AN ASSESSMENT OF INDEPENDENCE OF DATA PROTECTION AUTHORITIES IN EAST AFRICA: A COMPARATIVE STUDY OF KENYA AND TANZANIA

DIOGENESS DIOCLES MGANYIZI

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR AWARD OF THE DEGREE OF MASTER OF LAWS IN INFORMATION AND COMMUNICATION TECHNOLOGY LAW OF THE OPEN UNIVERSITY OF TANZANIA

2024

Certification

I, Prof. Dr. Alex B. Makulilo the undersigned, do certify that, I have read and hereby recommend for acceptance by the Open University of Tanzania, a dissertation titled, *An Assessment of Independence of Data Protection Authorities in East Africa: A Comparative Study of Kenya and Tanzania* in partial fulfillment of the compulsory requirement for award of the degree of Master of Laws in Information and Communication Technology Law of the Open University of Tanzania.

……

Signature

…….……

Date

Copyright

Declaration

I, Diogeness D. Mganyizi, declare that the work presented in this dissertation is original. It has never been presented at any other university or institution. Where other peoples' works have been used, references have been provided, and in some cases, quotations made. It is in this regard I declare this work as originally mine. It ishereby presented in partial fulfillment of the requirements of the award of Master of Laws in Information and Communication Technology Law.

…….

Signature

……

Date

Dedication

I dedicate this dissertation to my daughter, Clarah Kelvin January and that this work should awake and inspire her to fetch for education indefinitely. She should change accordingly with technological developments in this fast growing digital era.

Acknowledgement

All honor and adoration are presented to Alpha and Omega for being with me from the beginning to this end. I would not have made it without His grace and strength. My sincere gratitude goes to my supervisor, Prof. Dr. Alex B. Makulilo for his patient and insightful comments. I am also grateful to the community of the Open University of Tanzania and the entire staff for their unwavering support. I am deeply indebted to my friend Mr. Wilson for his appreciated comments and encouragements he made during this work.

To my parents, my daughter, my sisters, brothers and nephews, I would like to thank you for your prayers, calls, text and mails. I am very lucky to have you all. My fondest appreciation goes to my co-worker Mr. Evody Marcus for his support during the whole writing of this work. My Special thanks to Prof. Dr. Alex B. Makulilo, andother staffs their enriched lectures and mentorship. To my classmate in the LLM- ICTLAW programme, the time we had together will always be fondly remembered. It was blissful to have developed friendship with extra-ordinary people with varied age, ethnic, tribe, religion, experience and attitude like you guys!

In his eternal life, God bless you all!!

Abstract

This dissertation investigates the question of independence of data protection authorities in East Africa with particular focus on Kenya and Tanzania. Objectively this study aims at determining the formal independence of Data Protection Authorities in Kenya and Tanzania. The study is guided by three research questions namely, whether the structures of Data Protection Authorities in Kenya and Tanzania guarantee their independence, Whether the procedures for the appointment and removal from office of data protection commissioners in Kenya and Tanzania secure their jobs in order to act independently and whether the DPAs in Kenya and Tanzania have their budgets and resources adequately provided to exercise their independence. Objectively this study aims at determining the formal independence of Data Protection Authorities in Kenya and Tanzania. To accomplish this research investigation, this study engaged two research approaches: doctrinal legal research methodology which analyses law in the form of legislation, case law and international instruments as well as comparative legal research methodology which involves comparative analysis of identified criteria from Kenya and Tanzania. In relative terms, this research overall finds that the Kenyan data protection authority is more independent than the Tanzanian data protection authority.

Abbreviations and Acronyms

AI	Artificial Intelligence
CIPESA	Collaboration on ICT Policy in East and Southern Africa
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
DSM	Dar Es Salaam
EAC	East African Community
ECHR	European Court of Human right
e-Mail	Electronic Mail
EPOCA	Electronic and Postal Communications Act
EU	European Union
FCC	Federal Constitution Court of German
i.e	That is
ICDPPC	Conference of Data Protection and Privacy Commissioners
ICT	Information and Communication Technology
IP	Intellectual Property
IPR	Intellectual Property Right
ISP	Internet Service Provider
LTD	Limited
MP	Member of Parliament
ODPC	Office of the Data Protection Commissioner

OECD	The Organization for Economic Co-operation and Development
PC	Personal Computer
S	Section
TCRA	Tanzania Communication Regulatory Authority
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
URT	United Republic of Tanzania
US	United State
V	Versus
VoIP	Voice over Internet Protocol
www	World Wide Web
P	Page

List of Statutes

1. International and Regional Instruments

African Union Convention on Cyber Security and Personal Data Protection, 2014Coe 108

Universal Declaration for Human Rights, 1948

Europe

General Data Protection Regulations, 2018

2. National Legislation

(a) Tanzania

Banking and Financial Institution Act, 2006

Constitution of the United Republic of Tanzania, 1977

Electronic and Postal Communication Act, 2010

Tanzania Communication Regulatory Authority Act, 2003

Tanzania Personal Data Protection Act, 2022

2. Foreign

Kenya

Kenyan Data Protection Act, 2019

Uganda

Ugandan Data Protection Act, 2021

Rwanda

Rwanda Personal Data Protection Act, 2021

List of Cases

Deogras John Marandu V. Managing Director, Tanzania Beijing Huayuan Security Guard Service CO. LTD 2017High Court of Tanzania (Unreported)

European Court of Human Right (ECHR) - Szabo and Vissy v. Hungary (2016)

Court of Justice of Human Rights (CJEU) – Wirtschaftsakedemic Schleswing – Holstein (2014)

Federal Constitution Court of German (FCC) –BverfG, 1 BvR 16/13 (2018)

Deogratias John Marandu v. Managing Director, Tanzania Beijing Huayuan Security GuardServiceCO.LTD 2017 High Court of Tanzania

Jamii forums V. R (2018)

Table of Contents

CHAPTER ONE

INTRODUCTION AND BACKGROUND TO THE PROBLEM

1.1 Background of the Problem

The evolution of data protection and the breach of privacy came about around the 19th century as the first legislative initiative that occurred in Germany, the first country to adopt the la w of privacy and data protection in 1970, and in Sweden in 1973. Bennet observes that keeping individual data personally involves uncivilized procedures that may put individual data at stake.[1] The importance of privacy also took place during the era of dictatorship in the Roman Empire, where people were identified by the system of census.[2] This system was used because no inmate was supposed to have privacy due to the slogan "Big Brother is watching you.[3] During the era of surveillance and control, data protection and privacy emerged in European countries.[4] The countries in Europe saw the importance of protecting their citizen's data and decided that it should be kept in privacy no matter where a citizen of any member country is. This will be covered and protected by the European legislation known as the General Data Protection Regulation 2014. Also, the US in December 31 1974, enacted and established the Act of fair information practices on Federal agencies collection, maintenance, use, and dissemination of personally identifiable information. Following the mass need to protect data and privacy,

[1] [1]Bennet, C, J Regulating Privacy Data Protection and Public Policy in Europe and the United States Cornell University Press, Ithaca/London 1992 p.18
[2]Roos, A, The law of Data (Privacy) Protection A comparative and theoretical study LLD, Thesis UNISA South African Position South Africa law journal 2007 Vol 124
[3]George Orwell, Big Brother is watching You June 8, 1949 Science fiction and Social Science.
[4] Ibid

African countries followed the European path of data privacy policy.

To date about 36 countries in Africa out of 55 countries have adopted a data protection law and/or regulations.[5] Other sixteen Countries have signed the African Union Convention on Cyber Security and Personal Data Protection adopted on 27 June 2014 (Malabo Convention).[6]

The data protection authorities in East African countries are vested with powers to safeguard the right of privacy of individuals.[7] Whatever little of data protection legal provision there were, they were to be found in varying degrees in a number of sector related legislations. In the case of *Deogras John Marandu v. Managing Director, Tanzania Beijing Huayuan Security Guard Service Co. Ltd* the High Court of Tanzania held that privacy rights are not much well established in Tanzania.[8]

In the East African region, Tanzania took a significant step towards safeguarding personal data by implementing the Personal Data Protection Act in November 2022. This legislation was enacted to uphold the provisions outlined in Article 16 of the Constitution of the United Republic of Tanzania URT 1977, which explicitly guarantees every individual the fundamental right to privacy. Following Tanzania's initiative, other countries in the region such as Kenya, Uganda, Rwanda, and the

[5] Available; www.lexology.com the personal data collection, processing and dispute handling procedures in Tanzania 2023
[6] Ibid
[7] Available at https://www.dataguidance.com Tanzania data protection over view Guidance note
[8] Deogratias John Marandu v. Managing Director ,Tanzania Beijing Huayuan Security GuardServiceCO.LTD[14] 2017High Court of Tanzania (Unreported)

Democratic Republic of Congo (DRC) have likewise introduced comprehensive data protection laws. These legal frameworks aim to establish robust mechanisms for the protection of personal information, in alignment with international standards and best practices. By implementing comprehensive data protection legislation, the countries of East Africa underscore their dedication to fostering a culture of data privacy and guaranteeing the proper handling and safeguarding of individuals' personal information. These proactive measures not only serve to enhance the region's overall data security framework but also signal a clear message to both domestic and international stakeholders regarding the importance placed on upholding the fundamental rights of privacy and confidentiality. Furthermore, the enactment of robust data protection laws enables these nations to align with global standards and best practices, thereby fortifying their position in the increasingly interconnected digital landscape.

1.2 Statement of the Problem

The independence of Data Protection Authorities (DPAs) to any successful implementation of data protection legislation Section 8 (3) of Kenyan Data Protection Act expressly provides that, the Data Commissioner will act independently without the interference from other bodies.[9] The data protection legislation in Tanzania does not specifically address the issue of independence with regards to the Data Commissioner. The presence or absence of explicit provisions within data protection laws regarding the formal independence of the Data Protection Authority (DPA) does not automatically ensure its independence in both a formal capacity and practical implementation. It is imperative to recognize that the mere

[9] Kenyan Data Protection Act 2019 S. (3)

inclusion of language regarding independence in legislation does not inherently safeguard the autonomy and impartiality of the DPA in its operations. The effectiveness and genuine autonomy of the Data Commissioner's office rely not solely on statutory language but also on the broader institutional framework, practical implementation, and the extent to which the DPA can operate autonomously from external influences or interests.[10] The complete legal document must undergo a comprehensive evaluation and analysis in order to ascertain that a Data Protection Authority (DPA) exhibits formal independence. This entails a thorough examination of all relevant sections, clauses, and provisions within the law to ensure that the DPA is truly autonomous and operates with impartiality. Only through a holistic review of the text can a definitive conclusion be drawn regarding the formal independence of the Data Protection Authority as stipulated within the legal framework. Similarly examining the independence of a DPA requires assessment of its operations in practice.

The present study sought to examine the formal independence of DPAs in Kenya and Tanzania. Little is said about the independence of DPAs in practice in the two countries. This is because the data protection legislation practices in both Kenya and Tanzania are less than five years old, which is normally a minimum period for considering the practice of a particular law.

1.3 Objectives of the Study

1.3.1 General Objective of the Study

The main objective of this study is to determine the independence of DPAs in

[10] Kenyan Data Protection Act 2019 S. (3)

Kenya and Tanzania. The study focuses on the three major criteria of assessing independence namely, if the structures of Data Protection Authorities in Kenya and Tanzania guarantee their independence, the procedures for the appointment and removal from office of data protection commissioners in Kenya and Tanzania if secure their jobs in order to act independently and the DPAs in Kenya and Tanzania have their budgets and resources adequately provided to exercise their independence.

1.3.2 Specific Objectives of the Study

The specific objectives of this study are: -

i. To assess the structures of Data Protection Authorities in Kenya and Tanzania if they are guaranteed their independence relation to the question of independence.
ii. To examine the procedures for the appointment and removal from office of data protection commissioners in Kenya and Tanzania secure their jobs in order to act independently.
iii. To examine the provision of Data Protection Authorities in Kenya and Tanzania budgets and resources to adequately provided to exercise their independence.

1.3.3 Research Questions

The present study is guided by three research questions:

i. Whether the structures of DPAs in Kenya and Tanzania guarantee their independence.
ii. Whether the procedures for the appointment and removal from office of data

protection commissioners in Kenya and Tanzania secure their jobs in order to act independently.

iii. Whether the DPAs in Kenya and Tanzania have their budgets and resources adequately provided to exercise their independence.

1.4 Significance of the Study

The Data Protection Authorities (DPAs) independence is essential to safeguarding of personal data. This study will enlighten the reader on the importance of DPAs independence and how it can be strengthened. By assessing whether the DPAs in Kenya and Tanzania are independent, this study will help to go through the composition of the authority, the method of appointment of members, the power, and the time frame for exercising oversight functions. It will also help the reader understand the DPAs independence challenges and any possible ways to overcome them.

1.5 Literature Review

There is scant literature on the subject of the independence of DPAs in Africa generally and in the East African region in particular. This is not surprising for two main reasons. First, data protection laws and policies are a new development in Africa. Because of this, there is still limited research in this area of law. Secondly, Africa still suffers from a lack of academics and experts in the field of data privacy law; as such, this area is still virgin. However, a lot has been written by academics and scholars in Europe and Asia. This literature is relevant to the present study as it illuminates aspects that may be applicable in the African context of what should be considered independence for DPAs.

Greenleaf makes a compelling argument regarding the importance of carefully assessing the formal independence of a Data Protection Authority (DPA) within the framework of international instruments governing data privacy. To comprehensively evaluate the degree of independence of a DPA, it is imperative to consider the guidelines and standards set forth by international bodies in relation to the protection of individual rights, effective judicial enforcement, and the implementation of regulatory measures. By aligning the structural independence of DPAs with these established international principles, it becomes possible to ensure a consistent and robust approach to upholding data privacy standards on a global scale. Consequently, embedding these principles into the operational framework of DPAs can significantly enhance their autonomy and effectiveness in safeguarding personal data and enforcing compliance with data protection regulations.[11] He further identifies 13

[11]Greenleaf. G Independence of Data Privacy Authorities: International Standards and Asia – Pacific Experience Computer law &security Review, Vol 28issues 1&2 2012 rev.2014

factors as elements of independence, including independence guaranteed by legislation, adequate resources, appointment of commissioners for fixed term, and removal only for specified inadequate conduct. The author's arguments are relevant to this study hence his ideas are used in this study.

Schuez provides that DPAs are the key factor in protecting not only individual's personal data but also raising awareness among people about their basic right to privacy.[12] In his study, he analyzes the method of assessing the independence of DPAs in four countries in the European Union (EU). The levels of formal independence of DPAs might vary and should be carefully assessed to ensure that no political pressure is channeled via DPA Commissioners to impact DPA enforcement style. DPAs that are less independent and prone to political and private influence might adopt a laxer approach to enforcement due to external pressures. His focus was mostly on the government partial controls on the DPAs which infringes their privacy therefore he partially discuss on few aspects of assessing DPAs independence living a room for other scholars to dive in deep on the concept of DPAs independence.

The European Union Agency for Fundamental Rights discusses the elements of the DPAs by focusing on the current situation regarding budget, staff and training issues, task allocations, the estimated impact of data protection reform proposals and IT tools. However, their key factor in their report was about the financial status of the DPAs as their main focus which leads to inadequate stuffs and lack of recruitment

[12] Schutz GmbH & co. Data Protection Policy July 2020 https://www.schuetz.net./en/imprint

tools therefore his idea will be added in this study.[13]

Ducuing argues that the independence of DPAs is the cornerstone of data protection legislation. He provides for the principle of complete independence without clarifying the extent of that principle.[14] The author gives credit to the *Wirtschaftsakademic case (C-210/16),* namely the clarification by the CJEU (court of justice of the European Union) of the principle of independence of data protection supervision, but he did not show how independence of DPAs is assessed or how it can affect privacy, as will be discussed in this study.

Sesan argues that the East African laws of data protection and privacy should be revamped in order to meet the current living situation of the countries.[15] Also, the appointments of data protection commissioners should be look upon in order to guarantee their independence and neutrality also DPAs should be more transparent with their decision making hence the promotion of some measures in trust from data subjects. The author's argument is relevant to this study, hence the need to conduct this study.

Widiatedja underscores the importance of the Indonesian government's enactment of the data protection law in 2022. Despite the prolonged duration it took for the legislation to come into effect, its implementation was deemed critical due to the escalating incidents of data protection breaches within the country. This legal framework was long overdue, necessitated by the pressing need to address the

[13] Schutz GmbH & co. Data Protection Policy July 2020 https://www.schuetz.net./en/imprint
[14] Ducuing. C. Institutional aspects of the Wittschaftacademie case: focus on the independence of data protection supervision 2018 available at https://www.law.kuleuven.be
[15] Sesan.G, Olumide. B Data protection at the establishment, independence, Independence impartiality Efficiency of Data Protection Supervisory Authorities in the Two Decades of Their Existence on the continent 2021.

surging cases of data security violations and breaches. The delayed introduction of the law highlighted the urgent requirement for comprehensive measures to safeguard individuals' data privacy and enhance cybersecurity protocols across various sectors in Indonesia.[16] The author argues that, the existence of an independent data protection authority will be crucial in safeguarding the privacy if Indonesia's long term economic and political interests, including getting international recognition for being data destination. The author's argument is relevant to this study, hence the need to conduct this study.

Szydlo the author of this literature argues that, the principle of independence of DPA in the case laws on the side of case laws the author argued that the court of justice was confronted with the commissions in a case of *Commission v. Austria* a supervisory authority DPA within the directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, did not fulfill the requirement of complete independence in exercising functions required to them.[17] He interpreted as meaning that the supervisory authorities responsible for supervising the processing of personal data must enjoy an independence allowing them to perform their duties free from external influence. The author's argument is relevant to this study, hence the need to conduct this study.

Ishabakaki argues from two perspectives that personal or institutional independence entails two things. First, the personnel must be independent. This means that their

[16] Widiatedja. P Establishing an Independent Data Protection Authority in Indonesia: Future – Forward Perspective 2022 https://papers.ssrn.com

[17] Szydlo. Principles underlying independence of national data protection authorities: *Commission* v. *Austria* Marek Szydlo *Common Market Law Review* Volume 50, Issue 6 (2013) pp. 1809 – 1826 https://doi.org/10.54648/cola2013167

manner of appointment or recruitment should ensure that they are independent in discharging their functions. The best practice is for these personnel to be recruited through a competitive recruitment process rather than being appointed by the political authority.[18] Minimally, that ensures their independence in the execution of their duties. In order to ensure this independence is safeguarded, interference of any kind with the functions or powers of the authority is considered an offense. Financial independence refers to the ability of these regulatory bodies to operate autonomously without relying on external financial support. This autonomy is crucial for ensuring that these authorities can carry out their responsibilities effectively and without bias. In order to achieve financial independence, regulatory bodies must establish and maintain sustainable revenue streams that are separate from government funding or other external sources. By doing so, these authorities can uphold their integrity and independence while carrying out their essential functions of oversight and regulation within their respective industries. The author's argument is relevant to this study, hence the need to conduct this study.

Chaput argues that, the independence of data protection authorities is an essential feature of effective data protection shared by all modern data protection regimes around the world.[19] In 143 countries with data privacy laws, only 10 countries do not have an independent DPA that is separate from a government body (see Graham Greenleaf, PL & B IR 2021). Within the Asian region, a few countries stand out in terms of their approach to regulating public sector privacy. Taiwan particularly distinguishes itself by aiming to oversee public sector privacy without the presence

18 Ishabakaki A.B Enforcement Structure and Complaint Mechanisms Victory Arttoys 2022
19 Chaput S. A Independent data protection authority matters The Jakarta Post Jakarta.com

of a dedicated Data Protection Authority, although discussions are underway to potentially establish one. On the other hand, Singapore and Malaysia do have established DPAs, but these entities operate under the purview of the respective government ministries, although they function independently in administrative matters. The relevance of the author's argument underscores the importance of delving into this subject matter through a comprehensive study, further emphasising the crucial need for such research.

Sevilla aimed to capture and cluster different post-GDPR enforcement styles by Data Protection Authorities (DPAs) across the EU to better understand why enforcement over data protection issues varies across borders.[20] In his third hypothesis for variations in DPA enforcement styles investigates the level of independence of any given enforcement agency. According to the enforcement literature, independent, "stand-alone" agencies with weak ties to central government are more aggressive toward the regulated. Many skeptics question whether independence of DPAs is really possible against the backdrop of pressures to maintain a business-friendly environment and foreign investment. Still, the impact of agency-independence on enforcement style remains to be seen. The degrees of formal independence among DPAs can significantly differ and must be meticulously evaluated to safeguard against the possibility of political interference being exerted through DPA Commissioners in order to influence the enforcement style of DPAs. DPAs with lower levels of independence, susceptible to both political and private influences,

[20] Sevila. S. I Trends in Privacy Enforcement: A Comparative Analysis of po**st-**GDPR Enforcement Styles 2021

may choose to adopt a more lenient enforcement stance as a result of external pressures. This susceptibility can compromise the impartiality and effectiveness of DPAs in upholding data protection regulations. Consequently, a thorough examination of the independence of DPAs is imperative to ensure their ability to enforce data protection laws without undue influence, thereby promoting trust and compliance within the regulatory framework. Since the level of independence of DPAs post-GDPR is likely to vary, there is a range in how stringent DPAs are likely to be when enforcing the law (H3). The author's argument is relevant to this study, hence the need to conduct this study.

DPAs are independent authorities entrusted with the consistent application of the GDPR. They are obliged to facilitate the submission of complaints, notably by measures such as a complaint submission form, which can also be completed electronically without excluding other means of communication, in line with Art. 57(2) GDPR.[21] They are tasked with handling lodged complaints, and with investigating, to the extent appropriate, the complaints subject matter. This study delves into the current Data Protection Authority (DPA) practices concerning their duty to facilitate the submission of complaints, with a particular focus on the nexus between this duty and the entitlement to an effective judicial remedy against DPAs. The research methodology adopted for this investigation involves a meticulous blend of legal analysis, scrutinisation of DPA websites, and examination of the insights

[21] Fruster. G and others the Right to Lodge a Data Protection complaint: OK, But then What? an empirical

gleaned from the online public register of rulings made under the 'one-stop-shop' mechanism. It is noteworthy that the General Data Protection Regulation (GDPR) refrains from providing a specific definition of what constitutes a complaint and also falls short of providing detailed elaboration on this matter.

1.6 Research Methodology

The research methodology employed in this study encompasses two distinct approaches: doctrinal legal analysis and a case study methodology. The doctrinal legal analysis method entails a comprehensive examination of the relevant legal framework comprising legislation, judicial precedents, and international agreements pertinent to the subject under investigation. This rigorous approach involves the systematic collection, review, and interpretation of legal texts to elucidate the existing legal principles and norms governing the specific issue at hand. By scrutinizing the statutory provisions, court decisions, and international treaties, this method aims to provide a thorough understanding of the legal landscape shaping the research area. In addition to the doctrinal legal analysis, the study also integrates a comparative study approach to enrich the analysis. Through detailed examination of specific law provision of two countries Kenya and Tanzania and how are related to the research topic, this methodology offers valuable insights into the practical application of legal principles in real-world contexts. By delving into specific instances and exploring the intricate details of individual cases. The comparative study method complements the doctrinal analysis by offering a nuanced perspective on how legal principles are operationalised and interpreted in practice by comparing two countries. By combining these two methodological approaches, the study aimed

to provide a comprehensive and insightful analysis of the legal framework governing the research subject. These are considered primary data in the domain of legal research. However, to understand more about what this law means, the researcher relied on secondary sources such as books, journal articles, research papers, dissertations, and theses. Documentary analysis of available resources is important in this study as they provided an interpretative paradigm in understanding the independence of DPAs. Doctrinal legal research is used in this study since data protection legislation in both Kenya and Tanzania has only recently been brought into force. In Kenya the Data Protection Act was put into force in 2019, while in Tanzania Personal Data Protection Act was put into force in 2022. At present the law has yet to generate sufficient practice worth of being researched. Under the comparative study approach, the study selected two countries. Kenya and Tanzania, in order to undertake an in-depth analysis of data protection laws of each country for a deeper understanding of the question of the independence of DPAs. The two countries data protection laws have only recently been brought into force.

1.7 Data Analysis

Data analysis is the crucial process of meticulously organizing, structuring, and deriving significance from the vast amount of collected data. Within the realm of doctrinal legal research, analysis primarily encompasses the application of legal techniques to interpret statutory provisions effectively. The key legal techniques employed in this context are the literal rule, the golden rule, and rules of logic. These methodologies serve as fundamental tools in extracting meaningful insights from the data under scrutiny in the current study, enabling a comprehensive and

rigorous examination of the legal framework at hand. Through the judicious application of these techniques, the data analysis process can uncover valuable information that facilitates a deeper understanding of the legal principles and implications within the researched domain.

1.8 Limitation of the Study

Any research study is subject to certain restriction during its conduction. This study however faced limitations in terms of time since the topic of research is wide than the available time to conduct the research.[22] The researcher used the limited time to accomplish this work. Also, the researcher is employed therefore her time was limited not only that but also financial constraints repercussion that faced the researcher in his process of doing the study like stationery expenses since this research is unfunded one.[23] To overcome this limitation, the researcher used the available limited fund and donation from parents and colleagues to procure the required services.[24]

1.9 Conclusion

This chapter contains all the necessary components in conducting research study. It offers significant advantages and serves as a valuable resource for researchers by providing guidance on effectively addressing the research problem. It functions as a comprehensive guide, reminding researchers of the most suitable approach to adopt, particularly given the recent enforcement of regulatory frameworks in both Kenya

[22] Fruster. G and others the Right to Lodge a Data Protection complaint: OK, But then What? an empirical p 15
[23] Ibid p.9
[24] Data analysis, Interpretation and Presentation, Available at http://http://www.uio.no/studies

and Tanzania. Efficiently navigating these newly established regulations is paramount, and this chapter aids researchers in understanding the requisite methodologies and strategies essential for successful research conduct within the context of the evolving legal landscape in the two mentioned countries. By adhering to the insights and recommendations delineated in this chapter, researchers can enhance the quality and efficacy of their research endeavors while ensuring compliance with the pertinent regulations in Kenya and Tanzania.

CHAPTER TWO

CONCEPTUAL FRAMEWORK OF INDEPENDENCE DATAPROTECTION AUTHORITIES

2.1 Introduction

This chapter provides a general concept and understanding on the independence of data protection authorities and defines its key terminologies. As eluded to, the independence of a data protection authority is a cornerstone to the successfully functioning of an authority. The rem data refers to individual facts and statistics collected together for reference or analysis while, Data Protection refers to the legal control over access to and use of data stored in electronic devices and physical document. This part is going to consider the concept of independence of DPAs based on legislation, case law as well as literature.[25]

2.2 Independence of DPAs According to International Institutions

In the present-day interconnected and data-centric global landscape, the safeguarding of personal information stands as a critical priority. The escalating concern for the protection of individuals' privacy and the preservation of trust within the virtual environment has led numerous nations to institute DPAs. These autonomous entities serve as fundamental players in the reinforcement of data protection tenets and the execution of pertinent legislations and guidelines. By overseeing compliance, investigating breaches, and providing guidance to both organizations and citizens, these DPAs are instrumental in ensuring the integrity

[25] Supreme Courte of India – Justice K.S Puttaswamy (Retd) v. Union of India (2017);61

and security of personal data in the ever-evolving digital sphere. Theconcept of the independence of data protection authorities is deeply rooted in various international laws and conventions.

The General Data Protection Regulation (GDPR) The General Data Protection Regulation, enacted by the European Union (EU) in 2018, is one of the most influential and comprehensive data protection laws globally.[26] In accordance with the General Data Protection Regulation, Data Protection Authorities are mandated to maintain impartiality and autonomy in their decision-making processes and day-to-day functioning. This pivotal requirement demands that DPAs operate independently, free from external influences, particularly those stemming from political entities or commercial interests. It is imperative that DPAs are equipped with the requisite resources, expertise, and autonomy to effectively address complaints, conduct thorough investigations, and enforce penalties against data controllers and processors found to be in breach of data protection regulations. By upholding these fundamental principles, DPAs can fulfill their vital role in safeguarding individuals' personal data and upholding the integrity of data protection laws within the European Union.

Council of Europe Convention 108, Council of Europe Convention 108, also known as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, emphasizes the independence of DPAs.[27] It emphasizes that DPAs should function autonomously without being subject to any

[26]See the GDPR Article 52 (2-6) recital 171.
[27] Convention 108+ Convention for the protection of individuals with regard to the processing ofpersonal data 1981-2023 https://www.coe.int/dataprotection

instruction, pressure, or influence from any source. This includes the government, private organizations, or any other parties that may have vested interests in compromising data protection rights.

Also, OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data.[28] The Organization for Economic Co-operation and Development (OECD) has issued guidelines that promote the independence of DPAs as an essential aspect of privacy protection. According to these guidelines, DPAs must have the authority to take necessary actions to enforce data protection laws and must not be subject to any conflicts of interest that may undermine their impartiality and effectiveness.

The United Nations, in acknowledging the right to privacy as a fundamental human entitlement, has underlined its significance within the digital era through a dedicated resolution focused on this issue. Specifically, in its resolution on the right to privacy in the digital age, the UN General Assembly emphasised the pivotal role of independent Data Protection Authorities (DPAs) in upholding and promoting this essential right. The Assembly articulated the critical requirement for DPAs to maintain impartiality, receive adequate funding, and operate without undue influence to ensure the effective protection of individuals' privacy rights in an increasingly interconnected world. Through this emphasis on the autonomy and resources of DPAs, the United Nations underscores its commitment to safeguarding the privacy and personal data of individuals against potential threats and

[28] OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data available at https://bja.obja.obja.ojp.gov and https://www.oecd.org 2019

encroachments in the digital landscape.

2.3 The Concept of Independence According to Judicial and Court Decisions

Judicial independence encompasses several key elements that guide court decisions and protect the rule of law, freedom from political interference, security of tenure; judicial officers must enjoy secure tenure to protect them from arbitrary dismissal orretaliation due to their decisions.[29] This security allows judges to make rulings without fear of reprisals, upholding the integrity of the judiciary, financial independence ethical standards, judges are expected to adhere to high ethical standards, including impartiality, integrity, and fairness. Upholding these principles reinforces public trustin the judiciary and strengthens its independence in the digital age. The protection of personal data has emerged as a paramount concern in the modern digital landscape, resonating with both individuals and organizations at large. Within this realm, Data Protection Authorities (DPAs) assume a vital responsibility in upholding the privacy rights of individuals, ensuring adherence to stringent data protection regulations, and overseeing the appropriate management of personal information. DPAs are entrusted with the crucial task of not only enforcing data protection laws but also monitoring and guiding entities to implement robust mechanisms that safeguard the confidentiality and integrity of personal data. Through their regulatory functions, DPAs foster a culture of accountability and transparency, thereby cultivating a secure environment where the rights of data subjects are respected and upheld. The pivotal role played by DPAs underscores the significance of their contribution in cultivating a privacy-centric ethos and fostering

[29] Independence: Definition, Use & Examples https://study.com 2022

trust in the digital ecosystem.[30] A key aspect of their effectiveness lies in their independence from undue influence or interference by external forces. Itmeans that DPAs should be free from political and any other economic influence that could compromise their decision-making processes or hinder them from effectively enforcing data protection laws. An independent DPA can act objectively, without bias or external pressures, ensuring a fair and transparent approach to data privacy matters.

European Court of Human Right (ECHR)-Szabo and Vissy v. Hungary (2016). [31] In this landmark case, the ECHR emphasized the importance of an independent DPA. The Court held that the Hungarian data protection system lacked sufficient guarantees of independence, as the dismissal of the head of the DPA was made without clear legal grounds. The ruling underscored that DPAs should be free from arbitrary removals and political interference to uphold their independence.

Court of Justice of Human Rights (CJEU) – Wirtschaftsakedemic Schleswing – Holstein (2014)[32]

This case revolved around the interpretation of the independence of a German DPAin relation to EU data protection law. The CJEU ruled that the DPA must be genuinely independent, both in law and in practice, from any external authority. This means that DPAs should not only possess legal independence but also demonstrate their ability to act without influence or pressure.

[30] Merriam –Webster.com Dictionary, Merriam Webster https://www.meriamwebster.com /dictionary/independence 2022

[31]European Court of Human Right (ECHR)-Szabo and Vissy v. Hungary (2016)

[32] Court of Justice of Human Rights (CJEU) – WirtschaftsakedemicSchleswing –Holstein (2014)

Federal Constitution Court of German (FCC) –Bverf G, 1 BvR 16/13 (2018) The FCC[33] affirmed the necessity of an independent DPA to protect fundamental rights effectively. It ruled that the independence of German DPAs is a constitutional. Requirement and any legislative measures that undermine their autonomy would be deemed unconstitutional.[34] This case led to the recognition of the right to privacy as a fundamental right under the Indian Constitution. Although it did not directly address the independence of DPAs, it reinforced the importance of data protection and the need for independent regulatory authorities to protect citizens' privacy.

2.4 The Concept of Independence According to Authors

Independence is a fundamental pillar of any democratic system, and it plays a crucial role in upholding the rule of law and ensuring justice. Within the context of literature and authors, different scholars tried to pour their thoughts on how the term independence can be defined.[35]

This study dervishes into the definition of independence as interpreted through landmark authors and literature definition.[36] Independence means freedom from control by external power. It can take many different forms. For example, personal independence means freedom from control by another individual or organization political independence without the interference ofany other external forces.[37]

In contemporary societies, the concept of independence is widely esteemed, perceived as a fundamental principle underpinning individual and collective agency.

---

[33] Federal Constitution Court of German (FCC) –BverfG, 1 BvR 16/13 (2018)
[34] Supreme Courte of India – Justice K.S. Puttaswamy (Retd) v. Union of India (2017):61
[35] Independence: Definition, Use & Examples https://study.com 2022
[36] Ibid p.22
[37] Ibid

However, the realization of this cherished ideal is often obstructed by the pervasive influence of political regimes. While independence is ostensibly upheld as a societal tenet, its actual manifestation frequently falls prey to the intrusive interventions of governing powers. The imposition of political agendas and control mechanisms by authorities invariably compromises the autonomy and self-governance of citizens, thereby diminishing the authentic autonomy that independence should confer. Consequently, the noble aspiration for independence is thwarted by the overbearing presence of political interference, thereby necessitating a critical reexamination of the dynamics between societal values and governmental impositions.[38]

Also, Morris view independence as an assessment of discovering whether someone can do things on her own.[39] It's the way of seeing to what extent a person is able to perform tasks without assistance (independence) and use this as a basis for arranging the measures to help an individual when he or she is unable to do the tasks on her own.[40]

Independence is the central element of statehood in the modern system of political law which is free from political pressures and affairs ensuring the majority sovereignty in performing their duties and daily tasks. Independence is a basic requirement for statehood where a state has exclusive freedom regarding its territory.[41]

Independence means freedom from control by an external power. It can take many

[38] Northway R, what does independency mean? University of South Wales UK August 21, 2015
[39] Morris. J (1993) Independent lives. Community care, macmillanhttps://journals.sagepub.com
[40] Wood, M Independency Encyclopedia Princetoniensis Princeton University 2023
[41]Petrarca. R, Sailus. C Explore the concept of Independency learn the various meaning of independency 2022 https://study.com

different forms. For instance, personal independence means freedom control by another individual or organization. Political independence means the freedom of a country, state or other similar entity an external government.[42]

Merriam defines independence as a quality of being independent that means you're on your own term with the exclusion of all others in decision making and other categories and perspectives.[43]

2.5 Choice of Concept

Data Protection Structures can be addressed severally, ombudsman for data protection, Data protection Supervisory Authorities, Data protection Regulatory Authorities etc. In this study they will be referred to as Data Protection Authorities (DPAs). Additionally, the concept of independence has been extensively elucidated through various lenses, encompassing scholarly works, principles outlined in international treaties, and definitive rulings handed down by judicial bodies, each contributing to a comprehensive comprehension of the notion of absolute autonomy and self-reliance. In this study, the term complete independence will be of the same meaning as the term independence.

2.6 Conclusion

This Chapter has been specifically set forth by the researcher to present the key concepts that relates and are found in the research title. This chapter further explains upon the importance of having an efficient legal framework on data

[42]General assembly in its resolution 68/167 international human rights law Article 12 UDHR HRC 27TH SESSION Annual report of the United Nations Commissioner for human Right and reports the privacy in the digital age available at www.ohchr.org

[43] General assembly in its resolution 68/167 international human rights law Article 12 UDHR HRC 27TH SESSION Annual report of the United Nations Commissioner for human Right and reports the privacy in the digital age available at www.ohchr.org p.23

protection within the society for protection of personal data and information of data subjects. This part gives the reader a view on what really is data protection, how an individual's personal data is legally protected and why it is currently relevant and important to the society. Hence highlighting what will be discussed in detail within the following chapters. The independence of data protection authorities holds a crucial position within the realm of international data protection laws and conventions. This autonomy is paramount in enabling Data Protection Authorities (DPAs) to carry out their duties with impartiality, thus effectively enforcing data protection regulations and upholding the sanctity of individuals' privacy rights. Safeguarding the autonomy and integrity of DPAs is not merely a regulatory formality but a foundational element in cultivating public trust, fostering cross-border collaboration, and fortifying a resilient data protection infrastructure in our rapidly evolving digital landscape. The preservation of DPAs' autonomy is a linchpin in ensuring the efficacy and credibility of data protection mechanisms worldwide, underscoring the significance of their role in upholding privacy standards and promoting transparency in data handling practices. As technology continues to shape our lives, it is crucial to reinforce and protect the independence of DPAs to ensure that privacy remains a fundamental right for everyone.[44]

[44]General assembly in its resolution 68/167 international human rights law Article 12 UDHR HRC 27TH SESSION Annual report of the United Nations Commissioner for human Right and reports the privacy in the digital age available at www.ohchr.org p 23

CHAPTER THREE

INDEPENDENCE OF DATA PROTECTION AUTHORITIES IN TANZANIA

3.1 Introduction

Data protection has become an increasingly critical issue globally, with the rise of digital technologies and the growing volume of personal data being collected and processed. Many countries around the world have taken steps to strengthen data protection by setting up Data Protection Authorities as dedicated regulatory agencies tasked with upholding data protection legislation and upholding the privacy rights of individuals. In line with this trend, Tanzania, situated in the East African region, recently introduced a comprehensive personal data protection law. This legislative initiative represents a significant advancement in the realm of data protection within the country. Prior to the enactment of this law, the only relevant legal framework in place was the Cybercrimes Act, thereby highlighting the necessity for a more tailored and specific set of regulations to address the complexities of data protection and privacy rights. By establishing a robust legal foundation for safeguarding personal data, Tanzania aims to enhance trust in digital transactions, protect individuals from potential data breaches, and align its data protection practices with international standards and best practices.[45] The establishment of these laws is to be supervised by the Data Protection Regulatory Authorities also named as Data Protection Authorities (DPA).[46] In Tanzania the

[45] Tanzania Personal Data Protection Act December 2022
[46] Ibid pg 18

DPA is under the ministry of Communication and Information and TCRA.[47] In order to effectively manage personal data, governmental authorities opt to confer certain powers to individuals or organizations tasked with overseeing the handling of such sensitive information. This delegation is aimed at ensuring the safety of personal data and preventing its misuse. However, from an international perspective, there is a strong advocacy for the autonomy of this regulatory body. It is recommended that this supervisory entity operate independently from direct government control, thereby safeguarding the principle of personal data privacy. This approach is considered crucial in upholding the integrity and impartiality of data protection measures on a global scale. By establishing independence in the oversight of personal data handling, a more robust framework is envisaged to fortify data protection laws and safeguard individual privacy rights.[48] This autonomy is crucial for DPAs to act impartially, objectively, and in the best interests of the public.

3.2 Legal Framework of Data Protection Authorities in Tanzania

The legal frameworks governing data protection in Tanzania was put into practice in 2022 and it is used in Tanzania mainland and Zanzibar with exception of other things which are not referred to as union matters. This includes enacted dedicated data protection laws, while others rely on sector-specific.[49] These laws generally align with international standards, such as the General Data Protection Regulation (GDPR) of the European Union, but variations exist in terms of scope, enforcement powers,

[47] Tanzania Communication Regulatory Authority 2003 part 11 (4) , TCRA (Procedure for Rules of Inquiry) 2004 and Recital 117 of GDPR.
[48] See article 52 of GDPR 2008
[49] Ibid p. 16

and penalties.[50] The main objective of this law is to protect individual data and ensuring the proper collection and dissemination or data sharing of individual data. By ensuring that the individual are protected in Tanzania, it enacted the law of data protection in 2022 including the establishment of Personal Data Protection Commission in 2024.[51] The commission is vested with a wide range of powers, one of which includes the thorough monitoring of compliance by data controllers and data processors. This involves not only ensuring that all entities handling personal data adhere to the regulations but also taking proactive measures to address any potential breaches. Additionally, the commission is tasked with the reception, investigation, and resolution of complaints regarding alleged violations of personal data protection and individuals' privacy rights. It is empowered to delve into any issue that comes to its attention affecting the safeguarding of personal data and encroaching upon individuals' privacy, with the authority to take appropriate remedial actions. Furthermore, the commission is mandated to engage in continuous research and monitoring of technological advancements in data processing to stay abreast of developments that may impact data protection measures and privacy regulations.[52] The GDPR however advocates for the independence of data protection authorities for it to work with adequacy, here discussed below are the area to assess the independence of data protection authorities in Tanzania.[53]

[50]See Tanzania Personal Data Protection Act Dec 2022 S. 1-2
[51] Available at https://fbattorneys.co.tz Personal Data Protection Commission Operationalized 8 March 2024.
[52] Ibid
[53] Ibid p.17

3.3 Appointment and Removal from Office of Data Protection Commissioners Tanzania

In response to the growing apprehension surrounding data privacy and security, the Tanzanian government enacted the Personal Data Protection law. This legislation marked a pivotal moment in the country's commitment to safeguarding the rights of its citizens. By introducing the esteemed role of the Data Protection Commissioner, Tanzania solidified its dedication to ensuring the appropriate handling and protection of personal data. The establishment of this position underlined the government's acknowledgment of the paramount importance of data security in today's digital age, thereby bolstering trust and confidence among Tanzanian citizens and stakeholders alike.[54] This decision came as a vital measure to uphold the principles of data protection, ensure the responsible handling of personal information, and align the nation with international data protection standards. The law provides the procedures to appoint the Data Protection Commissioner but it does not provide the procedures and grounds on how to remove them as per *S.12 of Tanzania Data Protection Act 2019.*[55] The appointment of a Data Protection Commissioner signals Tanzania's commitment to safeguarding the personal data of its citizens. *S.8 of Tanzania Personal Data Protection* provides that he role of the commissioner is crucial in overseeing the enforcement of data protection regulations, advocating for citizen's privacy rights, and ensuring compliance with relevant data protection laws and frameworks of the board.[56]

[54] Available at https://fbattorneys.co.tz Personal Data Protection Commission Operationalized 8 March 2024
[55] Ibid
[56] See Tanzania Personal Data Protection Act Dec 2022 S. 8

The establishment of a Data Protection Commissioner in Tanzania reflects the government's recognition of the significance of data protection and privacy rights in the digital era.[57] This appointment signifies a commitment to safeguarding personal data and ensuring responsible data management practices across the nation. With the commissioner's oversight, however, in the case *S.11 Tanzania Personal Data Protection* the DPC is appointed by the president.[58] It is universally acknowledged that the president holds the highest authority in any given nation, and as such, every decision emanating from the office of the president is deemed to be ultimate and irrevocable in accordance with the established legal framework. The role of the president as the paramount leader of the country bestows upon them the responsibility of making determinations of critical significance, the ramifications of which invariably shape the course of the nation. It is imperative to recognise that, the decisions ratified by the president carry an inherent weight of finality, underscoring the unwavering adherence to the rule of law and the hierarchical structure of governance. The presidential prerogative, anchored in the bedrock of legal legitimacy, serves as the linchpin of executive authority, and thus underscores the non-negotiable nature of presidential decisions within the legal and constitutional paradigm of a given state. Not only that, but also the president has the mandate to remove from office the selected commissioner due to different reasons as he or wishes as provided under *S.12 of Tanzania Personal Data Protection*.[59] In different approaches we have seen the president of Tanzania mainland appoint and re appoint, dismissal, removal, or reassignment the different Director General of

[57] See Tanzania Personal Data Protection Act Dec 2022 S. 8
[58] See Tanzania Personal Data Protection Act Dec 2022 S. 11
[59] See Tanzania personal Data Protection Act Dec 2022 S. 12

different sectors including the recent appointment of Director General of UDART.[60] Also, the appointment and re-appointment of the Director General of TANESCO did not even last for 24 hours.[61] This trend proves that regardless the available procedures and the requirements on how a Director General of certain department is appointed, the president has the power to appoint a new one in case of any provided reasons. This act suggests and proves the political interference which limits the independence of structures of Data Protection authorities in Tanzania.

3.4 Budgets and Resources Provided to DPA s to Exercise Their Independence

Data protection authorities in Tanzania hold a pivotal position in upholding the confidentiality of individuals and upholding the regulations concerning data protection within the nation. Their autonomy stands as a fundamental element vital for guaranteeing their ability to execute their duties efficiently and without disruption from external pressures. The capacity for these authorities to function independently is essential in sustaining the integrity of data protection practices and promoting trust among the populace in the enforcement of data protection laws. Despite the various challenges they may face, such as limited resources or evolving technology, their freedom from undue influence is crucial in maintaining a robust and impartial data protection framework in Tanzania. The Data Protection Authority in Tanzania functions as an autonomous entity within the framework of legislative provisions. Established in accordance with the laws of the country, this regulatory body holds the responsibility of safeguarding the rights of individuals in relation to their

[60] Available at https://www.habarileo.co.tz Jan 11, 2024 *'Rais Samia atengua uteuzi wa Mkurugenzi DART'*

[61] Available at https://www.mwananchi.co.tz 23 Sept 2023 '*Rais Samia aigusa Tanesco, atengua wengine watatu'*

personal data. Operating independently, the Authority ensures compliance with data protection regulations and oversees the implementation of policies designed to secure the privacy and confidentiality of personal information. Through diligent monitoring and enforcement practices, the Authority plays a pivotal role in upholding data protection standards and fostering a culture of accountability among data controllers and processors in Tanzania.[62] This study explores how limited resources and budgetary challenges can impact the independence of data protection authorities in Tanzania, potentially hindering their ability to protect citizen's data rights.

Data Protection Authorities in Tanzania need financial independence to remain impartial and autonomous in their decision-making processes. If they heavily rely on government funding, there might be a risk of undue influence or interference in their operations by political interests. Securing a reliable and independent budget is crucial to ensuring the authority can carry out its duties without any bias. Tanzania data Protection Authorities gets their annual budget from the national assembly and the financial budget is posed to the Minister of ICT as per *S.51 of Tanzania Personal Data Protection*.[63] Not only that but also *S.52 of Tanzania Personal Data Protection* provides that the funds and money that are supposed to be used by the Personal Data Protection Authority (PDPA) are to be monitored by the Personal Data Protection Commission (PDPC) which has started to function in 2024.[64] Furthermore, the law provides that the Data Protection Commission Office is the one liable to supervise

[62] Available at https://www.mwananchi.co.tz 23 Sept 2023 '*Rais Samia aigusa Tanesco, atengua wengine watatu'*

[63] See S. 51 of Tanzania Personal Data Protection Act Dec 2022.
[64] See S. 52 of Tanzanian Personal Data Protection Act Dec 2022

all the resources and re allocation of resources according to the law.[65] On the other hand the Minister of Communication is required to recommend and changes in the report of annual report provided to his office as provided under *S.53 (3) of Tanzania Personal Data Protection*.[66] The regulations stipulated by the law regarding the management of the financial aspects of DPAs can lead to insufficient financial resources, thereby hindering the authority's capacity to carry out thorough investigations into data breaches and privacy infringements. Inadequate funding may impede the acquisition and utilization of advanced forensic technologies, causing delays in investigations and providing an opportunity for potential wrongdoers to avoid being held accountable, given that the DPAs are not granted complete autonomy over their financial resources. This financial constraint ultimately jeopardizes the effectiveness of the DPAs in enforcing data protection regulations and upholding privacy rights.

3.6 The structures of DPAs in Tanzania

Impartiality and independence are two foundations upon which this organization is built. Independence allows the authority uncompromised decision-making capacity in developing efficient and effective procedures.[67] DPAs must have sufficient resources, expert knowledge, and complete independence to perform their tasks effectively. Independence is something that is hard earned and must be protected as independence is a principle that any appointee can contravene, the authority will be

[65] See S. 52 of Tanzanian Personal Data Protection Act Dec 2022
[66] See S. 53(3) of Tanzanian Personal Data Protection Act Dec 2022
[67] Available https://www.pwc.co.tz Data Privacy- do you know your rights and obligations Nov 2023

established in a manner that is resistant to political or external pressures.[68]

In Tanzania the Data Protection Authority are independent and are supposed to practice their daily duties with freedom with exclusion of all others. The respects of the law on the guaranteed independence of DPA in Tanzania there have been some contradiction of laws. *The Tanzania Personal Data Protection Act 2022* advocates for the establishment of Personal Data Protection Commission (PDPC) which is required to supervise the performance of DPA in Tanzania as per *S.57 of Tanzania Personal Data Protection*.[69] Furthermore, the involvement of other figures like the Minister of the ministry in question leads to the interference of the DPA's independence contrary to the law.[70] By observing these provisions by the law it is safe to say that the law provides the room to put the independence of DPA at stake. In Africa there some countries like Botswana and Uganda whereby their respective DPA's are built within the telecommunication departments.

3.7 The Role of Independence in Effective Data Protection in Tanzania

Independent Data Protection Authorities (DPAs) function with a higher degree of efficacy when it comes to upholding data protection regulations, carrying out thorough investigations into data breaches, implementing appropriate penalties on non-compliant entities, and safeguarding the fundamental privacy rights of individuals. By virtue of their autonomy and detachment from external influences, independent DPAs are inherently more proficient in executing their duties with

[68] Available at https://car.dole.gov.ph security of tenure and causes of termination Regional Office CAR August 2 2023
[69] Available at https://car.dole.gov.ph security of tenure and causes of termination Regional Office CAR August 2 2023
[70] Ibid p.21

impartiality and integrity. Secure in their autonomy, these regulatory bodies possess the requisite authority and resources to oversee compliance with data protection legislation, ensuring that organizations adhere to the prescribed standards for the protection of personal data. Moreover, the autonomy of independent DPAs lends credibility to their enforcement actions, instilling trust in the general populace and reinforcing the significance of data privacy principles. This, in turn, contributes to fostering a culture of accountability and responsibility among data controllers and processors, thereby strengthening the overall data protection framework within a given jurisdiction.[71] DPAs can actwithout fear or favors, making decisions based on legal principles and the public interest rather than political or commercial pressures. The independence of DPAs is vital to their effectiveness in upholding data privacy rights. It ensures impartial decision-making, prevents conflicts of interest, and fosters public trust in the Regulatory process. Independent DPAs can enforce data protection laws objectively, without succumbing to political pressure or undue influence from powerful stakeholders.[72] This is due to the fact that one has the right to complain once their data are used without following the data protection and privacy principles.

3.8 Conclusions

The independence of data protection authorities in Tanzania is of paramount importance, as it transcends mere administrative considerations to form the bedrock of the entire data protection framework. This crucial principle not only safeguards the rights of citizens but also fosters a conducive environment for innovation and

[71] Available at https://car.dole.gov.ph security of tenure and causes of termination Regional Office CAR August 2 2023 p.22
[72] See S.39 Tanzanian Personal Data Protection Act 2022

bolsters the nation's reputation on the global digital stage. As Tanzania treads through the complexities of the digital era, the preservation and enhancement of the autonomy of its data protection authorities stand as a critical imperative that cannot be overlooked. Upholding the independence of these regulatory bodies is essential for ensuring transparency, accountability, and effectiveness in safeguarding data privacy rights, thus reinforcing the foundation of trust in the digital ecosystem. In a landscape increasingly shaped by rapid technological advancements and evolving data privacy challenges, the unwavering autonomy of Tanzania's data protection authorities is key to not only maintaining regulatory compliance but also nurturing a culture of responsible data handling and protection across all sectors of society. The independence of data protection authorities in Tanzania is a linchpin for upholding the principles of privacy and data security. By ensuring their autonomy, the Tanzanian government can reinforce citizen’s trust in digital processes, stimulate economic growth through responsible data practices, and contribute to a global standard of data protection. It is imperative that the Tanzanian government continues to prioritize and uphold the independence of its DPAs to secure a data-driven future for the nation.

CHAPTER FOUR

INDEPENDENCE OF DATA PROTECTION AUTHORITY IN KENYA

4.1 Introduction

Kenya is the East African country which is a neighbor of other EA countries like Tanzania.[73] Kenya is a vibrant and diverse East African nation which has experienced significant advancements in technology and digitalization over the years. With the growing reliance on digital platforms and data-driven services, the need to protect individual privacy has become a critical concern. To address these challenges and ensure the safeguarding of personal information, Kenya has taken significant strides by establishing data protection authority.[74]

In 2019, Kenya enacted the Data Protection Act, which marked a milestone in the country's approach to data privacy and security.[75] The enactment of this legislation signified a crucial step towards overseeing and controlling the gathering, manipulation, and retention of personal information, whether undertaken by corporate bodies or governmental institutions within the jurisdiction of Kenya. The framework of this law closely mirrors the principles set forth in the European Union's General Data Protection Regulation (GDPR), thereby harmonizing Kenya's data protection policies with prevailing global benchmarks. By aligning these regulations with internationally recognised standards, Kenya is positioned to enhance data privacy practices, safeguard the rights of individuals, and bolster trust

[73] Available https://www.nationsonline.org one world nations online 1998-2023
[74] Available at www.odpc.go.ke Office of the Data Protection Commissioner 2023
[75] See Kenya Data Protection act No 24 2019

in the digital ecosystem.[76]

The main authority responsible for enforcing the Data Protection Act is the Office of the Data Protection Commissioner (ODPC).[83] The ODPC is supposes to be an independent body entrusted with the oversight and enforcement of data protection laws in Kenya. This body however it's not free as it is required to work in consultation with the cabinet secretary for information as provided under *S.8 (2) of Kenyan Data Protection Act 2019.*[77] The act also expressively provides that the ODPC shall act independently in exercise of powers See S. 8(2) of Kenya Data Protection Act 2019.[78] Its primary objective is to protect individual's rights regarding the processing of their personal data while promoting responsible data management practices among data controllers and processors.

One of the key functions of the Data Protection Commissioner lies in the effective management and resolution of data breaches and privacy complaints brought to its attention. Acting as a diligent guardian of personal data, the DPC conducts thorough investigations into reported cases involving the unauthorized access, loss, or disclosure of sensitive information, thereby safeguarding individuals' privacy rights in accordance with legal provisions. Through the judicious application of enforcement measures, the office ensures accountability and imposes sanctions on any entities found to be in violation of data protection laws. Furthermore, the DPC plays a pivotal role in the realm of compliance by offering expert guidance and support to organisations, facilitating their adherence to stringent data protection

[76] See Kenya Data Protection act No 24 2019
[77] See s. 8(2) of Kenya Data Protection Act 2019
[78] See S. 8 (3) of Kenyan Data Protection Act 2019

regulations and fostering the adoption of industry best practices. By promoting a culture of data security and integrity, the DPC actively contributes to upholding the standards of privacy protection within the digital landscape. Through public awareness campaigns and educational initiatives, the Data Protection Commissioner also strives to empower citizens with knowledge about their rights concerning data privacy.

4.2 Legal Framework of Data Protection Authority in Kenya

The Data Protection Act of 2019 was enacted to align Kenya's data protection practices with international standards, such as the General Data Protection Regulation (GDPR) in the European Union.[79] It aims to provide comprehensive protection to individuals' personal data while promoting the growth of the digital economy. The Act applies to both public and private entities that collect, process, or store personal data within Kenya's borders, ensuring that all organizations must comply with its provisions.[80]

The Data Protection Authority is an independent body established under the Act and operates as the watchdog for data protection matters in Kenya.[81] The DPA is vested with extensive powers to enforce data protection laws, investigate data breaches, and impose penalties on organizations that violate the Act's provisions.[82] The Authority iscomposed of a board appointed by the Cabinet Secretary responsible for matters related to information and communication technology.

---

[79] See S. 8 (3) of Kenyan Data Protection Act 2019 P 19
[80] Githaiga. J and Kurji A.J Kenya: Data Privacy Comparative guide PricewaterhouseCoopers Limited 06 Feb 2023
[81] See S.5 of Kenya Data Protection Act No 24 of 2019
[82] See S.3 Of Kenya Data Protection Act No 24 of 2019

The main function of the Data Protection Authority in Kenya is to oversee the registration and licensing procedures of data controllers and processors. Data controllers refer to individuals or organisations with the authority to determine the specific purposes and methods utilised for processing personal data. On the other hand, data processors are entities entrusted with managing data on behalf of the data controllers. By regulating and monitoring the activities of these key players in data management, the Data Protection Authority plays a crucial role in upholding data privacy and security standards within the jurisdiction of Kenya.[83] Registration with the DPA ensures that organizations handling personal data are accountable for their data processing activities and are compliant with the Act's requirements.

The Act also outlines key principles for the processing of personal data, such as lawfulness, fairness, transparency, and purpose limitation.[92] Organizations are required to obtain consent from individuals before processing their personal data, and they must only collect and use data for specific, legitimate purposes. Furthermore, the Act imposes obligations on data controllers and processors to ensure the security and confidentiality of the data they handle.[84]

The ODPC has been instrumental in significantly improving transparency and raising public awareness, particularly among the personnel of the Data Protection Authority and the general population. The ODPC has taken on the responsibility of promoting data protection through comprehensive education and awareness programmes. These proactive measures have effectively informed both individuals and organisations about their rights and responsibilities concerning data protection.

[83] See S.3 Of Kenya Data Protection Act No 24 of 2019
[84] See S.25 of Kenyan Data Protection Act 2019

As a result of these initiatives, there has been a notable increase in knowledge and understanding of personal data protection, thus cultivating a widespread culture of data privacy throughout the nation. The GDPR however advocates for the independence of data protection authorities for it to work with adequacy.[85] Among the major requirement of DPA to perform its activities with efficiency is for it to be independent, however in some areas the Kenyan Data protection Authorities have seen to lack its freedom. Here discussed below are the areas to assess the independence of data protection authorities in Kenya;

4.3 Appointment and Removal from Office of Data Protection Commissioner in Kenya

One of the primary concerns surrounding the appointment of the Data Protection Commissioner in Kenya is the potential for political influence. The Act empowers the President to appoint the Commissioner under *S.6 (4) of Kenyan Data Protection Act 2019* which raises questions about the objectivity and impartiality of the selection process.[86] An appointment directly made by the President and approval from the national assembly might give a rise to conflicts of interest or the perception that the Commissioner may prioritize political interests over data protection concerns. The appointment of the Data Protection Commissioner by the President in Kenya has raised concerns regarding the potential compromise of the independence of the Office of the Data Protection Commissioner. One of the primary issues at hand is the risk that political affiliation could influence the Commissioner's decisions, leading to outcomes that may align more closely with

[85] See S.25 of Kenyan Data Protection Act 2019
[86] See S.6 (4) of Kenyan Data Protection Act 2019

the interests of the ruling party or other influential stakeholders, rather than prioritizing the safeguarding of individuals' data rights. This situation raises the crucial question of whether the appointed Commissioner would be able to carry out their duties with impartiality and autonomy, as required in upholding the integrity of data protection regulations and ensuring the rights and privacy of Kenyan citizens are adequately protected. Moreover, the specter of political influence looming over the Commissioner's role may erode public trust in the enforcement of data protection laws, potentially undermining the effectiveness of the Office in fulfilling its mandate to oversee and regulate data privacy matters in a fair and unbiased manner.

In addition to that influence on regulatory decisions contrary to the act in political pressure could influence the regulatory agenda and enforcement priorities of the Data Protection Commissioner in dealing with individual data as per *S. 26 of Kenyan Data Protection Act 2019.*[87] This has the potential to compromise the safeguarding of individuals' data rights, thereby diminishing public confidence. The perception of political intervention could undermine trust in the data protection authority, resulting in reluctance among citizens to report data breaches or pursue remedies for privacy infringements. Such erosion of trust may have far-reaching implications for the effectiveness of data protection regulations and the willingness of individuals to engage with relevant authorities in upholding their rights to privacy and data security. It is imperative that transparency and independence are maintained within data protection frameworks to preserve public trust and ensure

[87] Explained under section 26 of Data Protection Act No 24 of 2019

the enforcement of data privacy laws.[88] On the other hand as provided under *S.8 (2) of Kenyan Data Protection Act 2019* provides that the office of Data Commissioner may in the performance of its functions collaborate with the national security organs. This is act is supported by the law however it well known that if there is any interaction between one organ and the other, it is bound to be found that there will some contradictions in decision making.

4.4 Budgets and Resources Provided to DPA's to Exercise their Independence in Kenya

It is widely acknowledged that the independence of Data Protection Authorities (DPAs) is crucial for the maintenance of the rule of law and the promotion of fair and impartial enforcement of data protection regulations. DPAs serve as vigilant overseers, responsible for monitoring and regulating the manner in which organisations manage personal data, conducting thorough investigations into reported grievances, and levying penalties upon entities found to be in violation of data protection standards. The autonomy afforded to DPAs enables them to operate with impartiality and autonomy, thus fostering trust in the regulatory process and upholding the integrity of data protection mechanisms. By discharging their duties independently, DPAs reinforce the principles of accountability and transparency in the realm of data protection, thereby bolstering public confidence in the regulation and enforcement of data privacy laws.[89] Independence ensures they are not influenced by political agendas, economic interests, or undue pressure from

[88] Explained under section 26 of Data Protection Act No 24 of 2019
[89] See S.62-63 part VII of Kenya Data Protection Act 2019

powerful entities.[90] This act provides that the financial and budgetary resources will be given by the minister after the approval from the general assembly as provider under *S.67 (a) of Kenyan Data Protection Act*[91] After the completion of this process my jeopardize the DPA right to independence as government funding and the risk of Interference may lead to the financial reliance of DPAs on the government poses a significant risk to their autonomy. If DPAs are dependent on government funding, they may be subject to budget cuts or political interference, compromising their ability to function independently and effectively enforce data protection laws.[92]

Not only that but also S.67 of Kenyan Data Protection Act leads to another threat to DPA independence is the budget cuts and resource constraints which might lead to governments often allocate budgets to various agencies based on their priorities and political considerations. In times of fiscal austerity, DPAs might face budget cuts that hamper their operational capabilities. A lack of sufficient resources could lead to delays in investigations, reduced staff, and limited outreach and educational programs, making it challenging to address the growing complexities of data protection challenges leading to political influence and biased decision-making as when DPAs are reliant on the government for funding, there is a risk of political influence affecting their decision-making processes. Governments may exert pressure on DPAs to pursue or drop investigations that align with their political in tersest. This unwarranted interference significantly undermines the confidence of the general public in the enforcement of data protection regulations. Such

[90] See S.62-63 part VII of Kenya Data Protection Act 2019
[91] See s.67 (a) part IX of Kenya Data Protection Act No 24 of 2019
[92] Ibid

interference perpetuates the perception that Data Protection Authorities (DPAs) place greater emphasis on advancing political agendas, rather than safeguarding the fundamental privacy rights of individuals. Consequently, this detrimental impact leads to a profound erosion of trust in the ability of DPAs to function independently and uphold the core principles of data protection. It fosters a climate where the interests of citizens in maintaining the confidentiality and security of their personal data are relegated in favour of political expediency, thereby weakening the foundational trust essential for an effective regulatory framework in data protection.

4.5 The Structures of DPAs in Kenya

Independence is the foundation upon which this organization is built. Independence allows the authority uncompromised decision-making capacity in developing efficient and effective procedures.[93] The Data Protection authorities are required to be sufficiently equipped with the necessary resources to effectively carry out their duties, possess the requisite expertise, and operate with absolute autonomy. Institutional autonomy of the Data Protection Authority is imperative, ensuring its independence from any external authority. The roles and authority of the DPAs must not be influenced or meddled with by any other entity. This independence is crucial to uphold the integrity and impartiality of the Data Protection authorities in executing their responsibilities and upholding data protection standards.[94]

In Kenya the Data Protection Authority are bounded by law to be independent and are supposed to practice their daily duties with freedom with exclusion of all others

[93] Available https://www.pwc.co.tz Data Privacy- do you know your rights and obligations Nov 2023
[94] Ishabakaki. A.B Enforcement Structures and Complaint Mechanisms (2022) https://www.pwc.co.tz

as per *S.8 (3) of Kenyan Data Protection Act 2019*.[95] The respects of the law on the guaranteed independence of DPA in Kenya there have been some contradiction of laws.

S.8(2) of Kenyan Data Protection Act provides that the ODPC may collaborate with national security organs which are constitutionally defined as Kenyan Defense Forces, the National Intelligence service and the National Police Services.[96] On the other hand *S. 51 of the act* including national security and public interest, this is operationalized by the Data Protection regulation by giving discretions to the cabinet secretary of ICT to make decisions as to what amounts to national security.[97] Furthermore the involvements of other figures like the Minister of the ministry in question lead to the interference of the DPA's independence contrary to the law.[98]

The Office of the Data Protection Commissioner in Kenya collaborates closely with various government bodies to ensure comprehensive data protection enforcement. Apart from the bodies mentioned above ODPC works with judiciary system for the good aim of safeguarding individual right however by doing so this act might lead to put at stake of DPAs independence in Kenya.[99]

[95] See S. 8(3) Kenyan Data Protection Act 2019
[96] See S.8 (3) of Kenyan Data Protection Act 2019

[97] Andre. B, Masse. E, Pisanu. G, Skok. A, Okwara. E Data Protection in Kenya How is this right protected Oct 2021
[98] Ibid p.31
[99] Available at www.accessnow.org Data Protection in Kenya How is this right protected ii analyzing the Kenyan Data Protection Act 2019.

4.6 Conclusions

Kenya's proactive steps to create designated data protection authorities and put into effect the Data Protection Act reflect the nation's unwavering dedication to upholding data privacy standards in the modern digital age. Through the harmonization of its regulations with globally recognized norms, Kenya is steadfast in safeguarding its citizens' inherent right to privacy, thus paving the way for a conducive atmosphere that nurtures innovation and propels data-centric advancements. With the evolution of the digital landscape showing no signs of slowing down, Kenya's strategic positioning in aligning its legal framework with international benchmarks underscores its commitment to fostering a secure and progressive digital environment for both its general public and businesses alike.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This Chapter presents the comparative conclusion on the DPAs in Kenya and Tanzania on the assessment of independence of the Data Protection Authorities in East Africa: a comparative study of Kenya and Tanzania. The study has set forth to answer research questions which are: Whether the structures of DPAs in Kenya and Tanzania guarantee their independence, whether the procedures for the appointment and removal from office of data protection commissioners in Kenya and Tanzania secure their jobs in order to act independently, whether the DPAs in Kenya and Tanzania have their budgets and resources adequately provided to exercise their independence.

The purpose of attaining the objective of this research was to examine critically the patterns of Data Protection Authorities and its independence. By making a comparative study between the data protection and privacy and regulations act/laws of Kenya and Tanzania this study provides its findings and recommendations. This study analyses and presents data collected through the provision of laws from both countries by doctrinal legal research which analyses law in the form of legislation, case law and international instruments as well as comparative legal research which answers the research questions made for the study.

The study reveals that the Data Protection Authorities in East Africa are facing challenges in carrying out their duties independently, primarily due to the structural limitations within the DPAs of countries like Kenya and Tanzania.

These constraints have a direct impact on the autonomy of these authorities. The current level of independence of these Data Protection Authorities is deemed inadequate, as external forces, such as government officials who are granted legal leeway to participate in the decision-making processes of these authorities, pose a significant threat to their autonomy. This phenomenon opens the door to potential political interference and other extraneous influences that could compromise the impartiality and effectiveness of these regulatory bodies in upholding data protection standards.[100]

5.2 Data Presentation and Analysis

The study was conducted through doctrinal legal research which analyses law in the form of legislation, case law and international instruments as well as comparative legal research was done to gather response from the research questions; Whether the structures of DPAs in Kenya and Tanzania guarantee their independence, Whether the procedures for the appointment and removal from office of data protection commissioners in Kenya and Tanzania secure their jobs in order to act independently, Whether the DPAs in Kenya and Tanzania have their budgets and resources adequately provided to exercise their independence.

Based on the questions that this study aimed at answering, it shows that there is the lack of total independence which exclusively differentiates from the requirements provided by the laws and regulation.[101] This proves that the Data Protection Authorities in Kenya and Tanzania are not fully independent which may result to inferior in performing their duties. It is well known that with the current global

[100] Available at www.accessnow.org Data Protection in Kenya How is this right protected ii analyzing the Kenyan Data Protection Act 2019
[101] GDPR Article 52(3) 2008

technological changes data protection is a fundamental human right that guarantees the privacy and security of personal information in the digital era. To ensure effective implementation andenforcement of data protection laws, independent and autonomous data protection authorities play a crucial role. Therefore, findings on the state independence of Data Protection Authorities (DPAs) in Kenya and Tanzania, does not qualify to be termed as independent DPAs.

5.3 Comparative Analysis and Summary of Findings

When analyzing the operational frameworks of countries boasting robust and autonomous Data Protection Authorities (DPAs) such as Germany, the United Kingdom, and Australia, a wealth of invaluable insights can be gleaned for the benefit of Kenya and Tanzania. Drawing parallels and scrutinizing the best practices employed in these established jurisdictions can serve as a guiding light for enhancing the data protection landscapes in Kenya and Tanzania. Understanding the policies, legislative measures, and enforcement mechanisms that have proven effective in safeguarding data privacy rights in these nations can pave the way for the development and fortification of similar structures in the contexts of Kenya and Tanzania. By investigating deep into the methodologies and strategies employed by these exemplary DPAs, Kenya and Tanzania can aspire towards constructing their own formidable data protection frameworks that align with international standards and cater to the specific needs of their respective populations. Another insight can be found through studying the experiences of East African countries that have made significant progress in establishing independent DPAs, such as Kenya which enacted the Data Protection law in 2019. By comparing Kenya to Tanzania, it can highlight best practices and identify strategies

that have been successfully used in ensuring the autonomy and effectiveness of these DPA's. Kenya provides more references on this study unlike the country like Tanzania which is not yet matured in the data protection and Privacy field.

It is observed that the Data Protection Authority might be a single government officials with several members or it might be a private body, however the independence of such anauthority is a key factor and therefore in the assessing of its independence the factors like the structures of DPAs guarantee their independence, procedures for the appointment and removal from office of data protection commissioners in secure their jobs in order to act independently or if they have their budgets and resources adequately provided to exercise their independence[102]. In Kenya, the Data Protection Act was enacted in November 2019, providing the legal basis for the establishment of the Data Protection Commissioner (DPC). The DPC is tasked with overseeing and regulating the processing of personal data and ensuring compliance with the law. In Tanzania, the progression towards strengthening data protection saw a notable advancement through the enactment of the Cybercrimes Act in 2015, marking a pivotal milestone in the country's legal framework concerning cyber security and data privacy. This legislative development laid a solid foundation for addressing digital threats and safeguarding sensitive information in the rapidly evolving digital landscape. Building upon this foundation, in December 2022, Tanzania enacted comprehensive legislation specifically dedicated to data protection and privacy. This new law represents a crucial evolution in the country's approach to cybersecurity, underscoring its

[102] Data Protection and Privacy Laws identification For Development ID4D *https://id4d.worldbank.org*

commitment to ensuring the secure and responsible handling of data, thereby aligning its regulations with international standards and best practices in the realm of data protection.

The GDPR advocates for the total independence of the Data Protection Authorities and Privacy that the member of the authority shall work free and will not take any instructions from the external forces whether direct or in direct so that the interference from other sources will not lead to the destruction of their decisions.[103]

Basing on legislation, the provision data protection authorities in Kenya and Tanzania structures affects their independence as there is a room of DPAs to interact with other bodies. These bodies from both Countries data protection authorities are so much instituted and associated with the government as it is established within the laws as we have seen the procedures on the appointment of its officials.[104] By engaging high-ranking officials such as presidents and ministers in this decision-making process, the operational autonomy of data protection authorities is significantly constrained. This restriction arises from the foreseeable challenges that DPAs may encounter when attempting to enforce accountability measures against the government, particularly in instances where allegations of improper personal data usage are involved. The direct involvement of superior leaders creates a power dynamic that complicates the DPAs' ability to impartially address potential violations, potentially inhibiting their capacity to uphold data protection standards effectively. Consequently, DPAs may find themselves in a

[103] Available at www.accessnow.org Data Protection in Kenya How is this right protected ii analyzing the Kenyan Data Protection Act 2019
[104] Ibid

compromised position, unable to fulfill their daily responsibilities with the required autonomy and authority. This limitation underscores the importance of maintaining the independence of DPAs to execute their duties without undue influence from political figures, thus ensuring the proper safeguarding of individual's data privacy rights.[105] The lack of independence may result in biased enforcement of data protection laws. Data protection authorities should be impartial and able to take action against both private and public organizations when data breaches occur. However, government involvement might prioritize shielding government agencies from scrutiny, undermining the impartiality of the authorities. In contrast, government association might lead to reduced transparency, as sensitive information could be withheld or manipulated for political reasons. To ensure robust data protection, it is vital to maintain the autonomy of these authorities and insulate them from undue government influence.

In the ongoing discussion regarding the adequacy of financial resources allocated to the data protection authorities in Kenya and Tanzania to ensure their functional autonomy, it is imperative to delve into the intricacies of how budgetary allocations are administered within the context of data protection and privacy governance. Notably, the fiscal stewardship pertaining to the departments responsible for data protection and privacy in both countries is overseen by the respective Ministries, each falling under the purview of the governmental executive branch. These budgetary dynamics play a pivotal role in shaping the operational capacities and independence of the data protection authorities in Kenya and Tanzania, as the extent of financial allocations directly correlates with the ability of these regulatory bodies

[105] *Jamii forum v. R* www.jamiiForums.com 13 July 2023

to effectively carry out their mandates in safeguarding data privacy rights and enforcing compliance with relevant regulations within the digital domain. By examining the mechanisms through which budgetary provisions are managed and disbursed within the framework of data protection governance, a comprehensive evaluation of the structural foundations underpinning the autonomy and efficacy of data protection authorities in Kenya and Tanzania can be elucidated. In Kenya *Data Protection Act S. 67 (a)* states that the money to run the office of data protection Commissioner (ODPC) will be given to the office after the money that is approved in the National Assembly where by the representative of the office is the minister.[106] On the other hand *Tanzanian Personal Data Protection 2022 S.51* also advocates that the money to run the data protection and privacy office will be the money that is approved from the generally assembly.[107] Now it's a no brainer that these DPAs are built within the ICT Ministries therefore the money are not given directly to the DPAs commissioner rather theyare under the Minister of ICT of each country respectively. The financial interference of the government in Tanzania poses a grave threat to the independence of data protection authorities. As guardians of citizen's privacy rights, these authorities must remain impartial and autonomous. However, when the government exerts control over their funding and resources indirectly hence proved that their ability to act without bias is compromised. The interference experienced by data protection authorities in Tanzania poses a significant threat to their ability to effectively monitor and regulate powerful entities, ultimately compromising the accountability mechanisms

[106] The Act Nov 2019 Kenya Gazette Supplements No.181 (Act N0.24)
[107] The Act and Tanzania Communication Regulatory AuthorityAct 2003 part 1v (28)

that are essential for safeguarding personal information. This susceptibility to external influence creates a concerning opportunity for the misuse and exploitation of citizens' data, thereby jeopardizing their right to privacy. In the absence of robust and empowered data protection authorities, the integrity of the digital landscape is compromised, leading to a pervasive erosion of trust among the populace. It is therefore imperative to prioritize the preservation and autonomy of these regulatory agencies, as they play a crucial role in upholding democratic principles and ensuring the protection of citizens' privacy rights in Tanzania.

An analysis conducted as part of the study also delves into the procedural mechanisms governing the appointment and dismissal of data protection commissioners, aimed at safeguarding their tenure and ensuring their ability to operate with full autonomy. Central to this inquiry is an examination of the extent to which the appointed heads of the data protection authorities within the East African Community (EAC) are guaranteed job security and enjoy safeguards that shield them from arbitrary removal from their positions. This critical evaluation is integral to assessing the functional independence and operational resilience of these commissioners within the complex regulatory landscape of the EAC. By scrutinizing the legal frameworks underpinning the appointment and dismissal processes, the study seeks to ascertain the robustness of the safeguards in place to insulate data protection commissioners from external pressures that may compromise their impartiality and effectiveness in upholding data privacy standards across the region.[119] The procedures for the appointment and removal from office of data protection commissioners in securing their jobs in order to act independently of

data protection authorities is vital for safeguarding individual rights, promoting transparency, and fostering public trust in the handling of personal data. In East Africa, specifically in the countries of Kenya and Tanzania, the process of appointing the data protection commissioner follows a set of similar procedures. This vital regulatory position, essential for upholding data privacy and security laws in the respective nations, mandates a stringent selection process. In both Kenya and Tanzania, the appointment of the data protection commissioner involves rigorous assessments of qualifications, experience, and expertise in the field of data protection. Key stakeholders, governmental bodies, and regulatory authorities collaborate to ensure transparency and adherence to established criteria during the selection process. The overarching goal of these procedures is to warrant that competent and capable individual are entrusted with the significant responsibilities associated with safeguarding data rights and enforcing data protection regulations within the East African region.[108] The procedure provides that after every procedure followed the name of a commissioner on a vacancy position shall be given out by the president with the approval from the national assembly however the law does not provide the procedure for removal from office. In both countries the powers of the president in association with appointment of ODPC have been see together with its disadvantages. The president has the power to re appoint the Data Protection Commissioners even if the period of five years has not yet passed. This is due to the absence of clear procedures on the removal from the office also by following the trend of different changes made by the president in

[108] The Act and Tanzania Communication Regulatory AuthorityAct 2003 part 1v (28)

other sectors.[109] Hence this fact proves that there is the lack of independence in DPA, s in Kenya and Tanzania.

This study has also concluded that DPAs in Kenya and Tanzania are not independent by analyzing the structures of DPAs if they guarantee their independence. The study discovers that the structure of DPAs leaves the room for interferences from external sources leading to the room to jeopardize their decision making.[110] The operational mechanisms and available resources play a crucial role in determining the efficacy of data protection authorities. In both Kenya and Tanzania, the Data Protection Commission (DPC) has been actively functioning since the introduction of the *Personal Data Protection Act*. This has enabled the DPC to enhance its operational capabilities, cultivate specialized expertise, and forge collaborative relationships with various stakeholders, notwithstanding the need to involve the minister in certain functions. Adequate resources, encompassing financial support and well-trained personnel, are fundamental prerequisites for the DPC to effectively fulfill its designated responsibilities and obligations.

5.4 Significance of Independence of Data Protection Authorities

The independence of data protection authorities in Tanzania and Kenya is crucial for ensuring the effective and fair enforcement of data protection laws in these countries therefore data protection has a great importance to the public as explained below.

Independent Data Protection Authorities play a critical role in fostering a sense of

[109] The Act and Tanzania Communication Regulatory AuthorityAct 2003 part 1v (28)
[110] Ibid

trust and public confidence, attributes that are inherently associated with the autonomy and credibility of independent regulatory bodies. The impartiality and competence typically attributed to these independent DPAs are instrumental in safeguarding the privacy rights of individuals in the digital realm. Such assurance and credibility are pivotal in encouraging individuals to willingly disclose their personal data, knowing that it is being overseen and protected by an unbiased and proficient entity. This establishment of trust is not only paramount for ensuring the secure handling of personal information but is also fundamental in bolstering the overall progression of the digital economy. By instilling faith in the mechanisms and processes that govern data protection, independent DPAs contribute significantly to creating a conducive environment for the seamless flow of data essential for the growth and innovation within the digital landscape. Also, effective enforcement of Data Protection Laws is beneficial as independent DPAs have the authority and resources to enforce data protection laws effectively. They can investigate privacy breaches, issue fines, impose sanctions, and take legal action against non-compliant organizations. This enforcement capability acts as a deterrent, encouraging organizations to prioritize data protection. On the other hand, the establishment of independent Data Protection Authorities (DPAs) in both Kenya and Tanzania is crucial for ensuring the alignment of data protection laws and practices with international standards and guidelines. These autonomous regulatory bodies play a vital role in overseeing and enforcing data protection regulations to guarantee the privacy and security of personal information. By promoting harmonization with global data protection frameworks, independent DPAs facilitate seamless cross-border data transfers, strengthen international

cooperation on data governance issues, and ultimately bolster the region's standing as a trustworthy and secure hub for data processing activities. This alignment not only enhances data security measures but also cultivates a conducive environment for fostering trust among businesses, individuals, and foreign partners engaging in data exchanges within the region.

Both Tanzania and Kenya, the establishment and maintenance of an independent data protection authority would contribute significantly to the overall development and growth of their digital economies while safeguarding the privacy and rights of their citizens. By ensuring the proper handling of personal data, these countries can build trust with citizens, businesses, and international partners in an increasingly data-driven world.

In both Tanzania and Kenya, the creation and effective operation of autonomous data protection authorities are vital steps towards fostering the advancement and prosperity of their digital economies, all the while upholding the privacy and fundamental rights of their inhabitants. The establishment of such authorities serves as a key mechanism in overseeing the appropriate management of personal data, thereby enabling these nations to cultivate a sense of trust among their citizens, enterprises, and global collaborators within an ever-expanding data-centric landscape. Through the implementation of robust data protection frameworks, Tanzania and Kenya can not only enhance the reliability of their digital ecosystems but also fortify their position in the international arena as responsible custodians of sensitive information, positioning themselves favorably for sustained economic and technological growth.

Without stable and independent positions, these authorities might face undue influence and pressure from external entities, compromising their ability to enforce data protection laws effectively. This instability could lead to frequent personnel changes, resulting in inconsistent enforcement and weakened institutional knowledge. Additionally, the absence of security of tenure might deter competent professionals from taking up such roles, further hampering data protection efforts. Ultimately, this situation could erode public trust in data handling practices and hinder the region's ability to safeguard individual privacy rights.

5.5 Conclusion and recommendations

Legislative Reforms, that the government should enact laws that guarantee the security of tenure for data protection authorities. Establishing fixed terms and clearremoval procedures for key personnel can help insulate them from political interference. Also, investing in training and capacity building programmers for data protection authorities plays a crucial role in enhancing their proficiency to tackle the ever-evolving landscape of data privacy concerns. These initiatives equip authorities with the necessary skills and knowledge to effectively address emerging challenges in data protection, ultimately bolstering their operational effectiveness and credibility. By fostering a culture of continuous learning and skill development, data protection authorities can stay abreast of the latest trends and techniques in safeguarding individuals' data rights, thereby ensuring heightened levels of public trust and confidence in their regulatory capabilities.

Confidence in their abilities is crucial for data protection authorities to effectively carry out their duties. By maintaining independence from political and external

pressures, these authorities can focus on their mandate without any interference. It is essential to provide them with the necessary resources, reporting mechanisms, and transparency to ensure they can operate autonomously and uphold data protection laws without any external influence. Ensuring that data protection authorities have the confidence in their own capabilities is vital for their independence. By shielding the DPA's work from political and external forces, these authorities can focus on their responsibilities without any outside interference. Providing them with sufficient resources, clear reporting mechanisms, and transparency will further strengthen their ability to carry out their functions autonomously and uphold data protection laws effectively.

The independence of data protection authorities in Kenya and Tanzania holds significant importance in safeguarding the data privacy and security rights of citizens within the respective countries. In Kenya, notable progress has been achieved through the establishment of an autonomous Data Protection Commissioner empowered by comprehensive legal frameworks. This has enabled Kenya to effectively oversee and enforce data protection regulations independently. Conversely, Tanzania encounters obstacles concerning the explicit guarantee of autonomy for its regulatory body, the Tanzania Communications Regulatory Authority (TCRA). This lack of explicit independence raises concerns about the capability of the TCRA to impartially regulate data protection matters. As a result, ensuring and enhancing the independence of the TCRA is imperative for Tanzania to fortify its data protection governance and uphold the privacy rights of its citizens. It is imperative for both nations to consistently prioritize enhancing the independence

and capacity of their Data Protection Authorities (DPAs). This involves allocating sufficient resources to these regulatory bodies, enabling them to effectively carry out their duties in upholding data privacy standards in the increasingly digital landscape. Furthermore, fostering public awareness on data protection rights is essential for safeguarding individuals' personal information and ensuring compliance with relevant data protection regulations. By committing to these measures, both countries can reinforce the protection of data privacy and security in the contemporary era of rapid technological advancement.

REFERENCES

Andre. B, Masse. E, Pisanu. G, Skok. A, Okwara. E Data Protection in Kenya How is This Right Protected Oct 2021

Bennet, C, J. *Regulating Privacy Data Protection and Public Policy in Europe and the United States.* Cornell University Press, Ithaca/London 1992 p.18

Chaput S. A *Independent Data Protection Authority Matters.* The Jakarta Post Jakarta.com

Ducuing. C., *Institutional Aspects of the Wittschaftacademie Case: Focus on The Independence of Data Protection Supervision* (2018) available at https://www.law.kuleuven.be

Fruster. G et al., *The Right to Lodge a Data Protection Complaint: OK, But Then What? An Empirical.*

George, O. *Big Brother is Watching You Science Fiction and Social Science*. June 8, 1949

Greenleaf. G. Independence of Data Privacy Authorities: International Standards and Asia –Pacific Experience Computer law &security Review, Vol 28 issues 1&2 2012 rev.2014 Schutz GmbH & co. Data Protection Policy July 2020

Ishabakaki A. B *Enforcement Structure and Complaint Mechanisms Victory* Arttoys 2022.

Morris. J (1993) Independent lives. Community care, macmillanhttps://journals.sagepub.com

Morris. J Independent lives. Community care. Macmillan (1993) https://journals.sagepub.com

Northway R, *What Does Independency Mean?* University of South Wales UK August 21, 2015.

Northway R, what does independency mean? University of South Wales UK August 21, 2015.

Petrarca. R, Sailus. C. *Explore the concept of Independency learn the various meaning ofindependency* 2022 https://study.com

Petrarca.R, Sailus. C Explore the concept of Independency learn the various meaning ofindependency 2022 https://study.com

Roos, A, *The Law of Data (Privacy) Protection A Comparative and Theoretical Study LLD, Thesis UNISA South African Position South Africa*. law journal 2007 Vol 124.

Sesan. G, Olumide. B., *Data protection at the establishment, independence, Independence impartiality Efficiency of Data Protection Supervisory Authorities in the Two Decades of Their Existence on the continent* 2021.

Sevila. S.I. *Trends in Privacy Enforcement: A Comparative Analysis of po**st**-GDPR Enforcement Styles* (2021).

Szydlo. Principles underlying independence of national data protection authorities: *Commission* v. *Austria* Marek Szydlo *Common Market Law Review* Volume 50, Issue 6 (2013) pp. 1809 – 1826

https://doi.org/10.54648/cola2013167

Widiatedja. P. *Establishing an Independent Data Protection Authority in Indonesia: Future –Forward Perspective* 2022 https://papers.ssrn.com

Wood, M. Independency Encyclopedia Princetoniensis Princeton University 2023

THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY

THE OPEN UNIVERSITY OF TANZANIA

Ref. No OUT/PG202000581 **24th October, 2023**

To whom it may concern,

RE: RESEARCH CLEARANCE FOR MS. DIOGENESS DIOCLES MGANYIZI, REG NO: PG202000581

2. The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1st March 1993 by public notice No.55 in the official Gazette. The Act was however replaced by the Open University of Tanzania Charter of 2005, which became operational on 1st January 2007.In line with the Charter, the Open University of Tanzania mission is to generate and apply knowledge through research.

3. To facilitate and to simplify research process therefore, the act empowers the ViceChancellor of the Open University of Tanzania to issue research clearance, on behalf of the Government of Tanzania and Tanzania Commission for Science and Technology, to both its staff and students who are doing research in Tanzania. With this brief background, the purpose of this letter is to introduce to you **Ms. Diogeness Diocles Mganyizi, Reg.No: PG202000581),** pursuing **Master of Laws in Information and Communication Technology Laws (LLM-ICT).** We here by grant this clearance to conduct a research titled **"An Assessment of Independence of Data Protection Authorities in East Africa: A Comparative Study of Kenya and Tanzania".** She will collect the documentary review from 25th October 2023 to 25th October 2024.

4. In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O. Box 23409, Dar es Salaam. Tel: 022-2-2668820.We lastly thank you in advance for your assumed cooperation and facilitation of this research academic activity.

Yours sincerely,

THE OPEN UNIVERSITY OF TANZANIA

Prof.Gwahula Raphael Kimamala

For: VICE CHANCELLOR

International Journal of Law and Politics Studies
ISSN: 2709-0914
DOI: 10.32996/ijlps
Journal Homepage: www.al-kindipublisher.com/index.php/ijlps

IJLPS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Assessment of Independence of Regulatory Structures Governing Data Protection and Privacy in East Africa: A Case Study of Kenya and Tanzania

Diogeness D. Mganyizi
Department of Public Law, Open University of Tanzania, Box 23409 Dar es Salaam, Tanzania
Corresponding Author: Diogeness D. Mganyizi, **E-mail**: mganyizidiogeness13@gmail.com

| ABSTRACT
In an era of widespread digital information exchange, protecting personal data and privacy has become crucial. East African countries such as Kenya and Tanzania have implemented regulatory structures to address these concerns. However, the effectiveness and independence of these structures raise questions, necessitating a comprehensive assessment. Therefore, this study investigates the question of the independence of data protection authorities in East Africa with a particular focus on Kenya and Tanzania. This study was guided by three questions, namely, do the structures of data protection authorities in Kenya and Tanzania affect their independence? Are the data protection authorities in Kenya and Tanzania sufficiently funded to run their duties? And are the tenures of Commissioners of data protection authorities in Kenya and Tanzania secured? The study engaged two approaches: doctrinal legal research methodology, which analyses law in the form of legislation, case law, and international instruments, as well as comparative legal research methodology, which involves comparative analysis of identified criteria from Kenya and Tanzania. It was observed that the Kenyan data protection authority is more independent than the Tanzanian data protection authority.

| KEYWORDS

Data Protection, Regulatory Authorities, Data Privacy, law

| ARTICLE INFORMATION

ACCEPTED: 16 October 2023 **PUBLISHED:** 04 November 2023 **DOI:** 10.32996/ijlps.2023.5.6.2

1. Introduction

Data protection and privacy have become increasingly important in today's digital age. As individuals and organizations generate and store vast amounts of personal and sensitive data, the need to safeguard such information from unauthorized access and misuse has become paramount. Data breaches not only lead to financial losses and reputational damage but also jeopardize individuals' fundamental rights and freedoms. Consequently, regulatory structures governing data protection have emerged to ensure the secure and responsible handling of data, both at national and international levels. East African countries, being among the countries that have undergone a technological revolution, have also been facing several challenges to data protection and data protection needs[1]. Obstruction of privacy issues associated with big data through breaches is a sample of crimes that disturb data protection and privacy at large.

[1]The Kenya Data Protection (compliance and enforcement) Regulation Act 2021, the Ugandan Data Protection and Privacy and Regulation 2021 under section 39 of data protection and privacy of 2019, The Tanzania personal data Protection and privacy act 2022, The Rwanda Utilities Regulatory Authorities (RURA)

Similar to what has occurred in other parts of the world, most East African countries have taken the initiative to protect their individuals' data[2]. Greenleaf[3] argues that more answers satisfactory answer needs to be found in the international instruments on data privacy, individual and judicial implementation, and standards that have been proposed by the DPAs, where 13 factors were identified as an element of independence, five of which were commonly found which includes independence guaranteed by legislation, appointment of commissioners for fixed term, removal only for specified inadequate conduct The author's argument is relevant to this study, hence the need to conduct this study. Schuez[4] explained that DPAs are the key factor in protecting not only individual's data but also it raises awareness among people on their basic right to privacy. In his study, he showed the way of assessing the independence of DPAs in four countries in the EU. His focus was mostly on the government's partial control of the DPAs, which infringes on their privacy; therefore, he partially discussed a few aspects of assessing DPA's independence, giving room for other scholars to dive deep into the concept of DPA's independence.

The data protection authorities in East Africa and countries that are in EAC are vested with powers to safeguard the right to privacy of individuals[5]. East African Countries like Tanzania recently signed the Personal Data Protection Act of December 2022 as per Article 16 of the constitution of the United Republic of Tanzania URT 1977, which advocates for the right to privacy and security; the Kenyan Personal Data Protection Act 2019 sets the complaints against the breach of personal data privacy handling including the process and procedures on how one can be held liable[6]. The major turning point on personal data protection and privacy is the establishment of data protection structures (Data Protection Authorities), which have been given powers to protect individual data[7] by; which these bodies are acting independently without the interference of external pressure to ensure the proper protection of personal data.

The independence of Data regulatory Structures, also named data protection Authorities (DPA), is central to any successful implementation of data protection legislation. The question of data protection Authorities' independence relates to the institutional design and structures of the DPA resource. The Kenya Data Protection Act 2021 Under Part 11 has explicitly provided for the powers of the office of data protection and privacy, whereby throughout this part, the data commissioner is fully conferred powers to conduct an investigation on their initiatives on the data subject complaints or the third party also the commissioner has powers to exercise any powers prescribed by any other registration under section 9 (1) h however Section 9 (1) *b* allows the data commissioner to obtain professional assistance, consultancy within or outside public service. On the other hand, regarding the independence of data protection authorities, the Kenya Data Protection Regulation Act 2021 Section 67 1 (a-c) advocates for the funds whereby the funds to run the office mainly depend on the annual budget of the national assembly. This is a brainer that the independence of these bodies is limited since they have to wait for the other body to help them financially.

The Tanzania Personal Data Protection of 2022, when it comes to funds to operate the office as per section 51 (a), the money will either be coming from the budget from the parliament and other grants and gifts will help to sustain the office needs which is also argued that these authorities themselves are not indeed independent. Also, in section 53 (3), the minister of the required ministry is capable of ordering the board to make some changes to the estimated budget if it does not comply with it[8]. One of the key factors in ensuring the effective protection of an individual's personal information is the assessment of the independence of regulatory structures governing data protection and privacy. This assessment is particularly crucial in East Africa, specifically in the countries of Kenya and Tanzania. By evaluating the level of independence of these regulatory structures, we can determine whether they are equipped to enforce data protection laws impartially and without undue external influence.

Therefore, the main objective of this study was to critically examine the independence of data protection authorities by making a comparative study between the data protection, privacy, and regulations act/laws in Kenya and Tanzania by investigating their funds, interference with external forces, and their security of tenure. The formal way of assessing the DPAs' independence was done by assessing the textual provision of the Kenyan and Tanzania Personal Data Protection Act. Data protection and privacy authorities under the Data Protection and Privacy Act in East African countries were critically made referring to both laws in the particular countries. The observation under the Act[9] is the observation to what extent that the data protection authorizes is independent by making close observation of the principles of data protection and privacy. These Acts[10] appear to provide room

[2]The Kenya Data Protection (compliance and enforcement) Regulation Act 2021, the Ugandan Data Protection and Privacy and Regulation 2021 under section 39 of data protection and privacy of 2019, The Tanzania personal data Protection and privacy act 2022, The Rwanda Utilities Regulatory Authorities (RURA)

[3] Greenleaf. G Independency of data privacy authorities (part1): I International Standards 2011

[4] Schutz P. Comparing Formal Independence of Data Protection Authorities in in selected EU comparative perspective IFIP Prime life International Summer School June 2012 Available at https://link.springer.com

[5] Ibid pg 2

[6] Available at; https//www.dlapiperdataprotection.com Data Protection Laws of the world 2023

[7] Personal Data Protection Guidelines for Africa 2019 https://www.internetsociety.org

[8] Rwanda Personal Data Protection and Privacy Act

[9] Data Protection and privacy act in Kenya, Uganda, Rwanda and Tanzania 2019,2021,2022 respectively

[10] Ibid

for interference of other bodies as a result of the lack of indecency in making decisions to these authorities during the process of exercising their powers[11].

2. Independence of Regulatory Authorities in Tanzania and Kenya

2.1 Legal Framework of Regulatory Authority

The legal frameworks governing data protection in Tanzania were put into practice in December 2022, and they will be used in Tanzania mainland, and Zanzibar except for things that are not union matters[12] enacted dedicated data protection laws, while others rely on sector-specific.[13] These laws generally align with international standards, such as the General Data Protection Regulation (GDPR) of the European Union, but variations exist in terms of scope, enforcement powers, and penalties. The main objective of this law is to protect individual data and ensure the proper collection and dissemination of data sharing of individual data[14]. The GDPR, however, advocates for the independence[15] of data protection authorities for it to work with adequacy.

The Data Protection Act of 2019[16] was enacted to align Kenya's data protection practices with international standards, such as the General Data Protection Regulation (GDPR)[17] in the European Union. It aims to provide comprehensive protection for individuals' data while promoting the growth of the digital economy. The Act applies to both public and private entities that collect, process, or store personal data within Kenya's borders, ensuring that all organizations comply with its provisions[18]. The Data Protection Authority is an independent body established under the Act and operates as the watchdog for data protection matters in Kenya.[19] The DPA is vested with extensive powers to enforce data protection laws, investigate data breaches, and impose penalties on organizations that violate the Act's provisions.[20] The Authority is composed of a board appointed by the Cabinet Secretary responsible for matters related to information and communication technology.

2.2 Resources and Budgetary Concept of the DPA

Independent DPAs are essential for upholding the rule of law and ensuring fair and unbiased enforcement of data protection regulations. They act as watchdogs, overseeing and regulating how organizations handle personal data, investigating complaints, and imposing fines for non-compliance.[21] Independence ensures they are not influenced by political agendas, economic interests, or undue pressure from powerful entities. The Act[22] shows that the financial and budgetary resources will be given by the minister after the approval from the general assembly[23]; this process may jeopardize the DPA's right to independence as Government Funding and the Risk of Interference may lead to the financial reliance on DPAs on the government poses a significant risk to their autonomy. If DPAs are dependent on government funding, they may be subject to budget cuts or political interference, compromising their ability to function independently and effectively enforce data protection laws.[24] Not only that, but also another threat to DPA independence is the budget cuts and resource constraints, which might lead to governments often allocating budgets to various agencies based on their priorities and political considerations.

In times of fiscal austerity, DPAs might face budget cuts that hamper their operational capabilities. A lack of sufficient resources could lead to delays in investigations, reduced staff, and limited outreach and educational programs, making it challenging to address the growing complexities of data protection challenges leading to political influence and biased decision-making as when DPAs are reliant on the government for funding, there is a risk of political influence affecting their decision-making processes. Governments may exert pressure on DPAs to pursue or drop investigations that align with their political interests. This interference erodes the public's trust in data protection enforcement, as it creates an impression that DPAs prioritize political interests over citizens' privacy rights.

Data protection authorities in Tanzania need financial independence to remain impartial and autonomous in their decision-making processes. If they heavily rely on government funding, there might be a risk of undue influence or interference in their operations

[11] Ibid
[12] See Tanzania Personal Data Protection Act Dec 2022 S. 1-2
[13] Ibid pg 46
[14] See Tanzania Personal Data Protection Act Dec 2022 S. 4
[15] Ibid pg 37
[16] Ibid pg 46
[17] Ibid pg 46
[18] Githaiga. J and Kurji A.J Kenya:Data Privacy Comperative guide PricewaterhouseCoopers Limited 06 Feb 2023
[19] See S.5 of Kenya Data Protection Act No 24 of 2019
[20] See S.3 Of Kenya Data Protection Act No 24 of 2019
[21] See s.62-63 part VII of Kenya Data Protection Act No 24 of 2019
[22] Ibid pg 48
[23] See s.67 (a) part IX of Kenya Data Protection Act No 24 of 2019
[24] Ibid pg 50

by political interests. Securing a reliable and independent budget is crucial to ensuring the authority can carry out its duties without any bias. Tanzania data protection Authorities get their annual budget from the national assembly, and the financial budget is posed to the Minister of ICT[25]. Inadequate financial resources may restrict the authority's ability to conduct comprehensive investigations into data breaches and privacy violations. Insufficient funds may limit the use of advanced forensic tools and delay investigations, allowing potential wrongdoers to evade accountability. The authority's limited investigative powers may undermine its ability to take robust actions against entities violating data protection laws.[26]

2.3 Security of Tenure of Data Commissioners

Security of tenure refers to the assurance that data protection commissioners can remain in office for a specific term without arbitrary dismissal, removal, or reassignment. A fixed and predetermined term provides them with the necessary stability to act objectively, without fear of political repercussions, and to make decisions solely based on the interest of protecting individuals' data privacy rights.[27] Political Interference affects the security of tenure as it acts as a buffer against political interference. Commissioners, when secure in their position, are less likely to succumb to pressure from political figures or private entities seeking to influence their decisions. This independence fosters trust in the DPA's ability to enforce data protection laws impartially[28]. Tanzania's personal data protection advocates for the appointment of a DPC who will serve for five years and will be removed according to the law[29] ; however, his security of tenure is not guaranteed as he is appointed by the president and regardless of the president who has the power to do otherwise.[30]

Unfortunately, in Kenya, the lack of robust safeguards for tenure can lead to various negative consequences that directly impact DPA functions. In Kenya, data protection authorities often face challenges due to the lack of security of tenure; such reasons include political Influence, insecure tenure leaves data protection authorities susceptible to political pressure, leading to compromises in their decision-making processes. Political interference may prevent these authorities from taking strong stances against data breaches or holding powerful entities accountable for violations as per the Kenya Data Protection Act[31] . This act may lead to reduced Institutional Autonomy as Insecure tenure may deter talented professionals from joining data protection authorities, as they perceive potential instability and lack of job security.

Consequently, these institutions may struggle to attract and retain skilled personnel, impeding their effectiveness in handling complex data protection issues.[32] Not only that, but also a lack of security of tenure may lead to Inefficient Decision-making as fear of reprisals can lead data protection authorities to adopt a cautious approach, resulting in delayed or inadequate responses to data breaches and violations. This lack of decisive action could erode public trust in the authority's ability to safeguard their data, which results in **a** weakening Legal Framework; the lack of secure tenure can lead to frequent changes in leadership within data protection authorities. This creates inconsistency and uncertainty in implementing and interpreting data protection laws, undermining the overall effectiveness of the regulatory framework[33].

2.4 Appointments of Data Protection Commissioner.

The Personal Data Protection Law in Tanzania[34]In response to the increasing concern over data privacy and security, the Tanzanian government took a significant step in fortifying its citizens' rights by establishing the position of Data Protection Commissioner. This decision came as a vital measure to uphold the principles of data protection, ensure the responsible handling of personal information, and align the nation with international data protection standards. The appointment of a Data Protection Commissioner signals Tanzania's commitment to safeguarding the personal data of its citizens. The role of the commissioner is crucial in overseeing the enforcement of data protection regulations, advocating for citizen's privacy rights, and ensuring compliance with relevant data protection laws and frameworks of the board.[35]

The establishment of a Data Protection Commissioner in Tanzania reflects the government's recognition of the significance of data protection and privacy rights in the digital era. This appointment signifies a commitment to safeguarding personal data and ensuring responsible data management practices across the nation. With the commissioner's oversight, however, in this case, the

[25] See Tanzania Personal Data Protection Act Dec 2022 S. 51
[26] Ibid
[27] Available at https://car.dole.gov.ph security of tenure and causes of termination Regional Office CAR August 2 2023
[28] Ibid pg 44
[29] Tanzania Personal Data Protection Act 2022 section No 11
[30] Ibid
[31] See Section 12 of Kenya data protection Act No 24 Of 2019
[32] Ibid
[33] Available at www.accessnow.org Data Protection in Kenya How is this right protected part II analyzing the Kenyan Data Protection Act 2019; THE BAD oct 2021
[34] Ibid pg 41
[35] See Tanzania Personal Data Protection Act Dec 2022 S. 8

DPC is appointed by the president[36] , which suggests the political interference that once the president or the minister of the ministry where the DPAs are under, they cannot hold these political leaders since they already have the influence in the board of DPAs.

One of the primary concerns surrounding the appointment of the Data Protection Commissioner in Kenya is the potential for political influence. The Act empowers the President to appoint the Commissioner,[37] which raises questions about the objectivity and impartiality of the selection process. An appointment directly made by the President might give rise to conflicts of interest or the perception that the Commissioner may prioritize political interests over data protection concerns. The appointment of the Data Protection Commissioner by the President may pose several threats to the independence of the Office of the Data Protection Commissioner in Kenya, including Political Affiliation, as the Commissioner's potential political ties may lead to decisions that favor the ruling party's interests or powerful stakeholders, rather than focusing on the protection of individual's data rights.

In addition to that influence on regulatory decisions contrary to the act,[38] political pressure could influence the regulatory agenda and enforcement priorities of the Data Protection Commissioner, potentially undermining the protection of citizen's data rights, which leads to reduced Public trust as the perception of political interference may erode public trust in the data protection authority, leading to a diminished willingness among citizens to report data breaches or seek redress for privacy violations.[39]

3. Assessment of Regulatory Structures in Kenya and Tanzania

3.1 Data Presentation and Analysis

The study was conducted through doctrinal legal research, which analyses law in the form of legislation, case law, and international instruments as comparative legal research was done to gather responses from the research questions: Do the structures of data protection authorities in Kenya and Tanzania affect their independence? Are the data protection authorities in Kenya and Tanzania sufficiently funded to run their duties? Are the tenures of Commissioners of data protection authorities in Kenya and Tanzania secured?

Based on the questions, this study aimed at showing the lack of total independence, which exclusively differentiates the government from data protection authorities, hence proving that the data regulatory authorities in Kenya and Tanzania are not independent, leading to inferior in performing their duties. Data protection is a fundamental human right that guarantees the privacy and security of personal information in the digital era. To ensure effective implementation and enforcement of data protection laws, independent and autonomous data protection authorities play a crucial role. The findings on the independence of data protection authorities in Kenya and Tanzania, examining their establishment, legal frameworks, operational mechanisms, challenges, and implications for data privacy and security in the two countries, leave room for government interest.

3.2 Operational Mechanisms and Resources

The operational mechanisms and available resources significantly impact the effectiveness of data protection authorities. In Kenya, the DPC has been operational since the enactment of the Personal Data Protection Act, allowing it to build capacity, develop expertise, and establish partnerships with stakeholders. Adequate resources, including funding and staff, are essential for the DPC to execute its mandate effectively. In contrast, Tanzania's lack of a dedicated data protection authority limits the effective implementation and enforcement of data protection laws. Without the appropriate organizational structure, resources, and expertise, data protection enforcement may suffer, leaving citizens vulnerable to potential data breaches and privacy violations.

3.3 Comparative Analysis of Independency of DPAs in Kenya and Tanzania

In analyzing the assessment of the independence of regulatory structures governing data protection and privacy in East Africa, specifically in Kenya and Tanzania, it is vital to consider the various challenges and limitations faced by these nations. These include issues related to inadequate legislation, lack of resources for effective implementation, the influence of political factors, and limited public awareness about data protection. Studying the experiences of East African countries that have made significant progress in establishing independent DPAs, such as Kenya, can highlight best practices and identify strategies that have been successful in ensuring the autonomy and effectiveness of these regulatory bodies, unlike a country like Tanzania, which is not yet matured in the data protection and Privacy field[40].

The Regulatory Authority might be a single government official with several members, or it might be a private body; however, the independence of such an authority is a key factor, and therefore, in assessing their independence, factors like the structural

[36] See Tanzania Personal Data Protection Act Dec 2022 S. 8

[37] See S.6 (4) Of Kenya Data Protection Act No 24 of 2019

[38] Explained under section 26 of Data Protection Act No 24 of 2019

[39] Ibid pg 48

[40] Tanzanian Personal Data Protection Act 2022

composition of the body, method of appointment of the Commissioner, security of tenure and budget to run the office without depending on the other Organ[41]. In Kenya, the Data Protection Act was enacted in November 2019, providing the legal basis for the establishment of the Data Protection Commissioner (DPC). The DPC is tasked with overseeing and regulating the processing of personal data and ensuring compliance with the law. In Tanzania, the journey toward data protection took a significant step forward with the passage of the Cybercrimes Act in 2015. However, in Dec 2022, Tanzania passed the law of data protection and privacy.

The GDPR[42] advocates for the total independence of the Data Protection and Privacy Regulatory Authorities that the members of the authority shall work freely and will not take any instructions from external forces, whether direct or indirect, so that interference from other sources will not lead to the destruction of their decisions. Based on legislation provisions, supervisory Authorities in Kenya and Tanzania structures of data protection authorities in Kenya and Tanzania affect their independence. The EAC Countries' data regulatory authorities are much instituted and affiliated with the government[43] , and even the supervisors are appointed by top leaders like the President[44]; this whole process limits the freedom of supervisory authorities in performing their day-to-day duties since they will find it difficult to hold the government accountable once it's accused of using personal data wrongly[45] a lack of independence may result in biased enforcement of data protection laws. Data protection authorities should be impartial and able to take action against both private and public organizations when data breaches occur. However, government affiliation might prioritize shielding government agencies from scrutiny, undermining the impartiality of the authorities. In contrast, government affiliation might lead to reduced transparency, as sensitive information could be withheld or manipulated for political reasons. To ensure robust data protection, it is vital to maintain the autonomy of these authorities and insulate them from undue government influence.

In the question of whether data protection authorities in Kenya and Tanzania are sufficiently funded to run their duties[46] , Kenya and Tanzania countries budgets concerning the Department of Data Protection and Privacy are handled by the Ministries which are under the executive of the government. Kenya Data Protection Act[47] S. 67 (a) states that the money to run the office of the Data Protection Commissioner will be given to the office after the money is approved by the National Assembly. On the other hand, Tanzania Personal Data Protection 2022 S.51[48] also advocates that the money to run the data protection and privacy office will be the money that is approved by the general assembly. Now, it's a no-brainer that these supervisory authorities are built within the ICT Ministries; therefore, the money is not given directly to the regulatory authority commissioner; rather, they are under the Minister of ICT of each country. The financial interference of the government in Tanzania poses a grave threat to the independence of data protection authorities. As guardians of citizen's privacy rights, these authorities must remain impartial and autonomous. However, when the government exerts control over its funding and resources, its ability to act without bias is compromised. This interference undermines their capacity to hold powerful entities accountable, allowing for the potential abuse of personal information. With weakened data protection authorities, the citizen's right to privacy becomes vulnerable to exploitation, eroding trust in the digital landscape. Preserving the autonomy of these agencies is essential to safeguarding citizen's privacy and upholding democratic principles in Tanzania.

Security of tenure is another key factor in assessing the independence of data protection regulatory authorities in EAC[49]. The concept is whether the appointed leaders of the regulatory Authorities in EAC have security of tenure and whether they have the immunity to be not easily removed from office[50]. The security of the tenure of data protection authorities is vital for safeguarding individual rights, promoting transparency, and fostering public trust in the handling of personal data. In East Africa, both Kenya and Tanzania have the same procedures for appointing the data protection commissioner[51] . After every procedure followed, the name of a commissioner for a vacant position shall be given out by the president with the approval from the national assembly[52] . The independence of data protection authorities in Tanzania and Kenya is crucial for ensuring the effective and fair enforcement of data protection laws in these countries therefore data protection has a great importance to the public as explained below.

[41] Data Protection and Privacy Laws identification For Development ID4D *https://id4d.worldbank.org*
[42] See The General Data Protection Act 2008 Article 52 (1-6) and recital 121
[43] Tanzania Communication Regulatory Authority Act 2003 part 1v (28)
[44] Ibid pg 46
[45] www.jamiiForums.com 13 July 2023
[46] Ibid pg 29
[47] The Kenya Data Protection Act Nov 2019 Kenya Gazette Supplements No.181 (Act No. 24
[48] Tanzania Personal Data Protection Act Dec 2022 S.51 (a)
[49] Ibid
[50] Ibid
[51] The Kenya Data Protection Act Nov 2019 Kenya Gazette Supplements No.181 (Act No. 24 section 6(4)
[52] See Tanzania data protection act Dec 2022 S.11(1)

In comparing the regulatory structures governing data protection and privacy in Kenya and Tanzania, it becomes evident that there are significant differences between the two countries. While Kenya has established comprehensive data protection laws and an independent regulatory body, Tanzania lags behind with weak legislation and a lack of an independent authority. These disparities highlight the need for Tanzania to strengthen its regulatory framework to ensure the efficient protection of data and privacy rights. Evaluation of similarities and differences in the independence of data protection authorities in Kenya and Tanzania. It is evident that there are distinct similarities and differences in the independence of data protection authorities in Kenya and Tanzania. Both countries have established regulatory structures to oversee data protection and privacy, although Kenya's authority demonstrates a higher level of autonomy. However, both authorities face challenges in terms of funding, resource allocation, and political interference, which can hinder their ability to effectively protect citizens' data privacy. Overall, there is room for improvement in ensuring the complete independence of these authorities to enhance data protection and privacy in East Africa.

4. Conclusions

The independence of data protection authorities in Kenya and Tanzania plays a pivotal role in upholding citizen's data privacy and security rights. This study has assessed the independence of the regulatory structures governing data protection and privacy in Kenya and Tanzania. The formal way of assessing the data protection Authorities' (DPA's) independence was done by assessing the textual provision of the Kenyan and Tanzanian Personal Data Protection Act. A comparative study between powers of data protection and privacy authorities under the Data Protection and Privacy Act in East African countries was critically made referring to both laws in the particular countries. The assessment under the Act involves evaluating the degree to which the data protection regulations are enforced by closely examining the principles of data protection and privacy. These Acts seem to allow for potential interference from external bodies due to the absence of proper safeguards in the decision-making process of these authorities. It is important to note that without adequate oversight, these bodies may not be able to ensure their independence. This issue was explored further in this study, as the specific Acts vary between countries (Kenya and Tanzania), leading to differences in their application as well. According to the Tanzania Personal Data Protection of 2022, the office's funding will come from the parliament's budget and other grants and gifts. However, there are concerns about the independence of these authorities. The Kenya Data Protection Act 2021 has provisions for the powers of the data commissioner to conduct investigations on data subject complaints. The commissioner can also seek professional assistance and depend on the national assembly for funds. This limits the independence of the data protection authorities. These findings indicate that while both countries have made efforts to establish regulatory frameworks, there exist significant challenges in maintaining adequate independence. Factors such as political influence, limited financial resources, and inadequate enforcement mechanisms undermine the effectiveness of these regulatory bodies. It is, therefore, crucial for policymakers to strengthen the independence of these institutions to ensure the protection of data and privacy in East Africa. Both countries must continuously work towards strengthening the autonomy of their DPAs, ensuring adequate resources, and promoting public awareness to safeguard individuals' data rights in the digital age.

Funding: This research received no external funding.Conflicts of Interest: The authors declare no
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations or those of the publisher, the editors and the reviewers.

References

[1] Available at https//www.dlapiperdataprotection.com Data Protection Laws of the World 2023
[2] Available at https://car.dole.gov.ph security of tenure and causes of termination Regional Office CAR August 2, 2023
[3] Available at www.accessnow.org Data Protection in Kenya How is this right protected Part II analyzing the Kenyan Data Protection Act 2019; THE BAD Oct 2021
[4] Data Protection and Privacy Act in Kenya, Uganda, Rwanda and Tanzania 2019, 2021, 2022 respectively
[5] Data Protection and Privacy Laws identification For Development ID4D *https://id4d.worldbank.org*
[6] Explained under section 26 of Data Protection Act No. 24 of 2019
[7] Forum.com www.jamiiForums.com 13 July 2023
[8] Greenleaf. G Independency of data privacy authorities (part1): I International Standards 2011
[9] Githaiga. J and Kurji A. J Kenya: Data Privacy Comparative guide Price water house Coopers Limited 06 Feb 2023
[10] Ibid pg 37
[11] Ibid pg 46
[12] Ibid pg 46
[13] Ibid pg 48
[14] Ibid
[15] Ibid pg 44
[16] Ibid
[17] Ibid pg 50
[18] Ibid

[19] Ibid pg 46
[20] Ibid pg 41
[21] Ibid pg 48
[22] Ibid pg 46
[23] Ibid pg 29
[24] Ibid
[25] Ibid
[26] Ibid pg 2
[27] Kenya Data Protection Act No. 24 of 2019
[28] Personal Data Protection Guidelines for Africa 2019 https://www.internetsociety.org
[29] Rwanda Personal Data Protection and Privacy Act
[30] S.3 Of Kenya Data Protection Act No. 24 of 2019
[31] s.62-63 part VII of Kenya Data Protection Act No 24 of 2019
[32] s.67 (a) part IX of Kenya Data Protection Act No 24 of 2019
[33] Section 12 of Kenya Data Protection Act No. 24 Of 2019
[34] S.6 (4) Of Kenya Data Protection Act No 24 of 2019
[35] Schutz P.(2012) Comparing Formal Independence of Data Protection Authorities in selected EU comparative perspective IFIP Prime life International Summer School June 2012 Available at https://link.springer.com
[36] The Kenya Data Protection (compliance and enforcement) Regulation Act 2021, the Ugandan Data Protection and Privacy and Regulation 2021 under section 39 of Data Protection and Privacy of 2019, The Tanzania Personal Data Protection and Privacy Act 2022, The Rwanda Utilities Regulatory Authorities (RURA)
[37] Tanzania Personal Data Protection Act Dec 2022 S. 51
[38] Tanzania Personal Data Protection Act Dec 2022 S. 1-2
[39] Tanzania Personal Data Protection Act Dec 2022 S. 1-2 pg 46
[40] Tanzania Personal Data Protection Act Dec 2022 S. 4
[41] Tanzania Personal Data Protection Act 2022, section No 11
[42] Tanzania Personal Data Protection Act Dec 2022 S. 8
[43] Tanzania Personal Data Protection Act Dec 2022 S. 8
[44] Tanzanian Personal Data Protection Act 2022
[45] The General Data Protection Act 2008 Article 52 (1-6) and recital 121
[46] Tanzania Communication Regulatory Authority Act 2003 part 1v (28)
[47] The Kenya Data Protection Act Nov 2019 Kenya Gazette Supplements No.181 (Act No. 24
[48] Tanzania Personal Data Protection Act Dec 2022 S.51 (a)
[49] The Kenya Data Protection Act Nov 2019 Kenya Gazette Supplements No.181 (Act No. 24 section 6(4)
[50] Tanzania Data Protection Act Dec 2022 S.11(1)

DIOGENESS DIOCLES MGANYIZI's Thesis

ORIGINALITY REPORT

18%	13%	12%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	pure.uva.nl Internet Source	1%
2	nbn-resolving.de Internet Source	1%
3	"Data Governance and Policy in Africa", Springer Science and Business Media LLC, 2023 Publication	1%
4	"African Data Privacy Laws", Springer Science and Business Media LLC, 2016 Publication	1%
5	repository.out.ac.tz Internet Source	1%
6	Submitted to Institute of Technology Carlow Student Paper	1%
7	Robert Walters, Marko Novak. "Cyber Security, Artificial Intelligence, Data Protection & the Law", Springer Science and Business Media LLC, 2021 Publication	1%