 2002 on the telecommunications sector. + Law 10/002 of 20 August 2010 establishing the Customs Code. + Decree-Law 011/46 of 24 November 2011 regarding the application measures of the Customs Code.	

2.9 EAC Legal Framework for Cyber Laws 2008

The EAC Legal Framework for Cyber Laws 2008 is a framework of recommendations for cyber laws and regulations in the EAC. It was prepared by the EAC Task Force on Cyber laws, comprising representatives from the partner states and the EAC Secretariat, with the support of UNCTAD. The framework contains a series of recommendations made to the governments of the partner states about reforming national laws to facilitate electronic commerce and protect individual's privacy and online consumers. It was designed to harmonise the law reform process between the EAC Partner States, as well as reflect on international best practices in the field of cybersecurity.

The draft legal framework was developed in two phases. Phase I encompassed cybersecurity reforms in the areas of electronic transactions, electronic signature and authentication, data protection and privacy, consumer protection and computer crime. Phase II covers intellectual property rights, competition, taxation and information security. The recommendations made under Phase I were to be discussed at national consultative meetings while those in phase II, were designed to harmonise the law reform process between the EAC Partner States as well as reflect international best practices.

The task force provided recommendations specific to data protection and privacy. The task force recommended that further work needs to be carried out on data protection and privacy, paying attention to the privacy of citizens in the use of the Internet, formulation of legislation, the institutional implications of the reforms that are to be undertaken and international best practices

in the area.¹² These recommendations were intended for consideration at the national consultative meetings. The EAC Secretariat was tasked with monitoring the progress of the implementation of the recommendations among the Partner States.¹³ It is worth to note that the framework, remotely or otherwise, influenced the data protection legislation in Kenya, Uganda and Rwanda which passed their legislation afterwards.¹⁴

Even though the objective of the framework was to harmonise data protection regulations in EAC, it did not provide a model law or a blueprint of a data protection framework for partner states to adopt.¹⁵ Furthermore, the framework is not legally binding on the partner states but recommends for partner states to review and harmonise data protection legislation.¹⁶ The framework can be considered a precursor to the development of data protection laws in various partner states, with the anticipation that it could eventually lead to the harmonisation of these laws. Despite the desire for a unified approach in formulation, this objective was not realised, as each partner state opted to create their models. Since much has evolved since 2008, the framework is considered by many outdated and would now require to be reviewed.

2.10 The Malabo Convention

The [African Union Convention on Cyber Security and Personal Data Protection \(the Malabo Convention\)](#) entered into force on 8th June 2023 after Mauritania became the 15th state to submit its instruments of ratification. Of the East African countries, only Rwanda and DRC¹⁷ have ratified

¹² UNCTAD, "Harmonizing Cyber Laws and Regulations: The experience of the East African Community" UNCTAD/DTL/STICT/2012/4/Corr.1 https://unctad.org/system/files/official-document/dtlstict2012d4_en.pdf. recommendation 19.

¹³ UNCTAD, pg. 7.

¹⁴ Olumide Babalola, 'Data Protection Legal Regime and Data Governance in Africa: An Overview' <https://aercafrica.org/old-website/wp-content/uploads/2022/02/DG003.pdf> pg. 4

¹⁵ EAC, Background Paper for the Second Meeting of the EAC Task Force on Cyber Laws, EAC/TF/2/2008 (Annex I), p. 2; cf. also EAC, Report of the second EAC Regional Task Force Meeting on Cyber Laws, EAC/TF/2/2008, pg. 6.

¹⁶ Boshe, Patricia and Hennemann, Moritz and von Meding, Ricarda, African Data Protection Laws – Current Regulatory Approaches, Policy Initiatives, and the Way Forward (2022). Forthcoming in Global Privacy Law Review 2022, Available at SSRN: <https://ssrn.com/abstract=3947664>

¹⁷ * On April 4, 2023, the DRC Ministry of Digital announced the ratification of Ordinance Law No. 23/008 of March 10, 2023, authorizing the ratification by the DRC of the African Union (AU) Convention on Cybersecurity and the protection of personal data, and Ordinance Law No. 23/010 of March 13 on the Digital Code in the

the Convention.¹⁸ The Malabo Convention is a framework convention which is meant to provide general rules and principles on the broad themes of personal data protection, electronic commerce cybersecurity and cybercrimes. It offers a holistic continent-wide framework to harmonise data protection policies in Africa by catalysing digital rights, mainly data protection, privacy and internet freedom. All AU partner states are mandated to have domestic laws in each of the above policy areas which conform to various standards and principles outlined in the Convention. It mandates every state to establish a data protection framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of data, and to punish any violation of privacy.¹⁹ This framework is to be monitored and enforced by a national data protection authority with administrative independence, and a duty to ensure that the processing of personal data is duly regulated.

The Convention lists the basic minimum conditions that the national data protection laws should have.²⁰ The principles have been adopted in most of the EAC partner states' national data protection laws. The Convention can be seen as an attempt to formulate similar data protection laws on the continent by prescribing minimum standards and not harmonisation. In terms of cross-border data flows, the Malabo Convention obligates data controllers to only transfer personal data to non-member States that have an adequate level of protection of privacy and human rights of data subjects. This requirement does not however apply where the authorisation of the national protection authority is obtained before the transfer of personal data to another country.²¹

2.11 The Common Market Protocol

The [Protocol on the Establishment of the East African Community Common Market \(CMP\)](#) is focused on enhancing regional economic integration by aiming to create a single market, allowing goods, services, labour, and capital to move freely across the partner states. The CMP harmonises

DRC (the Digital Code). See: <https://cio-mag.com/rdc-lassemblee-nationale-ratifie-lordonnance-loi-autorisant-la-ratification-de-la-convention-de-malabo/>

¹⁸ Status of Countries that have ratified the Malabo Convention: [https://au.int/sites/default/files/treaties/29560-sl-
AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf](https://au.int/sites/default/files/treaties/29560-sl-
AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf)

¹⁹ Article 8 of the Malabo Convention.

²⁰ Article 13 of the Malabo Convention.

²¹ Article 14(6) of the Malabo Convention.

various aspects of national laws and places emphasis on the need to ensure the protection of personal data and encourage cross-border investments.²² With cross-border investments and the movement of labour and services comes the need to ensure the protection of personal data. The CMP therefore obliges partner states to align their national laws bringing them in line with international best practices. It is important to note that even though the protocol is binding, it employs soft terms such as “undertake” and does not set a timeline for the harmonisation of policies either. The CMP does not make a direct reference to data protection and privacy laws but it requires partner states to ensure that their national laws guarantee the protection of the citizens of the other partner states while in their territories under the free movement of persons. EAC partner states are therefore mandated to establish national laws that promote free movement of goods, services, and labour. These national laws include data protection and privacy laws.

Despite its emphasis on harmonisation, the CMP primarily concentrates on labour policies and programs, making no explicit references to data protection.²³ Nevertheless, it requires that partner states undertake to “approximate” their national laws²⁴ meaning that partner states should endeavour to “make their national laws similar as to resemble each other” but then prescribe harmonisation of policies and systems for implementation of the Protocol. The protocol consistently leans towards the harmonisation of policies but not national laws.²⁵ Based on this, it appears that the protocol recommends aligning national laws and not necessarily harmonisation. Given the circumstances, partner states must consider the adoption of national data protection laws with minimal variations and embrace the call to eliminate unnecessary data localization requirements. Such requirements can impede economic integration and may not align with the objectives of the CMP.

²² Article 5 (3); Article 3 of the Common Market Protocol.

²³ The AU Data Policy Framework, <https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> pg. 11.

²⁴ Article 47 of the Common Market Protocol.

²⁵ Articles 4, 5, 12, 30, 31, 32, 38, 39 of the Common Market Protocol.

3 LEGAL GAP ANALYSIS

This section presents an analysis of data protection laws within the EAC. Even though there are other differences, the primary focus is on how EAC partner states have approached the definition of personal data, the grounds and conditions that have been specified for the lawful processing of data, data localization, the approaches to cross-border data transfers and opportunities for collaboration in investigations of data breaches among DPAs. The objective of this analysis is to derive actionable short and long-term recommendations that can contribute to the development of a more cohesive and effective data protection framework in the EAC that enhances the protection of individual data privacy and protection and boost inter-regional trade.

3.1 Definition and Classification of Personal Data

The definition and classification of personal data is a critical concern because it determines the compatibility between various mechanisms used to facilitate cross-border data flows. To achieve this, consensus on the classification of personal data is necessary. The Data Protection Acts of the EAC partner states make the distinction between personal data and sensitive personal data. The more recent Acts, i.e. Rwanda, Somalia, Uganda and Tanzania, have broadened the scope of what personal data entails to any information relating to an identifiable natural person including religious and philosophical beliefs, political opinions, financial information, employment history,²⁶ health status and medical records.²⁷ In Tanzania, the scope of sensitive personal data includes membership in a trade union,²⁸ tax returns,²⁹ social security numbers, health status, and medical records. EAC Partner states should expand the scope of sensitive personal data to include financial information, membership to a trade union, tax returns and social security numbers as it affords data subjects a high level of protection and this goes a long way into guaranteeing that a state has adequate protection measures for cross data flows.

3.2 Cross-border Transfer of Data

The table below gives an overview of provisions of cross-border data flows in the EAC.

²⁶ Article 3 of the Personal Data Protection Act of Tanzania.

²⁷ Section 9(1) of Uganda's Data Protection and Privacy Act.

²⁸ Article 3 of the Personal Data Protection Act of Tanzania.

²⁹ This has been captured under the South Sudan Bill*

Table 2: Overview of the cross-border data flow provisions

Dimension	Rwanda	Tanzania	Kenya	Somalia	Uganda
Transfer of personal data	Registration is only for data controllers and data processors. A registration certificate is a pre-requisite to apply for authorisation to transfer personal data to third parties outside Rwanda.	An applicant seeking to transfer personal data outside Tanzania must show proof that the country receiving the personal data has ratified an international agreement providing requirements for the protection of personal data, there is an agreement between the recipient country and Tanzania or a contractual agreement between the person requesting the personal data and the recipient of the personal data who is outside the country.	The data controller or data processor has to submit proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data. For the transfer of sensitive personal data, the data subject needs to give consent and in addition to that appropriate safeguards must be demonstrated to and confirmed by the ODPC.	A data controller can only transfer personal data outside the country where the receiving country or organisation affords an adequate level of protection.³⁰ A non-repetitive transfer is allowed or a transfer that concerns only a limited number of data subjects or where a transfer is necessary for the purposes of compelling legitimate interests pursued by the data controller is permitted on condition that the data controller informs the Authority	Where a data controller or data processor based in Uganda, processes personal data outside Uganda, they need to ensure that the receiving country has adequate protection measures at least equivalent to the protection in Uganda's Data Protection and Privacy Act. Alternatively, a data controller or data processor based in Uganda that processes personal data outside Uganda, needs to ensure that the data subject has consented to the transfer.

³⁰ In Somalia, Adequacy of level of protection is assessed taking into account the existence and terms of any legally binding instrument between the Authority and a relevant public authority in the recipient country; the existence of an effective data protection law in the recipient country; the existence and functioning of an independent, competent data protection or similar supervisory authority with adequate enforcement powers; and international commitments and conventions binding on the jurisdiction of the recipient country and its membership in any multilateral or regional organisations.

Comparative study of the data protection legislation frameworks across the East African Community

Dimension	Rwanda	Tanzania	Kenya	Somalia	Uganda
				of the transfer and informs the data subject of the transfer and on the compelling legitimate interests pursued.	
Data Localisation	All data controllers or the data processors are mandated to store personal data in Rwanda. To store personal data outside Rwanda, the data controller or the data processor must have a valid authorisation certificate.	No provisions on storage of personal data outside the country.	The Data Protection Act provides for data localisation – in particular, it enables the prescription of data localisation based on grounds of strategic interests of the state or protection of revenue. ³¹	No provisions on storage of personal data outside the country.	The laws allow for a conditional flow regime where the transfer of personal data abroad is forbidden unless certain conditions are fulfilled. The data controller or data processor needs to demonstrate that the receiving country has adequate protection measures for transfer or the storage of personal data at least equivalent to the protection in the Data Protection and Privacy Act. Alternatively, a data controller or data processor based in

³¹ Section 50 of the Data Protection Act of Kenya; Regulation 26 of the Data Protection (General) Regulations of Kenya.

Comparative study of the data protection legislation frameworks across the East African Community

Dimension	Rwanda	Tanzania	Kenya	Somalia	Uganda
					Uganda who processes personal data outside Uganda, needs to ensure that the data subject has consented to the transfer.
Necessity	The necessary /exceptional grounds where personal data can be transferred are provided for under Article 48 of the Act.	Even where a country proves that they have adequate personal data protection, the recipient needs to establish necessity. In addition to necessity, the recipient also needs to show there is no reason to assume that the data subject's legitimate interests might be prejudiced by the transfer or the processing in the recipient country.	Need to prove that the transfer is necessary for performance of a contract between the data controller or processor and the data subject or for public interest, for the establishment, exercise or defence of a legal claim, purpose of compelling legitimate interests or to protect the vital interests of the data subject	Where there is absence of adequate protection the processing must be shown to be necessary for the entering into or performance of a contract with the data subject, transfer is necessary for the entering into or performance of a contract made in the interest of the data subject between the data controller and a third party, the transfer would benefit the data subject.	No provisions on necessity
Consent from the data subject	The data subject must give consent even where the third party has adequate safeguards	For a country which does not have adequate level of protection the data subject has consented to the proposed transfer.	The data subject must give consent for the transfer of personal data especially where there is absence of adequate protection.	Where there is absence of adequate protection the data subject must give consent.	Consent is required even where the recipient country has adequate protection measures.

Comparative study of the data protection legislation frameworks across the East African Community

Dimension	Rwanda	Tanzania	Kenya	Somalia	Uganda
Adequacy Measures and Cross border transfer of data mechanisms	The law mandates the supervisory authority to put in place a regulation determining other reasons for sharing or transferring personal data to a third party outside Rwanda.	Where the receiving country has ratified an international agreement providing requirements for the protection of personal data or there is an agreement between Tanzania and the country receiving the personal data it can amount to adequate safeguards.	Appropriate data protection safeguards include where the receiving country or territory has ratified the Malabo Convention, has a reciprocal data protection agreement with Kenya or has a contractual binding corporate rules. In addition, the Data Commissioner may make an adequacy decision based on assessment of essential equivalence of the legislative provisions in a third country.	A recipient can also show that the transfer is subject to a law, binding corporate rules, contractual clauses, code of conduct, certification mechanism or other measure that affords an adequate level of protection.	The PDPO is mandated by the Data Protection and Privacy Regulations to gazette countries that have adequate measures in place for the protection of personal data at least equivalent to the protection in the Act.

The requirements for cross border data transfer in Kenya,³² Rwanda,³³ Tanzania,³⁴ and Somalia³⁵ are almost similar in the sense that before any transfer of personal data outside the jurisdiction of the countries, a data controller or processor must provide proof to the DPA about the appropriate safeguards with respect to the security and protection of the personal data. In Uganda, a data controller or data processor needs to demonstrate to have complied with either of the requirements under Section 19 of the Data Protection and Privacy Act and Regulation 30.³⁶ A data controller or data processor needs to maintain evidence of either the adequacy assessment they conducted or records of consent obtained prior to the transfer of the data. This demonstration can be inspected by the regulator either during an investigation or audit, but is not provided to the regulator prior.

Generally, EAC partner states prohibit the transfer of personal data to a third country unless the receiving country has adequate levels of protection of personal data, the data subject has given explicit consent to the transfer, or the transfer is necessary for the protection of the vital interests of the data subject or of other persons. For example, in Tanzania³⁷ a data controller or data processor who intends to transfer personal data outside the country is required to submit proof that the receiving the personal data has ratified an international agreement providing requirements for the protection of personal data, or, there is an agreement between the United Republic of Tanzania and the country receiving the personal data regarding the protection of personal data, or, there is a contractual agreement between the person requesting the personal data and the recipient of the personal data who is outside the country. This is a very high threshold considering that for example only 15 states in Africa have ratified the Malabo Convention and there are not many conventions governing the transfer of data thus making it challenging for the transfer of personal data outside Tanzania.

³²Section 48 of the Data Protection Act of Kenya; The Draft DP Regulations

(<https://www.odpc.go.ke/regulations/data-protection-general-regulations-2021/>) prescribe the terms that must be contained in any cross-border transfer agreements.

³³ Article 48 of the Data Protection and Privacy Law of Rwanda.

³⁴ Part V of the Personal Data Protection Act.

³⁵ Chapter VI of the Data Protection Act of Somalia; Article 30 of the Data Protection Act of Somalia.

³⁶ Section 19 of the Data Protection and Privacy Act of Uganda; Regulation 30(2) of the Data Protection and Privacy Regulations.

³⁷ Regulation 20 (2) of the Personal Data Protection (Personal Data Collection and Processing) Regulations of Tanzania;

Rwanda on the other hand requires a data controller or processor to share data outside the country where they have obtained authorisation from the supervisory authority after providing proof of appropriate safeguards, the data subject has given consent and is necessary. The consent of the data subjects is necessary except for reasons provided for by the Law.³⁸ In Rwanda, a data controller or the data processor who shares or transfers personal data to a third party outside Rwanda, must enter into a written contract, prescribed by Rwanda's Data Protection Office and Privacy Office that sets out the respective roles and responsibilities of each party to ensure compliance with this Law.³⁹

Tanzania and Rwanda present an example of how the data protection laws in the EAC countries are generally restrictive on allowing transfer of data outside their jurisdictions. This could be attributed to grounds of national security⁴⁰ and the protection of individual rights and as such the laws require personal data to be stored within the countries except where a certificate is obtained from the relevant authorities to store data outside the countries.

Somalia allows binding corporate rules, contractual clauses, codes of conduct, certification mechanism as providing adequate safeguards and is open to any other measure as highlighted under Article 30(1) of the Data Protection Act of Somalia. Kenya on the other hand recognises contractual binding corporate rules as providing adequate protection safeguards. Kenya and Tanzania on the other hand recognise countries that have ratified the Malabo Convention as affording adequate protection safeguards to cross border transfers while Rwanda and Uganda have empowered their data protection authorities to determine whether receiving countries have adequate measures in place for the protection of personal data. It may seem that the simplest route to enhancing cross border data flows is through the Malabo Convention. Since the Convention obligates data controllers to only transfer personal data to non-member States that have adequate level of protection of privacy and human rights of data subjects, most data protection laws see the states that have ratified the Malabo Convention as having adequate protection safeguards.

³⁸ Article 48 of the Data Protection and Privacy Law of Rwanda.

³⁹ Article 49 of the Data Protection and Privacy Law of Rwanda.

⁴⁰ Regulation 21(a) of the Personal Data Protection (Personal Data Collection and Processing) Regulations of Tanzania.

Unfortunately, for the EAC, only Rwanda and DRC are parties to the Convention. Contractual binding corporate rules (BCRs) also seem to be widely accepted as providing adequate safeguards with Somalia and Kenya allowing for them. Other EAC partner states do not explicitly mention BCRs and are silent on them. Having BCRs will ensure that the same high standards of data protection are applied consistently across all entities within the corporate group, regardless of their location. This consistency helps address concerns about potential discrepancies in data protection practices in different jurisdictions and at the same time offer enforceable commitments to protect the privacy and rights of individuals as they are enforceable.

3.3 Lawful Processing of Personal Data

Generally, there are no major differences on the provisions on lawful collection and processing of data in the data protection laws of the EAC partner states. The EAC partner states, Kenya,⁴¹ Uganda,⁴² Tanzania,⁴³ Rwanda⁴⁴ and Somalia⁴⁵ require a data controller or data processor to inform the data subject of their rights, the fact that personal data is being collected and the purpose for which the personal data is being collected. The uniformity in the approaches taken by various partner states in handling the lawful processing of personal data presents a valuable opportunity for interoperability. Under the different laws, partner states mandate data controllers who hold personal data that was collected in connection with a particular purpose to use that personal data for other purposes only if the data subject authorises the use of the personal data for that other purpose, the purpose is lawful and the personal data is used in a form in which the data subject is not identified etc.

The ground of legitimate interests has been referred to as one of the lawful grounds for processing personal data in the laws of most, if not all of the EAC Partner states.⁴⁶ For the processing of data, the circumstances giving rise to legitimate interests pursued by the data controller or data processor have not been well defined in most of the data protection laws. For example, in Kenya,⁴⁷ a data controller or data processor has to provide evidence for the need to continue processing

⁴¹ Section 30(1)(iv) and (vi) of the Data Protection Act of Kenya.

⁴² Section 12 of the Data Protection and Privacy Act of Uganda.

⁴³ Section 22(2)(a) of the Personal Data Protection Act of Tanzania.

⁴⁴ Article 19 of Personal Data and Privacy Law of Rwanda.

⁴⁵ Article 14 of the Data Protection Act of Somalia.

⁴⁶ Regulation 10 (2)(b), (3) (4) of Uganda's Data Protection and Privacy Regulations

⁴⁷ Section 36 of the Data Protection Act of Kenya.

the data of that individual where a data subject objects to the processing of data.⁴⁸

For this reason, clarity must be provided on what are “compelling legitimate grounds” to avoid broad interpretation and potential abuse. In the absence of jurisprudence further clarifying the interpretation of legitimate interest, we can look to the EU where as a legal requirement under the GDPR, if legitimate interest is used as a legal basis for processing, an organisation must perform a balancing test: Is this processing activity necessary for the organisation to function? Does the processing activity outweigh any risks to a data subject’s rights and freedoms? If the answer to either of those questions is “no,” then the organisation cannot use legitimate interest as its legal basis for processing.⁴⁹ The GDPR and relevant case law from the Court of Justice of the European Union (CJEU) provide examples of legitimate interests, even though there is no exhaustive list that highlights what legitimate interest entails.⁵⁰

To address potential misuse of data, the EAC should provide clear guidelines on "compelling legitimate grounds," drawing inspiration from the EU. The EAC partner states could implement a balancing test similar to the EU, requiring organisations to assess the necessity of data processing for their functioning and weigh benefits against potential risks to data subjects’ rights. Crafting distinct privacy notices for each market becomes challenging, risking inconsistencies and non-compliance. A recommended solution for the EAC partner states is to explore harmonisation measures, creating a unified framework or template for privacy notices. This approach would streamline compliance efforts, offering businesses operating in multiple markets within the EAC a more efficient and consistent approach to data protection practices.

3.4 Investigations

The data protection authorities of the EAC partner states are mandated to investigate complaints where there has been an infringement of personal data. This could be a collaborating point for the data protection authorities to cooperate with each other on investigations, how to handle

⁴⁸ Regulation 8 (7) of the Data Protection (General) Regulations, 2021; Analysis of Kenya’s Data Protection Act by Privacy International, 2020, Available at: https://privacyinternational.org/sites/default/files/2020-02/Analysis%20of%20Kenya%20Data%20Protection%20Act%2C%202019_Jan2020.pdf pg. 10.

⁴⁹ GDPR fundamentals: Legal Basis for Processing Data by Mark Hinely August 2018: <https://kirkpatrickprice.com/video/gdpr-fundamentals-legal-basis-for-processing/>

⁵⁰ Process personal data lawfully by the European Data Protection Board: https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en

investigations and borrow best practices. There are several shortcomings to this, one is that the nature of some of the investigations have been made to be confidential. There is also an oath of secrecy attached to those undertaking the investigations of complaints. Nonetheless, the data protection laws in the EAC encourage cooperation for the purpose of gathering and exchange of information for any investigations and with regards to any information necessary to assist the data protection authorities in investigations.⁵¹ Cooperation on investigation would enable DPAs to collaborate on new approaches to investigations of data breaches and could save DPAs a lot of time and resources.

⁵¹ Regulation 44 of the Data Protection and Privacy Regulations of Uganda, 2021

4 BEST PRACTICES FROM OTHER REGIONAL BODIES

In regions where laws regarding data protection vary significantly due to differing levels of development, it can be argued that harmonization could pose a considerable challenge. Therefore, it is valuable to examine best practices from other regions that have navigated similar disparities in legal maturity, providing insights for effective harmonization efforts. The case studies below depict scenarios where regional bodies adopted different approaches to having a unified common data protection law. The divergence in national data protection laws and the varying developmental stages of partner states played a pivotal role in shaping their collaborative intentions.

The GDPR exemplifies a comprehensive unification of laws across EU partner states. Conversely, the ASEAN countries maintained their individual data protection laws while fostering interoperability through the adoption of adequate safeguards to facilitate cross-border data flows. In the EAC, there are several regulatory frameworks in place; the Malabo Convention prescribing minimum standards, the EAC Cyberlaws framework focusing on harmonisation and the EAC Common Market urging alignment of laws within the region. Given these considerations, the question arises: what approach would be prudent for the EAC? This introduction sets the stage for a segment titled "Best Practices from Other Regional Bodies," inviting exploration into effective strategies employed by different regions in addressing data protection challenges.

4.1 The European Union General Data Protection Regulations (GDPR)

The EU implemented the [GDPR](#)⁵² which is a data protection regulation designed to protect the personal data of individuals in the EU and to regulate how organisations handle and process data. The main goals of the GDPR are to give individuals more control over personal data, simplify and harmonise data protection regulations across the EU partner states, and enhance the accountability and transparency of organisations in regard to data protection.⁵³ The EU adopted a “one-stop shop” approach to the enforcement of its data protection legislation that focused on streamlining cooperation between the data protection authorities. The GDPR was adopted in 2016, providing

⁵² The GDPR stands for the General Data Protection Regulation and enter into application on 25th May 2018.

⁵³ The General Data Protection Regulation, [GDPR](#)

a single set of rules for data protection to all EU partner states that already shared a common basis for data protection under the former EU Directive 95/46.

The GDPR includes a limited number of provisions that empower partner states to extend beyond the GDPR's rules for specific situations. The EU partner states have established their own national data protection authorities, tasked with safeguarding personal data. The European Data Protection Board (EDPB) facilitates their effective operation by ensuring cooperation and the consistent application of the GDPR across the EU. These national data protection authorities have the responsibility of enforcing the GDPR within their respective countries. When dealing with complaints that extend beyond national borders, they work together through the one-stop-shop mechanism. The EDPB can make binding decisions on cross-border cases on which no consensus is reached between the national data protection authorities.⁵⁴

The EU opted for a common approach to regulations on data protection⁵⁵ through unifying the national data protection regulations and the adoption of a unified regulatory framework. The data protection laws in the EAC on the other hand do not vary much compared to the European laws before 2018 since they have all been enacted between 2019 and 2023 and are heavily inspired by the GDPR. Even though the one-stop shop approach is seen as feasible, it could lead to a lengthy reform process of the existing positive laws or the lowering of the existing levels of protection set by the national data protection laws leading to "lower" "common" standards. The coordination between national data protection authorities and the EDPB in investigations, capacity building, training and coordination is one of the positive aspects that the EAC can borrow from the EU model as well as desire to ensure consistency in national laws.

Under the GDPR, cross border data transfers to countries within the European Economic Area (EEA) is allowed without any specific safeguards as the countries are bound by the GDPR. For cross border transfers to countries outside the EEA, the GDPR requires that specific mechanisms be in place to allow for safe data flows.⁵⁶ These mechanisms can be in the form of Adequacy

⁵⁴ The European Data Protection Board; https://edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/gdpr-cooperation-and-enforcement_en

⁵⁵ European Parliamentary Research Service, How the General Data Protection Regulation changes the rules for scientific research, pg. 1

⁵⁶ Tehrani, P M., Sabaruddin, J S B H., & Ramanathan, D A (2018). Cross border data transfer: Complexity of adequate protection and its exceptions. *Computer law & security review*, 34(3), 582-594.

Decisions, Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), and more.⁵⁷ The EAC has not recognised Standard Contractual Clauses (SCCs) but the Kenyan law has covered SCCs in the provisions of the Act and regulations which looks at organisational and technical safeguards where transfer of data is concerned. Further, the Kenyan regulations provide for agreements as an appropriate safeguard. Kenya and Somalia have recognised Binding Corporate Rules (BCRs) as adequate safeguards. Perhaps further research on whether SCCs would better serve the EAC to promote cross border data flows need to be done.

4.2 Association of South-East Asian Nations (ASEAN)

The [ASEAN](#) region is composed of 10 members in the South East with the aim of accelerating economic growth and development in the region through joint endeavours for a prosperous and peaceful community of Southeast Asian Nations.⁵⁸ The [ASEAN Economic Community \(AEC\)](#)⁵⁹ has a harmonised e-commerce framework which includes among its targets, the adoption of best practice on data protection. In the ASEAN region there are a number of multilateral arrangements ensuring that govern data protection, privacy as well as cross border data flow.⁶⁰ [The ASEAN Framework on Personal Data Protection](#) indicates a set of principles to guide the implementation of data protection measures at both national and regional levels.⁶¹ It constitutes the intention of partner states to cooperate with and implement in their domestic laws and regulations the principles of personal data protection and does not create any legally binding and enforceable

⁵⁷ Voss W, "Cross-Border Data Flows, the GDPR, and Data Governance" (2020). 29 Wash. Int'l L.J. 485. Available at SSRN: <https://ssrn.com/abstract=3629348>

⁵⁸ The ASEAN Inter-Parliamentary Assembly (AIPA) is not the Parliament of ASEAN, but is a body that seeks to ensure close collaboration between the parliaments of the ASEAN member states. It neither has legislative powers and its resolutions are non-binding.

⁵⁹ ASEAN news (2018). ASEAN 4.0:What does it mean for regional economic integrations? Available at: <https://www.thailand-businessnews.com/asean/70455-asean-4-0-what-does-it-mean-for-regionaleconomic-integration.html>.

⁶⁰ The frameworks includes the [ASEAN Framework on Personal Data Protection \(2016\)](#), the [ASEAN Framework on Digital Data Governance \(2018\)](#), [ASEAN Model Contractual Clauses for Cross Border Data Flows \(2021\)](#) and the [Implementing Guidelines for ASEAN Data Management Framework and Cross Border Data Flows \(2021\)](#).; UNDP, 'Enabling Cross Border Data Flow: ASEAN and Beyond Report' 2021. Accessed here: <https://www.undp.org/sites/g/files/zskgke326/files/2021-10/enabling-cross-border-data-flow-asean-and-beyond-report.pdf>

⁶¹ https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf pg. 13

obligations.

The framework recognises the different levels of development of the partner states and therefore allows a member state to delay the application of the framework until such time that it is ready to implement it by informing the other participants in writing.⁶²

The ASEAN system is akin to that of the EAC, where there are some partner states with no specific data protection laws, others with data protection provisions in telecommunication laws and partner states at different levels of implementation. ASEAN chose not to go the harmonisation route (unified data protection laws) but prescribed non-binding guidelines on data management and cross-border data flows for partner states. They chose this model because of the difference in legal systems. Some of the partner states adopted a common law system, other civil law systems and others with hybrid civil and common law countries. In 2021, the partner states adopted the [Implementing Guidelines for ASEAN Data Management Framework and Cross Border Data Flows \(2021\)](#) (ASEAN DMF and ASEAN CBDF) to enable harmonised standards for data management and cross-border data flows within ASEAN. The ASEAN DMF and ASEAN CBDF Mechanisms are non-binding on ASEAN Member States and organisations and do not create additional rights or obligations for ASEAN Member States. The ASEAN DMF is a guide for businesses, particularly Small and Medium Enterprises (SMEs), to put in place a data management system, which includes data governance structures and safeguards based on data sets' purpose throughout its lifecycle.⁶³

While convergence is a positive goal, harmonisation may not be necessary or desired as it could lead to lengthy reform of existing positive law or a lowering of the existing level of protection for a "lower common" standard. Adopting a framework that encapsulates the mutual intention of EAC partner states to collaborate and integrate agreed-upon principles of personal data protection into their domestic laws and regulations without imposing legally binding and enforceable obligations could be a more feasible option. This approach may be favourable because it allows for a faster and smoother adoption without encountering the potential legal and lengthy

⁶² Paragraph 7 of the Implementing Guidelines for ASEAN Data Management Framework and Cross Border Data Flows (2021)

⁶³ Paragraph 4 of the Implementing Guidelines for ASEAN Data Management Framework and Cross Border Data Flows (2021)

complexities of having a binding instrument. The EAC partner states could consider establishing guidelines or a framework that captures the intention of EAC partner states to cooperate with and implement their domestic laws and regulations.

From the ASEAN model, the EAC can also lobby for the incorporation of Binding Corporate Rules (BCRs) when transferring any personal data between enterprises or groups among others. Model Contractual Clauses creating template contractual terms and conditions that may be included in the binding legal agreements between businesses transferring personal data to each other across borders could be another option that can be adopted in promoting cross-border data flows. This could help reduce the negotiation and compliance costs and time, especially for SMEs while ensuring personal data protection when data is transferred across borders.

5 RECOMMENDATIONS

This section proposes recommendations from the study above based on desktop research and the discussions that were held during the first workshop. These recommendations serve as a foundational framework for further exploration and refinement through extensive research and multi-stakeholder engagement. The suggestions provided are not definitive solutions but rather starting points for deeper investigation and inclusive dialogue among DPAs and stakeholders.

5.1 Preliminary Recommendations for Short-Term Measures

Recommendation 1: Support DPAs to accelerate the pace at which Data Protection Laws, regulations and policies are being operationalised.

The EAC partner states are at varying levels of implementation of their data protection laws with some partner states still in the early developmental stages. Operationalising data protection and privacy laws ensures that personal data is safeguarded and fosters trust among data subjects and businesses. It also mitigates risks associated with data breaches and facilitates cooperation, ultimately contributing to economic growth and empowering individuals with control over their data. The EAC partner states can develop regulations, guidance notes, awareness and communication strategies, carry out multistakeholder dialogues on specific topics/sectors, increase capacity and develop guidelines on investigations, design and install computer systems to ease processes like registration among others. This presents an opportunity for EAC partner states with established DPAs to support the other DPAs.

Recommendation 2: Support Partner States to Ratify the Malabo Convention (The AU Convention on Cyber Security and Personal Data Protection)

The Malabo Convention mandates the AU partner states to have domestic laws in data protection which conform to various standards and principles outlined in the Convention. Of the EAC partner states, only Rwanda and DRC have ratified the Malabo Convention. Before ratifying the Malabo Convention, partner states need to embark on a thorough review and analysis of the Convention's provisions to understand its implications and alignment with existing laws and policies, engage in consultation and engagement with various stakeholders as well as assess their domestic legislation related to cybersecurity, data protection, and electronic transactions to identify any gaps or conflicts. Under the Malabo Convention, all AU partner states are mandated to have domestic laws in each of the above policy areas which conform to various standards and principles outlined in the Convention. It is therefore important to have the countries with no data protection laws tailor the bills in accordance with the Convention. As highlighted in the cross-border section,

states that have ratified the Convention are deemed to have adequate safeguard standards. EAC partner states can ratify the convention and recognise each other as having adequate standards for the purposes of cross-border flow of data.

Recommendation 3: Capacity Building and Training of DPAs on Handling Data Breaches.

To supplement the efforts being undertaken by the national DPAs in handling data breaches, there is a need for capacity building to ensure swift containment and preservation of data subjects' privacy rights. Strengthening the capacity of data protection authorities will equip them to adeptly address widespread breaches of protection and privacy laws, effective response, preserve privacy rights, contain breaches, and mitigate risks, enhancing the trust of DPAs to ensure compliance and promote a data protection culture.

Recommendation 4: Adoption of the Alternative Dispute Resolution (ADR) framework to hasten resolution of complaints instituted at the DPAs.

Other DPAs may look into adopting Alternative Dispute Resolution mechanisms such as meditation, negotiation and even arbitration to ensure quick settlement of complaints that have been lodged to the DPAs. The Kenya and Somalia DPA⁶⁴ have adopted the ADR adopting the policy framework. The ADR policy framework serves as a guide on processes to settle data protection disputes through the means of alternative dispute resolution mechanisms. In particular, the guidelines state that they aim to improve on the provisions of the Data Protection Complaint Handling Procedure and Enforcement Regulations. The guidelines aim to give parties an opportunity for amicable resolution of data protection disputes through conciliation, mediation, and negotiation and provide the structures, processes, and safeguards to support ADR. The ADR guidelines have significantly reduced and eased the number of complaints that are investigated and resolved by the DPAs thus saving the DPAs valuable time. Other DPAs can develop guidelines that facilitate ADR mechanisms in resolution of data handling breached disputes.

Recommendation 5: Definition of Common Terms

The EAC partner states have no unified definition of common terms, for example, what personal data entails. There needs to be a common definition of terms to improve the convergence of the different legislation and the potential unification or harmonisation of laws. Through stakeholder

⁶⁴ Somalia ADR <https://www.dpa.gov.so/assets/legal/procedures/ADR%20PROCEDURE%20.pdf>

engagement and collaboration, DPAs can undertake various activities to facilitate the alignment of a common understanding of these terms. This will entail conducting stakeholder consultations, fostering exchanges DPAs, reaching agreements on common principles and establishing consensus on shared definitions. Once these common understandings are established, efforts can be made to transpose them into the respective laws of each member state, thereby promoting coherence and consistency in the region's data protection framework.

Recommendation 6: Increasing Awareness for the General Public on Data Protection and Privacy Laws

Given that the majority of DPAs are relatively new entities, one of their key priorities includes enhancing awareness of privacy and data protection. Increasing awareness of data protection and privacy laws among the general public promotes cross-border data flows by fostering trust and confidence in the data protection laws and authorities. This awareness also presents an opportunity for DPAs to collaborate, as it encourages dialogue, facilitates compliance, and empowers individuals to exercise their data rights.

5.2 Preliminary Recommendations for Long-Term Measures

The long-term recommendations are also based on desktop research and the discussions during the first workshop. They serve as a foundational framework for further exploration and refinement through multi-stakeholder engagement and extensive research. The recommendations include the development of common guidelines for assessing data protection adequacy, the formation of a dedicated working group, the strengthening of penalties and regulatory mechanisms and the convergence of data protection laws. Through collaborative efforts and strategic initiatives, these recommendations aim to create a cohesive and resilient data protection framework that supports cross-border data flows and safeguard individuals' privacy rights. The recommendations are considered long-term due to the complexity of their implementation and the sustained effort required to achieve meaningful outcomes. These efforts include the need for extensive consultations, stakeholder engagement, potential revisions to existing laws and policies, resource allocation and policy alignment meaning that this initiative is likely to take several years to implement fully. As a further consideration, research should be conducted on the effects of the AfCFTA digital protocol on the long-term measures that have been proposed.

Recommendation 7: Development of Common Guidelines on Assessing adequacy Levels of Personal Data Protection that can be adopted by the EAC

East African countries can recognise the laws of each member state as having adequate protection measures for cross-border transfers of personal data. Developing a common and consistent criterion for assessing adequacy levels of personal data protection within the EAC is crucial to facilitating smooth cross-border transfers. This standardised approach ensures a unified understanding and application of data protection standards across partner states. With harmonised criteria, businesses and individuals can navigate cross-border data transfers with confidence, knowing that a consistent level of protection is maintained. This not only promotes trust in the digital ecosystem but also simplifies compliance for organisations operating in multiple EAC countries.

A shared framework for assessing adequacy levels streamlines regulatory processes, fostering a more efficient and interconnected regional data landscape. Some of the proposed guidelines that could be adopted are Model Contractual Clauses or Binding Corporate Rules that will in effect boost trade and movement of people and labour. This will make it easier for businesses to comply with and transfer data without restrictions, given that partner states have different requirements in restricting cross-border data flows. This will create a greater opportunity for the growth of trade and investment across the region. These adequate safeguard measures could be developed by the EAC in association with the East Africa Business Council. In having a standard approach, the level of protection offered should not lower the level of protection set by another EAC partner state.

Recommendation 8: Formation of a Working Group on Data Protection

The formation of a working group that would handle work relating to the implementation of legislation and policies on the protection of personal data, alignment of national data protection laws, identifying priority areas where resources are needed and advising EAC policymakers on regional strategies and capacity building is a welcomed idea. The working group would consult with all stakeholders and draw on expertise from an EAC regional-wide base and Ministries and DPAs at the national level, institutions, businesses, representatives from academia, the technical community, and civil society. The working group could also look into inconsistencies in sectoral laws that are different in the EAC partner states and contain conflicting requirements and uncertainty in crucial fields such as finance.

Recommendation 9: Strengthening Penalties and the Regulatory Framework

Generally, all countries should strengthen the penalties for violations of the data protection laws. The current penalties for violating the law are relatively weak. This means that data processors and

data controllers have little incentive to comply with the law. The government should increase the penalties for violating the law so that any legal persons handling personal data are more likely to take their data protection obligations seriously. The EAC partner states data protection laws do not cover all the questions arising from the emergence of new technologies such as artificial intelligence.

Recommendation 10: Convergence and Unification of Data Protection Laws in the EAC

Having a common set of data protection regulations across the EAC would be a strong incentive for organisations to drive operational efficiencies and to offer uniform services and products across the EAC single market. The promise of convergence of data protection laws would also bring legal certainty for individuals in the EAC, who are increasingly mobile and participating in cross-border transactions. The unification of data protection laws should be undertaken in such a way that it does not lower the level of protection set or required in any of the EAC partner states.

Recommendation 11: Translation of Data Protection Laws into Swahili and Local Languages

Translating data protection laws and regulations ensures that data protection laws are more accessible and improves clarity and understanding of the laws. This ensures legal compliance across borders and fosters trust and confidence in the digital ecosystem. This is essential for fostering a more inclusive and comprehensible legal framework and by doing so, governments can ensure that a broader segment of the population, particularly those who primarily speak Swahili and various local languages, can easily access, and understand the intricacies of data privacy regulations. This move not only enhances legal compliance but also empowers individuals by providing them with the knowledge to navigate and assert their rights regarding the protection of their personal information. The accessibility of information in native languages contributes to a more informed citizenry, fostering a culture of data privacy awareness and accountability. Moreover, such an approach demonstrates cultural sensitivity, recognizing and respecting the linguistic diversity within the region, thereby promoting a more equitable and just implementation of data protection measures.

6 BIBLIOGRAPHY

Journal Articles

- 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>
- 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.
- 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).
- Drysdale, P. ‘ASEAN: The Experiment in Open Regionalism that Succeeded,’ Available at https://www.eria.org/5.1.ASEAN_50_Vol_5
- Corrales C, Marcelo & Aboy, Mateo and Minssen, Timo, ‘Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)’ (2021). Available at SSRN: <https://ssrn.com/abstract=3951085> or <http://dx.doi.org/10.2139/ssrn.395108>
- Voss W, “Cross-Border Data Flows, the GDPR, and Data Governance” (2020). 29 *Wash. Int'l L.J.* 485. Available at SSRN: <https://ssrn.com/abstract=3629348>
- Wolff J & Atallah N, “Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020” (2020). *TPRC48: The 48th Research Conference on Communication, Information and Internet Policy*, 11, 63-103, 2021. Available at SSRN: <http://dx.doi.org/10.2139/ssrn.3748837>
- Ademuyiwa I & Adedeji A. “Assessing Data Protection and Privacy in Africa.” *Assessing Digitalization and Data Governance Issues in Africa*, Centre for International Governance Innovation, 2020, pp. 4–6. JSTOR, <http://www.jstor.org/stable/resrep25330.7>.
- Dove, E S, “The EU general data protection regulation: implications for international scientific research in the digital era.” *Journal of Law, Medicine & Ethics*, (2018). 46(4), 1013-1030.
- Tehrani, P M., Sabaruddin, J S B H., & Ramanathan, D A (2018). Cross border data transfer: Complexity of adequate protection and its exceptions. *Computer law & security review*, 34(3), 582-594.

Working Group Reports

- Implementing Guidelines for ASEAN Data Management Framework and Cross Border Data Flows (2021) <https://asean.org/wp-content/uploads/2021/08/Implementing-Guidelines-for-ASEAN-Data-Management-Framework-and-Cross-Border-Data-Flows.pdf>
- UNDP, ‘Enabling Cross Border Data Flow: ASEAN and Beyond Report’ 2021 <https://www.undp.org/sites/g/files/zskgke326/files/2021-10/enabling-cross-border-data-flow-asean-and-beyond-report.pdf>

Websites

- Analysis of Kenya’s Data Protection Act by Privacy International, 2020, Available at: https://privacyinternational.org/sites/default/files/2020-02/Analysis%20of%20Kenya%20Data%20Protection%20Act%2C%202019_Jan2020.pdf pg. 10

The Paradox of Control: Can Mandatory Registration Really Ensure Data Protection?’ African Academic Network on Internet Policy by Dorcas Tsebee, 2023. Available at: <https://aanoip.org/the-paradox-of-control-can-mandatory-registration-really-ensure-data-protection/>

The African Union’s Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond? by Yohannes Eneyew Ayalew, 15 June 2023.

<https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/>

GDPR fundamentals: Legal Basis for Processing Data by Mark Hinely, August 2018. Available at: <https://kirkpatrickprice.com/video/gdpr-fundamentals-legal-basis-for-processing/>

ASEAN news . ASEAN 4.0:What does it mean for regional economic integrations? (2018) Available at: <https://www.thailand-businessnews.com/asean/70455-asean-4-0-what-does-it-mean-for-regionaleconomic-integration.html>.

Personal Data Protection Commission of Singapore, ‘ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows’ January 2021

<https://www.pdpc.gov.sg/Help-and-Resources/2021/01/ASEAN-Data-Management-Framework-and-Model-Contractual-Clauses-on-Cross-Border-Data-Flows>

The African Union’s Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond? by Yohannes Eneyew Ayalew, 15 June 2023.

<https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/>

Examining Cross-Border Data Flows Provisions in Africa’s Free Trade Agreements,
<https://insights.advocates.ke/examining-cross-border-data-flows-provisions-in-africas-free-trade-agreements/>



Strathmore
UNIVERSITY