



The University of Nairobi

Institute of Diplomacy and International Studies (IDIS)

**Effectiveness of Domestic Data Protection Laws in African Countries: A
Case Study of The Data Protection Law in Kenya**

Eugene Wanekeya

(R50/33958/2019)

Supervisor

Dr. Kenneth Mutuma

**A Research Project submitted in partial fulfillment of the Degree of Master
of Arts in International Studies**

March 2023

Declaration

I, **Eugene Wanekeya** hereby declare that this research project is my original work and has not been presented for a degree in any other University.

Signature: 

Date: 24/3/2023

Name: **Eugene Wanekeya**

Student no. **R50/33958/2019**

This project has been submitted for examination with my approval as University Supervisor.

Signature:



Date: 28/3/2023

Name: **Dr. Kenneth Mutuma**

Abstract

This study sought to evaluate the effectiveness of domestic data protection laws in African countries, with a particular concentration on the recently gazetted Data Protection Law in Kenya, typically referred to as the Kenya Data Protection Act, 2019. The study aimed at achieving three specific objectives namely, establishing whether the domestic data protection law in Kenya was enforceable, to evaluate whether the domestic data protection law in Kenya conformed to international standards and to explore techniques that could be employed to strengthen the domestic data protection law in Kenya. The study was explanatory in nature because effectiveness of domestic data protection laws in African countries and particularly in Kenya, is still a new concept and has not been adequately explained by previous studies that the researcher was able to evaluate. The researcher settled on Nairobi County as the study area, specifically narrowing down the study area to the Nairobi Central Business District, which was home to the key target population that included policy makers, Internet Service Providers (ISPs) and internet users, as at the time the study was being carried out. Basically, the sample size was made up of Members of the National ICT Steering Committee, Members of the top ten ICT companies in Nairobi, members of the main internet distributors in Nairobi, and the Ministry of ICT in Nairobi County. A structured questionnaire with a mix of open-ended questions as well as closed ended questions was used and complemented by an interview guide. For the purpose of data analysis, the study employed descriptive as well as inferential statistics. Based on findings from the study, it was evident that Kenya's domestic data protection legislation is enforceable and can be properly implemented if a significant number of Kenyans are educated on best practices to be adhered to when handling personal data, including data processing and data protection, and if all relevant stakeholders were actively involved in the process of developing a roadmap for implementation of these laws. The study also found that Kenya's domestic data protection law, that was enacted in 2019 is largely influenced by the General Data Protection Regulation (GDPR) that was adopted by member states of the European Union (EU) in 2016 and currently stands as the gold standard in data protection regulations. The results also show that the Kenya Data Protection Act of 2019, is a thorough data protection law that safeguards individuals' personal data. The researcher was also able to establish that the African Union (AU) Convention on Cyber Security and Personal Data Protection, a treaty developed by member states of the AU to facilitate a unified approach to addressing cyber security and data protection for African states, has only been ratified by a very small number of African nations (seven as at the time of this study), with Kenya among the 48 countries in the AU yet to ratify the treaty. The researcher therefore came to the conclusion that data protection cannot be the responsibility of a single sovereign state, single international agreement, or single global treaty, and that Africa's or Kenya's success in safeguarding personal data of its citizens can only be ensured through one unified AU authority, such as adoption of the AU Convention on Cyber Security and Personal Data Protection, which cooperates with other international authorities like the GDPR in the EU. As part of the recommendations of this study, it would be prudent for policymakers, lawmakers, and all other key industry stakeholders to raise public knowledge about the Personal Data Protection Act of 2019, and to compare it to the worldwide best practices such as the GDPR to create a unified and simple regulatory framework. Overall, the findings support the liberalism theory, which is based on the idea that cooperation among states, as well as between states and non-state actors, can and should be anchored, organized and formalized in institutions, thereby promoting cooperation and conformity to predetermined agreements without the need for a hegemonic player.

Abbreviations

AU	The African Union
CBD	Central Business District
CEMAC	The Central African Economic and Monetary Community
ECCAS	The Economic Community of Central African States
ECOWAS	The Economic Community of West African States
EU	The European Union
GDP	Gross Domestic Product
GDPR	The General Data Protection Regulation
ICT	Information Communication Technology
ISP	Internet Service Provider
KNBS	The Kenya National Bureau of Statistics
MSME	Micro, Small and Medium Enterprise
NACOSTI	The National Council of Science and Technology
ODPC	Office of the Data Protection Commissioner
POPIA	The Protection of Personal Information Act
SADC	The Southern African Development Community
SPSS	The Statistical Program for Social Sciences
UNCTAD	The United Nations Conference on Trade and Development

Dedication

This research project is first and foremost dedicated to God Almighty, my creator, through whom I draw an inner source of inspiration and self-motivation, as well as the insight, knowledge, and understanding needed to complete my work. Special dedication also goes to my wife, Lavenda, and son, Sekani, who have been a constant source of joy, support, and encouragement to me as I struggled to find a work-school-life balance during my graduate school years.

Acknowledgement

I could not have successfully completed this study report without the guidance of my supervisor, Dr. Kenneth Mutuma. His zeal, intelligence, and meticulous attention to detail, particularly on matters of international law, have been an inspiration to me, and have been critical in keeping me on track with my study. I also wish to thank Vincent Muindi, a professional acquaintance whose expertise in data collection and analysis was critical in assisting me to complete the research technique component of my project report flawlessly. I also express my gratitude to my class representatives, Stephen Nyaga, Cicily Muiruri, and Diana Nkatha, for keeping me informed of the necessary processes and timetables for the completion of my research study.

Table of Contents

Declaration	ii
Abstract	iii
Abbreviations	iv
Dedication	v
Acknowledgement	vi
List of Tables	ix
List of Figures	x
CHAPTER ONE: INTRODUCTION	1
1.1 Background of the Study.....	1
1.2 Statement of the Problem.....	5
1.3 Research Objectives	7
1.4 Research Questions	7
1.5 Hypothesis of the study.....	7
1.6 Justification of the study	8
1.7 Chapter outline.....	8
CHAPTER TWO: LITERATURE REVIEW	9
2.1 Introduction	9
2.2 Theoretical Framework	9
2.2.1 Liberalism Theory	9
2.3 Empirical Review	11
2.3.1 Enforcing Domestic Data Protection Laws	11
2.3.2 Conforming Domestic Data Protection Laws to International Standards	14
2.3.3 Techniques that can be Employed to Strengthen Domestic Data Protection Laws ...	16
2.4 Summary of the Knowledge Gap	18
CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY	20
3.1 Introduction	20
3.2 Research Design.....	20
3.3 The Study Area.....	21
3.4 Target Population	21
3.5 Sample Size and Sampling Procedure.....	22
3.6 Data Collection.....	23
3.7 Data Analysis Techniques	25

3.8 Ethical Considerations.....	26
CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION	27
4.1 Introduction	27
4.2 Response Rate	27
4.3 Respondents’ Demographics	28
4.4 Response on Domestic Data Protection Law Enforceability	32
4.5 Similarities between Kenya Data Protection and International Data Protection Laws	35
4.6 Techniques that can be employed to strengthen the domestic data protection law.....	38
4.7 Inferential Statistics.....	39
4.8 Discussion	42
CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS	47
5.1 Introduction	47
5.2 Summary of Findings	47
5.3 Conclusion.....	48
5.4 Recommendation.....	49
5.5 Limitations of the Study	50
5.6 Suggestions for Further Research.....	50
References	51
Appendix 1: Map of Nairobi County	53
Appendix 2: Research Authorization University of Nairobi	54
Appendix 3: Research Authorization NACOSTI	55
Appendix 4: Questionnaire	56

List of Tables

Table 1: Target Population.....	21
Table 2: Sample size	23
Table 3: Response Rate.....	27
Table 4: Case Processing Summary.....	39
Table 5: Difficulty enforcing domestic data protection law * YES/NO Cross tabulation.....	40
Table 6: Chi-Square Tests.....	40
Table 7: Case Processing Summary.....	40
Table 8: Domestic data protection law conform to international standards * YES/NO Cross tabulation.....	41
Table 9: Chi-Square Tests.....	41
Table 10: Case Processing Summary.....	41
Table 11: Techniques available that Kenya can use to strengthen its domestic data protection law * YES/NO Cross tabulation	42
Table 12: Chi-Square Tests.....	42

List of Figures

Figure 1: Conceptual Model	18
Figure 2: Frequency Distribution of Respondents by Gender	28
Figure 3: Frequency Distribution of Respondents by Age	29
Figure 4: Frequency Distribution of Respondents by Education Level.....	30
Figure 5: Frequency Distribution of Respondents by Field of Expertise	31
Figure 6: Frequency Distribution of Respondents by Number of Years in the Specific Field	32
Figure 7: Respondents on Familiarity with the Kenya Data Protection Act 2019.....	33
Figure 8: Respondents on Domestic Data Protection Law Enforceability	34
Figure 9: Respondents on Domestic Data Protection Law Similarities with International Data Protection Laws	36
Figure 10: Respondents on Relevance of Kenya Data Protection Act for Kenya as a Sovereign State.....	37
Figure 11: Respondents on Benefit to African Countries Pursuing Data Protection through one unified African Union (AU) Authority	38

CHAPTER ONE: INTRODUCTION

Are you aware that around 12 per cent of international trade takes place online? Over the last half-century, the proliferation of internet technology has been the primary driver of globalization, resulting in the formation of multinational corporations that develop and operate the technologies that enable globalization of trade, security, politics, education, transportation, and media, among other things. These global businesses function independently of governments, and the majority of them have grown rapidly to the point that they now wield more influence than governments. Nations have attempted to limit multinational businesses' dominance through legislation, but it has been a tall order because technology advances quicker than states can legislate. However, it has recently been realized that the key to controlling any technology is the data that drives the technology, not the technology itself. As a result, states have shifted their focus to enacting legislation pertaining to data protection in order to reclaim control from multinational corporations.

As a result, this research sought to examine the effectiveness of domestic data protection laws in African countries using a case study of Kenya's recently enacted data protection law. The goals were to determine whether Kenya's domestic data protection law was enforceable, to assess whether Kenya's domestic data protection law met international requirements, and to investigate approaches that could be used to strengthen Kenya's domestic data protection law. The researcher was particularly interested in determining whether African countries, as sovereign entities, would have sufficient leverage to enforce adherence to domestic data protection legislation, particularly by multinational corporations, the majority of which made profits that far exceeded the GDP of most African countries. Was it thus wiser for African countries to bolster their bargaining power by pursuing data protection through a united African Union (AU) data protection authority?

1.1 Background of the Study

Consumers International (2018)¹ defines data protection as the safeguarding of any personal information that may make it possible to achieve a positive identification of a living person. The information typically includes but is not limited to a person's name, photographs or video footage. Commonly used identifiers on various platforms on the internet such as IP and email

¹ Consumers International. *The state of data protection rules around the world: A briefing for consumer organizations*. 2018

addresses, phone numbers, date of birth and home addresses also fall under the category of personal data. A data protection legislation, on the other hand, is a law that governs how a government institution, or a private organization can access and use an individual's personal information. Most modern internet-based technologies, such as e-commerce platforms, social media platforms, and e-mail platforms, among others, are largely reliant on data since they provide the mechanism through which individuals, governments, and commercial companies transmit information across international borders.

The 1990s notably represent the dawn of the digital era which brought forth plenty of enthusiasm on the positive transformation that emerging technologies would bring on various sectors of society. The thought of being able to communicate in real-time, and access as well as share information instantaneously across geographical borders, brought new meaning to the concepts of democracy and freedom, as it was set to pioneer a new age of increased openness as well as transparency in communication, international trade and business. Unfortunately, technology proved to be a double-edged sword, as internet-based platforms such as social media networks and e-commerce sites, significantly contributed to the disregard for personal data and increased the prevalence of propaganda which is today commonly referred to as fake news or deep fake content. This was further compounded by the rapid rise in cybercrime, and these factors have ended up dampening the early enthusiasm for a connected world.² As a result, governments continually found themselves under pressure to protect their citizenry from the ills of rapid advancements in technology and this could only mostly be done through legislation that not only guided and protected citizens as they interacted with these emerging technologies, but also created an enabling environment for the organizations developing these technologies to thrive from a business perspective. Governments therefore would often find themselves having to strike a balance in multiple interdependent areas such as ensuring that regulations that are developed, address emerging global issues such as data protection, cyber security and cybercrime, without infringing on individual liberties of their citizenry as they use technologies driven by the internet, and also did not impede on the ability of enterprises that develop these technologies to thrive.

A report prepared and presented by the United Nations Conference on Trade and Development (UNCTAD) in 2016³, revealed that goods, services, as well as finances worth

² Kurbalija. *An Introduction to Internet Governance (6th ed)*, 2019 pg. 4

³ UNCTAD. *Data protection regulations and international data flows: Implications for trade and development* 2016. Pg 12

close to \$30 trillion were transferred across borders, with transactions over e-commerce platforms accounting for 12 per cent of this figure. This figure represents the extent to which internet-based commercial platforms owned and run by multinational firms are beginning to actively contribute to international trade. This study sought to emphasize on data privacy as a significant topic of interest in this burgeoning digital economy, warning that a lack of adequate protection will certainly harm the business by lowering consumer confidence.

This has elevated data protection to the forefront of international law, as it is critical to facilitating international trade in this era of globalization and the rise of digital economies fueled by multinational enterprises. As Brown and Ainley (2005)⁴ rightly note, that currently, one of the biggest topics of discussion in international relations revolves around the world economy, and the pursuit by state as well as non-state actors to not only manage it but also regulate it. Since international trade forms a critical component of international relations, states need to actively collaborate more with multinational corporations and international non-governmental organizations which form the biggest batch of non-state actors, in their response to the challenges brought about by globalization taking into consideration the critical role they play as an enabler of globalization through technologies and resources they provide. One facet of this collaboration is the development of policies to bring order to international commerce, with a particular focus on the digital economy, while remaining true to trade liberalization principles.

The General Data Protection Regulation, commonly referred to as GDPR, was enacted in the EU in response to the need to secure personal data belonging to European individuals who are actively involved in the digital economy. This legislation was enacted in mid-2018 to provide a regulatory mechanism that addresses emerging challenges associated with the digital age by strengthening the rights of the consumer whose data drives the digital economy, strengthening the regulatory capacity of EU regulators responsible for enforcing data protection regulations, and ensuring accountability by businesses, both national and multinational, who collect, store or are responsible for storing, and make use of personal data that belongs to citizens from EU member states (Consumers International, 2018)⁵.

⁴ Brown, Chris. and Ainley, Kirsten. *Understanding international relations, 3rd Edition*. 2005 Pp. 141

⁵ Consumers International. *The state of data protection rules around the world: A briefing for consumer organizations*. 2018. Pg 1

Multinational corporations operating within the EU are now more accountable. UNCTAD (2016)⁶ notes that the comprehensive nature of the GDPR and the fact that it has been able to balance the interests of consumers, regulators and businesses within the EU has prompted governments outside of the EU to adopt data protection legislation modeled on the GDPR. As governments and corporate organizations embrace ICTs, this is part of an effort to develop a regulatory framework to oversee online activities, as socio-economic as well as political activities are progressively migrating to the online space.

The initial success of the GDPR in enhancing compliance to the tenets of data protection by state as well as non-state actors operating within the EU, can be credited to the sudden steady drive by African states to begin the push to develop and enact data protection laws. It is noteworthy that almost half of Africa's 55 countries have enacted or are in the process of adopting some form of regulation that will enhance their ability to provide mechanisms to ensure the protection of personal data of their citizenry⁷. The adoption of the Convention on Cyber-security and Personal Data Protection, referred to as the Malabo Convention in short, by the AU in 2014, was touted as a game changer as it had the potential to be an extremely significant step in the right direction for the African continent. However, almost a decade since it was adopted, a paltry 14 out of the 55 states within the AU have appended their signature to the pact, with only seven going a step further by ratifying it. This is significant because for this convention to take effect, a minimum of 15 AU member states must not only append their signatures to the document, but also ratify it, and thus far, this has been a very slow process.

The Economic Community of West African States (ECOWAS) is one of the regions in Africa that has thus far managed to develop and enact a binding regional agreement on data protection that has been enacted by 11 of its 15 member states. This agreement was achieved through the 2010 Supplementary Act on Data Protection which heavily borrows from the GDPR in the EU, with experts touting it as Africa's only binding data protection agreement that is currently operational.⁸ South Africa on the other hand has enacted two legislations into law that is, the Cybercrimes and Cybersecurity Act of 2021 and the Protection of Personal Information Act (POPIA, 2021), both of which are up to international standards. These

⁶ UNCTAD. *Data protection regulations and international data flows: Implications for trade and development*. 2016. Pg 13

⁷ Gruzd. 'Multi-Stakeholder Initiatives: Lessons Learned'. SAIIA Research Paper. 2018.

⁸ African Union, *African union convention on cyber security and personal data protection* e.pdf, 2019 p. 13.

legislations outline all the rights individuals are entitled to, provided that the data belongs to them, thus promoting the protection of this data as it is made use of by either public or private bodies. These legislations also seek to regulate how personal data flows across international borders, going ahead to mandate data processors to report any cases of data breaches and goes on to impose penalties in the event these laws are violated.⁹

Kenya is among the minority AU countries that have enacted a domestic data protection law which is known as the Kenya Data Protection Act of 2019¹⁰, a data protection law modeled after the GDPR. This Act is the primary legislation through which Kenya is able to ensure the protection of personal data of its citizenry and is anchored on Article 31 c) and d) of the country's Constitution promulgated in 2010, which guarantees the individual's right to privacy.¹¹ This law establishes a legal framework that guides both government and commercial organizations on how to collect, process, store and make use of any personal data that belongs to Kenyan citizens.

1.2 Statement of the Problem

The rapid increase in reported cases of international cybercrime, multinational corporations' disregard for personal data, and the prevalence of deep fake content as well as fake news have necessitated the need for data protection legislation. Currently, the EU is leading this charge having developed and enacted the GDPR, which governs the movement and use of data belonging to EU citizens across international boundaries. Thus far, the EU is one of the bodies that has developed what is considered as the most comprehensive laws on data protection.¹² Due to Africa's rapid growth in internet proliferation which has increased the continent's participation in the global economy and international trade through e-commerce and other platforms in the cyber space that require transfer of data and information across international borders, the AU finds itself with an increased need to follow in the footsteps of the EU by adopting some of the best practices in data protection and cyber governance that the EU has already established.¹³

⁹ *Ibid.*, p. 24

¹⁰ The Kenya Data Protection Act 2019

¹¹ The Constitution of Kenya 2010

¹² Brzezinski. 'Moving into a technetronic society,' in *Information Technology in a Democracy*, Harvard University Press. Cambridge, Mass., 2017, pp. 161–7.

¹³ Chander and Uyen, 'Data nationalism', *Emory Law Journal*, 3rd Edition, Pg. 64, 2015,

On this note, Africa has registered considerable progress in development of regional model legislation on data protection and cyber governance such as the Cybersecurity Guidelines enacted by members of the ECOWAS, The Data Protection Model Law enacted by members of ECCAS, the Directives on Cybersecurity enacted by members of CEMAC and the model law on data protection, e-transactions and cybercrime enacted by members of SADC. Domestically as well, almost half of the 55 states in Africa have developed some form of legislation on data protection.¹⁴ This therein lies the problem. Whereas there exists the Malabo Convention, a treaty that was developed by the AU back in 2014, African states have opted not to ratify this treaty and instead adopted a fragmented approach of developing other domestic and regional laws on data protection that are not in harmony with the Malabo Convention due to their failure to ratify it.

The failure by AU member states to ratify the Malabo Convention has primarily been blamed on lack of political will as a paltry 14 out of the 55 members of the AU have appended their signatures to this convention, with only seven states going a step further by ratifying it. It is noteworthy that eight years down the line, this treaty is yet to come into force, as the requirement for at least 15 states to ratify it, for the treaty's provisions to come into force, is yet to be met.¹⁵ There is therefore a clear contrast between the EU's and AU's approach to data protection legislation, as AU states seem to prioritize their sovereignty over adopting a unified data protection framework that covers all members. In fact, the AU's approach focuses on advising its members to develop their own domestic data protection and cybersecurity laws.¹⁶

This study was therefore motivated by knowledge gaps in the previous related studies done in Kenya. Despite lack of sufficient empirical evidence, available studies such as Orero & Nduta (2020), Issaias (2019), and King'ori (2020) failed to demonstrate the enforceability of local data protection legislation and if it complies with international standards. The studies did not look into techniques that could be used to strengthen Kenya's legal framework. As a result, this formed a sound foundation for the current topic. Using Kenya's domestic data protection law as the case study, this research assessed the efficacy of domestic data protection laws in African countries. The study answered the question of whether it will be

¹⁴ Consumers International. *The state of data protection rules around the world: A briefing for consumer organizations*.

¹⁵ Murithi, 'The African Union at ten: An appraisal', *African Affairs*, 111, 445, 2012, p. 663

¹⁶ African Union, 'List of countries which have signed, ratified/acceded to the AU Convention on Cyber Security and Personal Data Protection'. 2020

possible for AU member states to formulate strong and enforceable laws as individual sovereign states or whether AU will be much better off following the direction of the EU by formulating a unified law under an AU regime for the entire continent, which will be enforced by a central AU authority.

1.3 Research Objectives

The general objective of this study was to evaluate the effectiveness of the domestic data protection law in Kenya.

The specific objectives were:

- i. To establish whether the domestic data protection law in Kenya was enforceable.
- ii. To evaluate whether the domestic data protection law in Kenya conformed to international standards.
- iii. To explore techniques that could be employed to strengthen the domestic data protection law in Kenya.

1.4 Research Questions

This study sought to give answers to the following interrelated research questions:

- i. Is the domestic data protection law in Kenya enforceable?
- ii. Does the domestic data protection law in Kenya conform to international standards?
- iii. Are there techniques that can be employed to strengthen the domestic data protection law in Kenya?

1.5 Hypothesis of the study

1. **H₀**: Kenya will have difficulty enforcing its domestic data protection law especially when non-compliance is by a multinational corporation.
2. **H₁**: Kenya's domestic data protection law will conform to international standards as it is largely based on the EU's GDPR.
3. **H₁**: There are techniques available that Kenya can use to strengthen its domestic data protection law.

1.6 Justification of the study

The findings that have been obtained from this study will undoubtedly provide value to a number of parties including policy makers, academia and the general public. For policy makers, especially those involved in formulating policy that has an impact on international trade, the study may help identify methods that can be used to formulate stronger policies and the value of developing policy that is compatible with other international legal regimes. For academia, the fact that technology over the past half century has rapidly developed and intertwined with multiple sectors of society resulting in insufficient academic knowledge on the same, this study will help provide more academic information and reference material specifically in the area of data protection legislation, how it impacts on international trade and in shaping cooperation among states as well as with non-state actors. As for the general public, data protection touches on them directly because most of the data being collected and used by state and private corporations belongs to citizens. Therefore, the public may benefit by having more knowledge on how data protection will impact their lives.

1.7 Chapter outline

Chapter One: Covers the background and introduction of domestic data protection law, looking at how and whether Kenya has been able to enforce these laws.

Chapter Two: Is a review and analysis of available literature and looks at how and whether Kenya has been able to conform its domestic data protection law to international standards. The chapter also discussed the techniques that Kenya has been able to employ in order to strengthen its domestic data protection law.

Chapter Three: Highlights the research methodology and techniques used in the course of this study.

Chapter Four: Provides an analysis of the data collected in the course of this to evaluate the effectiveness of the domestic data protection law in Kenya.

Chapter Five: Highlights the key summaries and conclusions, providing recommendations from the researcher and suggestions for possible further research.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter covers three main sections: The theoretical framework, empirical review, and the conceptual framework of the variables, which highlights the important variables examined in the study. The chapter looked at history and current studies on data protection legislation from a global, regional, and Kenyan viewpoint as the case study. This chapter also examined the liberalism theory in international relations, which was a major focus of this study.

2.2 Theoretical Framework

2.2.1 Liberalism Theory

The researcher primarily based this study on the Liberalism theory in international relations. Scott Burchill, et al. (2005)¹⁷, point out that the liberalism theory is based on the premise that cooperation among states as well as between states and non-state actors can and ought to be organized, anchored and formalized in institutions. Here in this example, institutions refer to the sets of norms that control states as well as non-state actors' behavior in specific policy areas. Proponents of this idea believe that by cooperating, it is feasible to ensure conformity with predetermined agreements without the need for a hegemonic player to do so. This argument supports the researcher's claim that, similar to the EU, AU countries should approach data protection legislation as a single AU institution rather than as distinct sovereign states, as is now the case.

Scott Burchill, et al. (2005)¹⁸, however, devotion to the ideas of free trade and an open market free of government intervention is a vital component of the liberalism ideology, according to the author. On the one hand, calling for the development of strong institutions to improve adherence to legislation while still advocating for a free market appears to be a contradiction. Proponents of this idea, on the other hand, are open to the government assisting in the establishment of measures to prevent anarchy. This is why it is critical for states and non-state actors to work together to establish independent institutions that are concerned with the total welfare of all parties involved rather than the interests of particular entities.

¹⁷ Scott Burchill, et al, *Theories of International Relations, 3rd Edition*. 2005. Pp. 57-66

¹⁸ Ibid

The GDPR as prescribed by the EU is a stronger and effective legislation because the institution of the EU draws its strength from its combined membership which combines economic and political power of its individual members. This has assured the existence of a powerful EU data protection authority with the clout to penalize any multinational firm that attempts to break the rules. The interests of EU consumers, international firms, and EU member states are all protected under this arrangement. It may not be a win-win situation for all parties involved, but it is a fair system that does not favor the government over non-governmental entities. This is a perspective supported by Brown and Ainley (2005)¹⁹, who are of the opinion that through the liberalist approach it is possible to reconcile international economics and national interests by creating harmony in these interests. This is made clear by the fact that the GDPR is meant to streamline the transfer of data and information across transnational borders while also protecting the rights of individuals, while at the same time safeguarding interests of corporations with operations within the EU and the individual member states of the EU.

As the rest of the international community seeks to catch up with the EU by formulating data protection legislation, Consumers International (2018)²⁰ proposes the harmonization of these laws globally to enhance cooperation, therefore reducing confusion and making it easier to resolve cross-border issues of data protection. This view is supported by Deloitte (2017)²¹ that points out that as technology continues to advance, increasing cross-border trade, data protection legislation that complies with and is compatible with international standards is imperative. As they begin the process of establishing domestic data protection legislation, AU member states should keep this perspective in mind. As a result of globalization, increasing cooperation among states and non-state entities appears to be the most highly recommended strategy to help address the challenges associated with cross-border transfer of data and information, therefore bolstering the researcher's argument that members of the AU should tackle the subject of data protection as a unified entity rather than individually.

¹⁹ Brown, Chris and Ainley, Kristen *Understanding international relations, 3rd Edition*. 2005 Pp. 22, vol 141.

²⁰ Consumers International. *The state of data protection rules around the world: A briefing for consumer organizations* 2018. Pg 5

²¹ Deloitte. *Privacy is Paramount: Personal Data Protection in Africa*. 2017. Pg 3

2.3 Empirical Review

This section examined the empirical literature currently available in the field of data protection legislation, as well as the body of knowledge that exists and its implications for this study.

2.3.1 Enforcing Domestic Data Protection Laws

An empirical analysis conducted by Nikkei (2019)²² shows that it will be a tall order putting in place global agreements that safeguard personal data and information, as well as internet freedoms, primarily because there exist significant ideological differences among states. Case in point, is a state like China, that strongly believes in the concept of cyber sovereignty whereby the government has absolute power to regulate access to and use of internet within its jurisdiction, without any external interference from either state or non-state actors.²³ This has essentially meant that the government has the power to completely cut off or limit its citizens and corporations operating within its jurisdiction from accessing internet services or specific internet-based platforms such as websites and search engines. Some experts have even expressed concern that China is likely to influence countries including those in Africa that are beneficiaries of its global development initiative dubbed the China Belt and Road Initiative, to adopt similar ideology as they receive infrastructure and technological support from China.²⁴

Also of note is the fact that many of the current laws on data protection in use around the globe have slight differences that make it difficult for them to be interoperable across borders. Parshotam²⁵ cites an example of how different countries define the rules of data collection, processing and storage in their respective jurisdictions. Particularly, is the subject of which type of data must be processed and stored in servers within a country's jurisdiction or servers outside of a country's jurisdiction but in a country with equal or better regulatory framework. For a country like Russia, this rule applies to all personal data, for Sweden and Nigeria, this

²² Nikkei Asian Review, 'Beijing exports "China-style" internet across Belt and Road'. 2019

²³ *Ibid.*

²⁴ Orji. 'The African Union Convention on Cybersecurity: A regional response towards cyber stability?' in *Masaryk University Journal of Law and Technology*, 12th Edition, Vol2, 2018 pp. 92.

²⁵ Parshotam. 'Can the African Continental Free Trade Area Offer a New Beginning for Trade in Africa?' Johannesburg: SAIIA (South African Institute for International Affairs), 2018. Occasional Paper no. 280.

rule applies to all government data, whereas in USA and Australia, this rule applies to all health records.²⁶

According to a report by Deloitte²⁷, it will be very difficult for businesses across the globe to engage in international trade if they are not compliant with international legislation on data protection legislation. This is because non-compliance with these laws can obstruct an organization's capacity to move data globally, which is a critical component of international trade, particularly in the rising digital economy. This trend is particularly relevant for multinational corporations with a global footprint, according to the report, because their businesses are heavily reliant on their ability to conduct business across international borders, with cross-border data transfer being a key component of these operations. This essentially means that data protection authorities will use this as leverage to enforce compliance with data protection legislation.

It is worth noting, however, that in order for a data protection body to enforce such compliance, it must have the ability to do so. It is insufficient to have legal authority alone. It is vital to have the ability to sanction both state and non-state actors who violate data protection regulations. Deloitte (2017)²⁸ agrees, stating that bolstering the ability of data protection authorities in the EU, China, Japan, and Australia, among others, to be able to enforce laws on data protection, is currently a major theme, owing to the fact that these authorities have previously proven insufficient in their ability to sanction parties who have broken these laws. In reality, the United States of America is lauded as the sole authority that has so far been successful in enforcing data privacy rules to some extent, relying on hefty penalties and sanctions as a deterrent.

UNCTAD (2016)²⁹ points out the challenge of determining jurisdiction as a major issue in law, especially where data protection is concerned. Because data travels across international borders and there is currently no one universal data protection agreement, defining jurisdiction can be difficult. This is exacerbated by the globalization problem, which has resulted in the emergence of multinational corporations whose operations are not restricted

²⁶ Turianskyi, 'Balancing Cyber Security and Internet Freedom In Africa', Johannesburg: SAIIA (South African Institute for International Affairs), 2018. Occasional Paper no. 275.

²⁷ Deloitte. *Privacy is Paramount*

²⁸ Ibid

²⁹ UNCTAD. *Data protection regulations and international data flows: Implications for trade and development*. 2016. Pg 31

by physical borders. As observed by Consumers International (2018)³⁰, this is being corrected by the establishment of legal frameworks such as the GDPR, which is being utilized as the perfect tool to widen the jurisdiction of the EU's data protection authority, allowing it to enforce compliance across the entire EU.

The GDPR has established a single central body in the EU with the right to inflict harsh penalties on state and non-state actors who do not follow the law, regardless of whether they are based in the EU. The GDPR empowers the EU's data protection authorities to punish any party that handles personal data belonging to an EU citizen. The fact that EU member states are working together on this ensures that the GDPR regime has the ability, resources, and political support to successfully implement its legal rules (Consumers International, 2018)³¹.

In Africa however, the fact that members states of the AU are approaching data protection laws as sovereign states, it is still unclear whether these states will have the ability to successfully enforce these laws. According to Deloitte (2017)³² there are considerable legislative discrepancies among African countries when it comes to data privacy regulation, which will inevitably lead to enforcement and compliance challenges. Issues of jurisdiction, capacity, resources, and political support will undoubtedly arise, and the AU's lack of a single legal regime may disfavor individual member states, making compliance impossible to enforce. This disconnected approach is likely to generate loopholes that allow multinational firms to breach individual AU member states' domestic data protection legislation.

It will be fascinating to assess the enforceability of Kenya's data protection legislation now that they have taken effect. While the Kenyan data protection authority will have the capacity to penalize local firms that handle citizen data since they fall within its jurisdiction,³³ multinational corporations situated outside of Kenya may face a different situation. It may thus be wiser for Kenya and the AU membership as a whole to learn from the EU's experience and follow in its footsteps, given the EU has a comprehensive model that has proven to be beneficial thus far. Kenya and other AU members may be better able to enforce adherence to their domestic data protection legislation if the AU adopts a unified data protection regime.

³⁰ Consumers International. *The state of data protection rules around the world: A briefing for consumer organizations*. 2018. Pg 1

³¹ Consumers International. *The state of data protection rules around the world: A briefing for consumer organizations*. 2018. Pg 5

³² Deloitte. *Privacy is Paramount: Personal Data Protection in Africa*. 2017. Pg 8

³³ The Kenya Data Protection Act 2019

2.3.2 Conforming Domestic Data Protection Laws to International Standards

UNCTAD (2016)³⁴ acknowledges the increasing prominence of the information economy and the opportunities that lie therein especially when it comes to international trade. However, in order to enable states and non-state actors maximize on these opportunities, then they need to formulate internationally compatible data protection regimes that put into effect a conducive ecosystem for all parties to freely participate in cross border transactions. According to Consumers International (2018)³⁵, the GDPR is now the world's strongest data protection framework and should serve as a model for other countries' domestic data protection regulations. The GDPR is written in a way that it empowers the data protection authority in the EU to compel compliance by multinational enterprises as well as states both inside and outside the EU.

A descriptive research done by Murithi (2020)³⁶, stated that the best solution to data protection may be the regional approach. According to the study³⁷, the EU, with its 27 member countries, gives a perfect example of what can be achieved through unity. The idea that all EU member states can commit to sharing similar economic and political principles, is the primary reason as to why the EU has been able to put in place unified regulations and policies within its single market. This culminated in the enactment of the GDPR, which was a first attempt at putting in place uniform rules adhered to by member states of a single political and economic community, a factor that has seen the EU to be regarded as a norm entrepreneur in cyberspace.³⁸ "*A normative or value-driven institution that encourages its constituency to uphold a set of standards for the development of the livelihood of individuals who fall under the jurisdiction or authority of that constituency.*" according to the definition.³⁹

One of the key aspects of the GDPR is its compatibility with other legal regimes. The European Commission and the US Department of Commerce designed and adopted an EU-US Privacy Shield Framework, meant to offer guidance to companies on both sides of the

³⁴ UNCTAD. *Data protection regulations and international data flows: Implications for trade and development*. 2016. Pg 4

³⁵ Consumers International. *The state of data protection rules around the world: A briefing for consumer organizations*. 2018. Pg 3

³⁶ Murithi, 'The African Union at ten: An appraisal', *African Affairs*, 111, 445, 2012, p. 667

³⁷ *Ibid.*, p. 673.

³⁸ Schwab, *The Fourth Industrial Revolution*, 2016, New York: Crown Business.

³⁹ Doninioni, 'The geopolitical meaning of Europe's Cybersecurity Act', Istituto per gli Studi di Politica Internazionale (ISPI)

Atlantic on how to comply with the GDPR particularly when personal data is being transferred from the EU to the USA. This is an example of close collaboration between the US and the EU (Consumers International, 2018).⁴⁰ This is a policy that has been put in place to help transatlantic trade.

UNCTAD (2016)⁴¹, underlines governments' attempts to model their domestic data protection legislation after the GDPR, particularly in developing nations. However, this is proving difficult due to the fact that many countries are taking much too long to pass this law, as well as the financial requirements of implementing and enforcing a data protection regime being beyond their resources. The fact that there is insufficient coordination among states and non-state actors in the policy-making process exacerbates the problem. This is reflective on the fact that according to Consumers International (2018)⁴², only 19 countries in Africa have so far been able to enact data protection and privacy laws which have largely been modeled on the GDPR, with six others having these laws in the draft stage. The 29 remaining states either have no legislation in place or there is no available data on where they are at with data protection legislation process.

It's unclear why the bulk of African countries are dragging their feet, given that the Convention on Cyber Security and Personal Data Protection was adopted by the AU back in 2014, well before the GDPR was enacted by the EU in 2018. It is worth noting, however, that there are active attempts at the regional level to address data protection inside regional blocs. This is being done in a fashion similar to how the GDPR was fashioned by the EU. This strategy has been employed so far by SADC, through a model law that seeks to harmonize regulations in the ICT sector, including data protection, for countries in Sub-Saharan Africa. A similar action is being put in place by ECOWAS through the Supplementary Act A/SA.1/01/10 on Personal Data Protection. Francophone countries in Africa also have membership in the French-Speaking Association of Personal Data Protection Authorities (AFAPDP) that was formed to promote principles of personal data protection in French-speaking countries (UNCTAD, 2016).⁴³

While these efforts are positive strides forward, the fact that the AU membership's attitude to data protection legislation is still divided is concerning. It is still unclear why African Union

⁴⁰ Consumers International. *The state of data protection rules around the world*

⁴¹ UNCTAD. *Data protection regulations and international data flows*. Pg 13

⁴² Consumers International. *The state of data protection rules around the world*. Pg 3

⁴³ UNCTAD. *Data protection regulations and international data flows*. Pg 13

member states are not simply establishing a data protection regime under a unified AU authority, as it will clearly be more practical to conform to such a legal regime to international standards than to try to conform fragmented domestic and regional laws to international standards. Even as Kenya joins other member states of the AU in enacting domestic data protection laws fashioned on the GDPR for purposes of conforming domestic laws to international standards, it is important for Kenya and other AU member states to first strengthen the legal regime under the AU to increase the compatibility of this regime to international standards.

2.3.3 Techniques that can be Employed to Strengthen Domestic Data Protection Laws

Among the initial hurdles that states have encountered as they attempt to introduce data protection legislation is non-compliance by stakeholders, especially multinational corporations. UNCTAD (2016)⁴⁴ notes that one of the primary contributing factors to the non-compliance is that most of these data protection regimes are seldom internationally compatible, and thus calls for the promotion of international data protection regime compatibility. This can be accomplished by avoiding duplication and fragmentation in regional and international approaches to data protection. As a solution, UNCTAD (2016)⁴⁵ recommends that states abandon the idea of pursuing multiple data protection legislation initiatives as individual sovereign entities or regional organizations and instead focus on a single unified initiative or a smaller number of internationally compatible initiatives. States can base their local data protection legislation on a more robust international data protection regime in this way.

Furthermore, UNCTAD (2016)⁴⁶ emphasizes the importance of balancing all legitimate needs and interests of all stakeholders as states formulate data protection legislation, while also respecting the tenets of a liberal market, to ensure that this legislation does not overly restrict international trade. Failure to strike the correct balance could be costly in the sense that the legislation could go against the idea of fundamental rights protection or have a negative impact on international trade and development. States should engage non-state players in a global multi-stakeholder discussion, taking advantage of multilateral institutions

⁴⁴ UNCTAD. *Data protection regulations and international data flows: Implications for trade and development*. 2016. pg 4

⁴⁵ UNCTAD. *Data protection regulations and international data flows*. pg 14

⁴⁶ Ibid

like UNCTAD, which provide a suitable forum for such dialogue. UNCTAD (2016)⁴⁷ notes that a similar approach has worked in other aspects of international law where international and regional organizations have rallied behind a single legal regime to drive compatibility and harmonization, citing the case of cybercrime law, in which over 54 countries from within and outside the EU have signed the Council of Europe Convention on Cybercrime 2001 in an effort to standardize and strengthen cybercrime laws.

In Africa, two reports Deloitte (2017)⁴⁸ and Consumers International (2018)⁴⁹ highlight the glaring legislative disparities and enforcement disparities across the continent, terming this as an area of weakness in data protection laws in the continent that will significantly contribute to non-compliance especially by multinational corporations. The fact that all the 19 AU members that have enacted data protection legislation, and the six that have laws in draft stages are formulating their laws based on the GDPR, is not sufficient. As previously stated, this fragmented approach to legislation contributes to the weakening of these laws. States in the African Union will have a greater chance of strengthening their domestic legislation if the continent has a single data protection system that is compliant and harmonized with other international regimes like the GDPR.

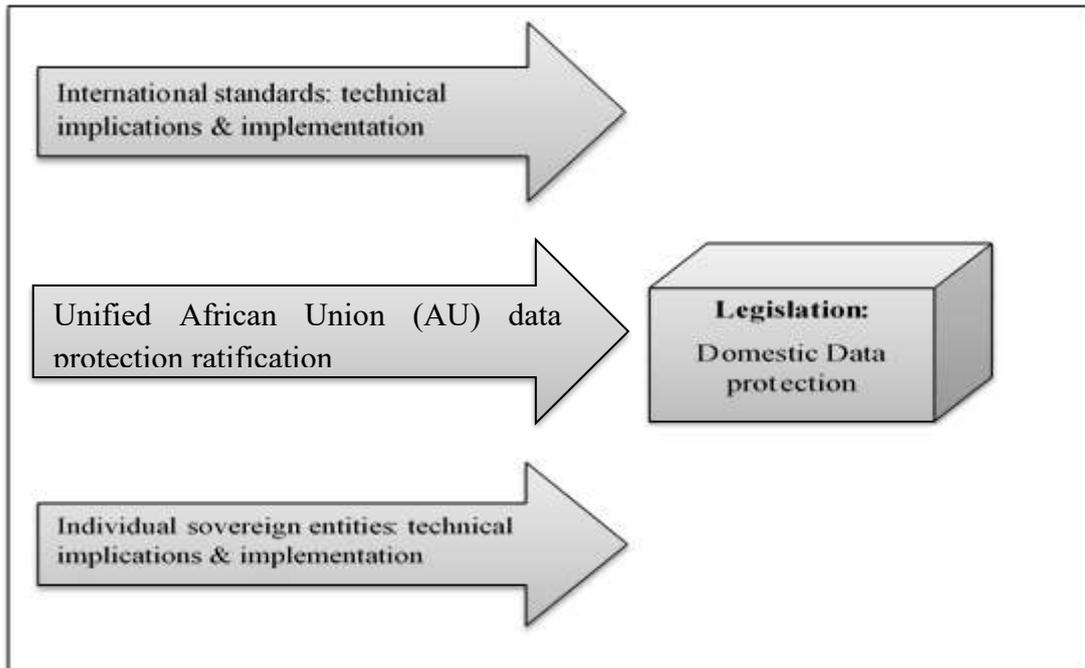
Even as Kenya joins other AU member states in enacting domestic data protection laws modeled after the GDPR in order to bring domestic laws in line with international standards, it is critical for Kenya and other AU member states to first strengthen the legal regime under the AU in order to make it more compatible with international standards. Kenya and other AU member states have a roadmap they can follow in their effort to construct strong data protection legislation, as illustrated by the EU and US actions to formulate data protection regimes that are compatible, thus widening the jurisdiction under which they can be jointly implemented. If AU member states can come up with a legislative framework that is compatible with the GDPR and other international data protection regimes, this will help to expand the jurisdiction under which these rules can be implemented, hence increasing compliance.

⁴⁷ UNCTAD. *Data protection regulations and international*. pg 78

⁴⁸ Deloitte. *Privacy is Paramount: Personal Data Protection in Africa*. 2017. Pg 8

⁴⁹ Consumers International. *The state of data protection rules around the world: A briefing for consumer organizations*. 2018. Pg 3

Figure 1: Conceptual Model



Source: Author (2021)

2.4 Summary of the Knowledge Gap

According to the liberalism theory described in this paper, it is possible to enforce conformity with predetermined agreements through collaboration, like as the AU, without the necessity for a hegemonic player to do so. While some studies advocate for liberalism by advising the AU to learn from the EU which has already put in place and tested the effectiveness of the GDPR with tremendous results and adopt this as a best practice in cyber governance, others in the literature review advocated for illiberalism, such as the concept of 'cyber sovereignty,' synonymous with a country like China which never shies away from promoting this approach. In this context, the reviewed literature also contends that the inability by the 55 member states of the AU to find consensus on an approach to ratify the Malabo Convention, will continue to derail initiatives by the AU when it comes to matters to do with legislation around the cyberspace. In addition, the degree to which a unified approach (liberalism) influence effectiveness of domestic data protection differs among the studies reviewed. The current literature, for example, stated that GDPR is the most ambitious attempt to have some form of control on how both states and multinational corporations use of personal data belonging to the EU citizenry, and that it gives consumers with a range of rights about how data may be used and how they can withdraw their agreement for data usage. Other studies, on the other hand, claim that the GDPR's legislative approach falls well short of establishing

a property rights system in personal data, preventing consumers from exploiting and monetizing data about themselves. According to the examined literature, there has never been general consensus on the optimum way for ensuring the effectiveness of domestic data protection regulations. The studies carried out in different regions contradict each other. It is therefore the lack of empirical evidence that motivated the need for this study.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter highlights and presents the methodology that was applied when undertaking this study. The chapter will delve into the research design, the study area, the target population, and how the sample size as well as sampling procedure was determined. The chapter will also look into the research instruments and procedure for data collection and conclude with the ethical considerations as well as the operationalization of the research variables.

3.2 Research Design

Research design is a term used to make reference to the general approach that the researchers used in the course of conducting the study. The research design will provide a concise and logical method for addressing the specific research issue and this is achieved through collection of data, analysis and interpretation, as well as discussion⁵⁰. The effectiveness of Kenya's domestic data protection law was investigated using an explanatory research design. Explanatory study is conducted to investigate a phenomenon that has not previously been researched or adequately explained⁵¹. The motivation for using explanatory design was due to limited information from existing literature sources in order to try and fill the gaps. Explanatory research as a form of research design, focuses on explaining the study's findings in a timely manner⁵². To achieve this, the following alternate hypothesis were used to explain how enforceability; international standards; and techniques available influence the effectiveness of domestic data protection law in Kenya:

Hypothesis 1:

H₁: Kenya will have difficulty enforcing its domestic data protection law especially when non-compliance is by a multinational corporation.

Hypothesis 2:

H₁: Kenya's domestic data protection law will conform to international standards as it is largely based on the EU's GDPR.

Hypothesis 3:

⁵⁰ Mugenda, & Mugenda, Research methods: *Qualitative and quantitative Approaches*, Africa Center for technology studies, Nairobi, Kenya. 2003.

⁵¹ Foss, Rhetorical criticism: *Exploration and practice*. Waveland Press. Behavioral Sciences, 6th ed. Pycszak Publishing. 2017.

⁵² *Ibid.*

H₁: There are techniques available that Kenya can use to strengthen its domestic data protection law

3.3 Study Area

The study area for this research was Kenya’s Capital City of Nairobi, with particular emphasis on the Central Business District (CBD). The Nairobi CBD is within the larger County of Nairobi which is also one of 47 counties in Kenya, with an estimated population of 4.397 million⁵³. According to Kenya National Bureaus of Statistics⁵⁴, Nairobi has the highest literacy rate in Kenya, at 87.1 percent, making it an appropriate place for the present issue because knowledgeable respondents have a greater ability to handle information and access to information. When compared to other counties, the County has the highest internet connectivity, which means that the majority of citizens are susceptible to data privacy concerns⁵⁵.

3.4 Target Population

Target population can be defined as a large group of goods, objects, or even beings with comparable characteristics that the researcher can use to extrapolate research findings⁵⁶. The target population of this study was composed of internet users, internet providers and policy makers who the researcher opined were knowledgeable enough on data protection.

Table 1 shows how the researcher categorized the target population for this study.

Table 1: Target Population

Name	Population
Members of the National ICT Steering Committee	9
Members of Top ten ICT companies in Nairobi	243
Members of Main internet distributors in Nairobi	186
Ministry of ICT	128
Total	566

⁵³ Kenya National Bureau of Statistic (KNBS), *Kenya Population and Housing Census Results Report*, 2019.

⁵⁴ *Ibid.*

⁵⁵ Kenya National Bureau of Statistic, *National ICT Survey Report*, 2019

⁵⁶ Hunt and Tyrrell, *Coventry University Probability Sampling Techniques*, 2001.

3.5 Sample Size and Sampling Procedure

The statistically representative section of persons or sub-groups generated from the target population to participate in a study is referred to as the sample size⁵⁷. The process or technique of selecting a statistically representative sample of individual research respondents or sub-groups from the target population to participate in a study is known as sampling procedure. A good research sample should be large enough to address the research questions properly.⁵⁸

3.5.1 Sample Size

The study selected a 15 per cent random sample from the target population which is consistent with a recommendation by Mugenda and Mugenda⁵⁹ who states that a sample size of between 10 and 30 per cent is sufficient if well-selected and the elements in the sample are more than 30. To achieve this, Mugenda and Mugenda (2003) proposes the use of Slovin's formula a simplified formula that can be used to calculate sample size for a population of less than 10,000, as shown below:

$$n = \frac{N}{1 + Ne^2}$$

Where: n – sample size,

N – Target population

Ne^2 – Working sample {15% * sample frame (566)}

$$0.15 * 566 = 84.5$$

Based on this, the researcher was confident that with a sample size of 85 respondents, there was a sufficient representation of the target population as demonstrated in Table 2 below:

⁵⁷ Mugenda, & Mugenda, *Research methods: Quantitative and qualitative Approaches*. 2003

⁵⁸ Snedecor, and George, *Design of Sampling Experiments in the Social Sciences*. 1997.

⁵⁹ Mugenda, & Mugenda, *Research methods: Qualitative and quantitative Approaches*, Africa Center for technology studies, Nairobi, Kenya, 2003.

Table 2: Sample size

Name	Sample size
Members of the National ICT Steering Committee	1
Members of Top ten ICT companies in Nairobi	37
Members of Main internet distributors in Nairobi	28
Ministry of ICT	19
Total	85

3.5.2 Sampling Procedure

This study made use of simple random sampling, which was meant to ensure that every person in the target population stood an equal opportunity of being selected⁶⁰. The procedure was done as follows: first the researcher obtained a list of all Members of the National ICT Steering Committee, members of Top ten ICT companies in Nairobi, members of the main internet distributors in Nairobi, and the Ministry of ICT in Nairobi County. Out of the list, the researcher randomly selected individuals from that list for the sample.

3.6 Data Collection

Data collection can be defined as the process of gathering and analyzing relevant data on study variables of interest so as to be able to answer research questions, test hypotheses, and assess outcomes⁶¹. As a result, this section outlined the numerous techniques used to collect meaningful data from participants throughout the research.

3.6.1 Questionnaires Surveys

This study benefited from qualitative as well as quantitative data, with both sets of data collected through the use a standardized questionnaire with a Likert scale of 1 to 5. A structured questionnaire with closed-ended questions was used since it allowed respondents to respond in less time and provided a high level of data consistency. They were also simple to administer, collect, and analyze.

The study employed a structured interview guide to collect qualitative data from four key informants (KIs) who were well-versed in domestic data protection regulations. A key informant is a person who the researcher believes will provide important information on the

⁶⁰ Neuman and Lawrence. *Understanding research*. Pearson, 2016.

⁶¹ Hunt and Tyrrell, Coventry University Probability Sampling Techniques. 2001.

present issue⁶². The KIs were interviewed at their workplaces using a structured interview guide that had been created ahead of time.

3.6.2 Pilot Testing

A pilot study can be defined as a preliminary study which is a small-scale study of the main study meant to be used to assess the feasibility, cost, duration, and any other adverse events. It is also used to improve the study design, to ensure that by the time the full-scale research is being carried out, all the I's have been dotted and T's crossed. A pilot study with a tenth of the total sample with homogeneous characteristics, according to Mugenda & Mugenda (2003), is appropriate for the pilot study. One week before the main study began, the author conducted a pilot study on a random sample of 10 participants from the ministry of ICT at Teleposta Towers in Nairobi's CBD, which allowed the researcher to fix some flaws in the questionnaire's validity and reliability. However, the pilot results were not used to make inferences on the main study.

3.6.3 Reliability of Research Instruments

Reliability of tools in research can be defined as the degree to which the research tools used in a study produce the same results every time a test is performed under similar conditions on the same topic⁶³. To do so, a test re-test technique was employed to estimate the research tools' reliability. This was accomplished by presenting the same research instrument to the same group of respondents who had been identified for this purpose multiple times.

3.6.4 Validity of Research Instruments

In any research process, validity cannot be wished away. Mugenda and Mugenda (2003), define validity as the accuracy and significance of inferences drawn from research findings. The questionnaire was validated to guarantee that it acquired correct data from the field. This was accomplished through triangulation and cross-checking (validation and/or verification) during data analysis, which improved data validity.

⁶² Patton, *Qualitative evaluation and research methods* (2nd ed.). 1990.

⁶³ *Quantitative, and Mixed Method Approaches* (4th ed.). Thousand Oaks, California: SAGE Publications.

3.7 Data Analysis Techniques

Data analysis entails the process of packing and arranging the collected data in a way that the primary aspects are structured in such a way that the results may be effectively communicated⁶⁴.

Before any further analysis, the data was coded, revised, and any data that needed cleaning was completed. To evaluate the data and test the study hypotheses, the researcher employed descriptive and inferential statistics. This was accomplished by processing and analyzing raw data using the Statistical Program for Social Sciences (SPSS) calculator to obtain the study's results. The SPSS calculator provides a wide choice of highly adaptable statistical models that are suitable for the study's data analysis needs⁶⁵. The mean scores and standard deviations for predictor variables were calculated for descriptive analysis. The aggregate relative prevalence of efficacy of the domestic data protection law in Kenya was shown by the mean scores, which demonstrated the ranking of key components of the data protection law in Kenya. The standard deviation revealed the range of responses. Pearson's correlation analysis, analysis of variance (ANOVA) F-statistics and t-tests, and multiple regression analysis were among the inferential statistics used.

The multiple regression model for this study was as follows:

Dependent variable (Y) – effectiveness of domestic data protection law in Kenya

Independent variables:

X₁ - Unified African Union (AU) data protection ratification,

X₂ – Individual sovereign entity,

X₃ - International standards,

and ε was the error term denoting there may be a non-linear relationship between the independent and dependent variables which is referred to as “noise”.

The regression model equation is illustrated as follows:

⁶⁴ George, Design of Sampling Experiments in the Social Sciences. 1997.

⁶⁵ Park, Fundamental Applications of Statistics Sage Publications. 1992.

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon$$

$\beta_0 - \beta_4$ are the coefficients of determination.

3.8 Ethical Considerations

Before beginning the data collection process, the researcher obtained a letter of introduction from the University of Nairobi, which enabled the researcher to seek and obtain a research authorization letter from the National Council of Science and Technology (NACOSTI), the body responsible for issuing research clearance certificates and authorizing the process of data collection in Kenya⁶⁶. The authorization letter from NACOSTI ensured consent from the target institutions thus, access to staff and offices. The wishes of members not willing to participate in the study were respected based on research ethics. All information provided was treated as confidential and was only used for academic purposes. This study was therefore conducted in full compliance of the standards, laws, rules and regulations of Kenya.

To ensure the research participants confidentiality and scientific honesty, respondents were allowed to fill up un-identical structured questionnaires in privacy and anonymity. All the collected data was presented in its original form without manipulation of content, consistencies and findings.

⁶⁶ Mugenda, & Mugenda. Research methods: *Quantitative and qualitative Approaches*.2003.

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the findings of this study that sought to evaluate the effectiveness of domestic data protection legislation in African countries with specific reference to the data protection law in Kenya. This chapter therefore presents an analysis from the findings which were obtained from questionnaire responses. The analysis was divided into three sections. The first section (Section A) is an analysis of response rate and respondent's demographic characteristics. The second section (Section B) presents the descriptive statistics which are guided by the specific study objectives which were: data protection law enforceability; domestic data protection law in Kenya vs international standards; and techniques that can be employed to strengthen the domestic data protection law in Kenya. The last part (Section C) presents the inferential statistics. A multiple regression analysis was performed with the intention of determining which of the three independent variables aforementioned were significantly related to the effectiveness of domestic data protection legislation in Kenya.

4.2 Response Rate

This section sought to establish the actual number of respondents who fully participated in the questionnaire response compared to the targeted sample size. It essentially looks at the total number of respondents who successfully answered all the questions in the questionnaire that was administered to the sample size selected from the target population during the study period, as shown below in (Table 3):

Table 3: Response Rate

Sample Size	85
Participants available	85
Total response	71
Non – response bias	16.47%
Usable responses	71
Un – usable responses	14
Usable responses rate	83.53%

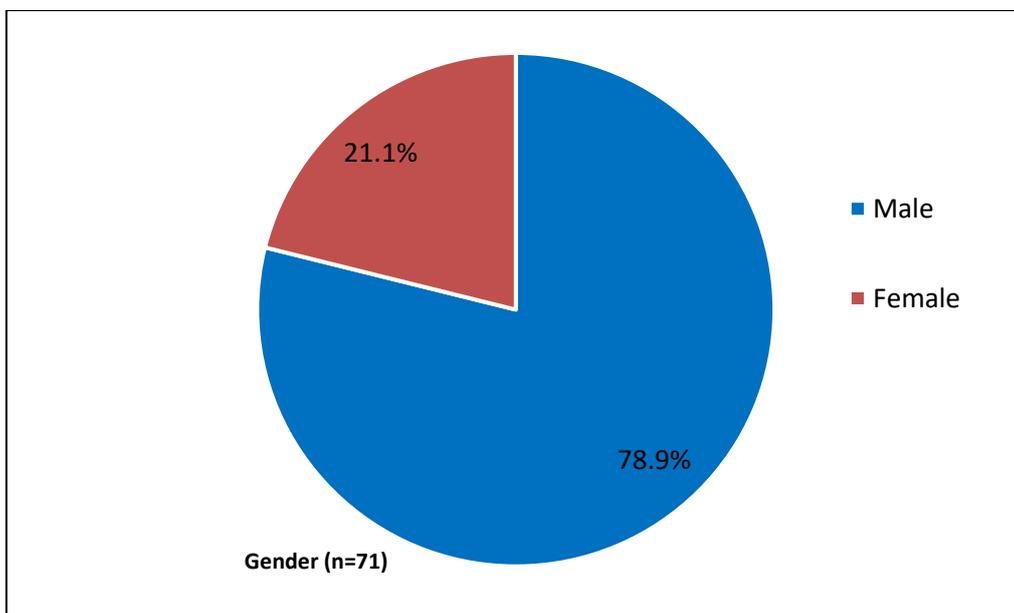
Table 3 shows that, of the 85 participants who formed the sample size selected from the target population, all were accessible, with 85 questionnaires administered through Google forms. 71 responses were recorded, with the questionnaires successfully completed and data usable for the study. With reference to Baruch (2008), in the event of a distinction between the

number of returned questionnaires versus the number of usable questionnaires, then it is recommended that the researcher rely on the number of usable responses to form the numerator when determining the response rate. Based on this approach, 83.53 per cent was recorded as the study's response rate. The researcher determined this as more than sufficient, relying on Mugenda and Mugenda (2003), who espouse that 50 per cent as a recorded response rate is adequate for analysis and reporting; 60 per cent as a recorded response rate is good for analysis and reporting, and 70 per cent and above as a recorded response rate is excellent for analysis and reporting.

4.3 Respondents' Demographics

When analyzing respondents' demographics, six (6) themes were looked at which included gender, age, level of education, field of expertise and number of years involved in the specific field as presented in subsequent Figures below:

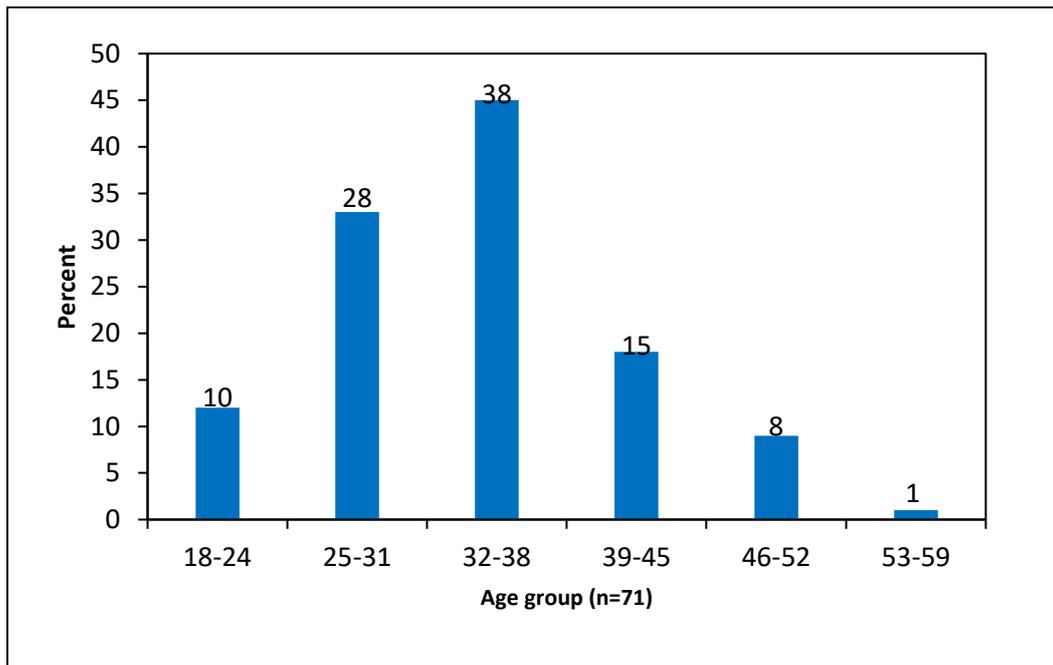
Figure 2: Frequency distribution of respondents by gender



The results in Figure 2 show that male respondents made up more than half that is 78.9 per cent of the total participants interviewed. The female respondents made up only 21.1 per cent of the total respondents. This could mean that males are much involved in fields that touch on domestic data protection in Kenya more than their female counterparts. The findings imply that the female gender distribution as recorded from the study sample is less than the minimum criterion of 30 per cent set by Kenya's 2010 constitution in order to achieve a just,

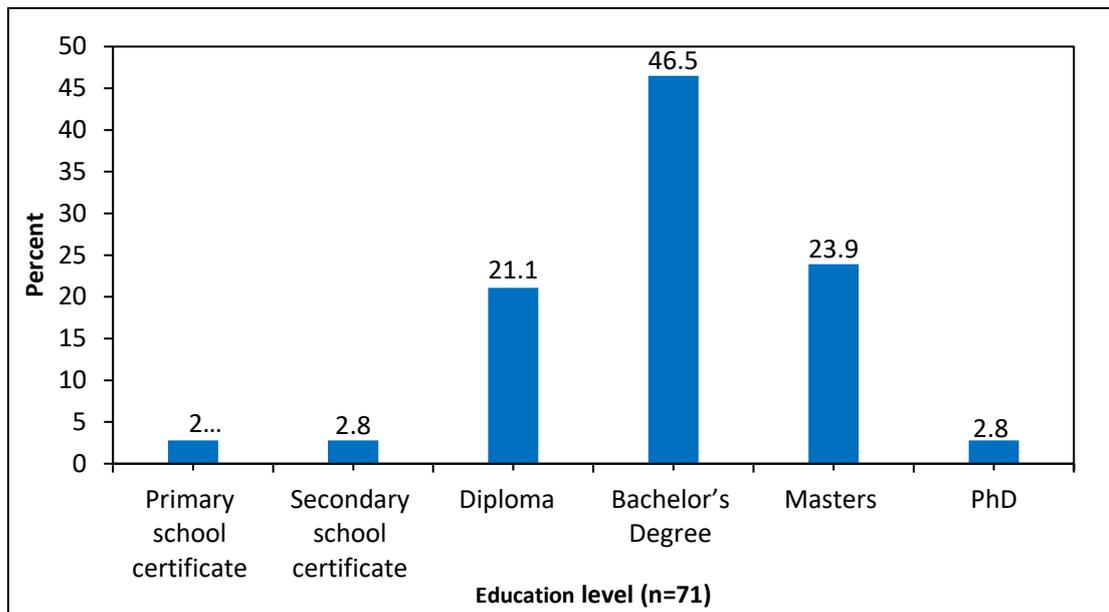
fair, and reformed society free of gender-based discrimination in all aspects of life. Gender was significant in this study because different genders might bring different qualities and thinking processes to the table, which are important for a thorough examination of Kenya's data protection regulations.

Figure 3: Frequency distribution of respondents by age



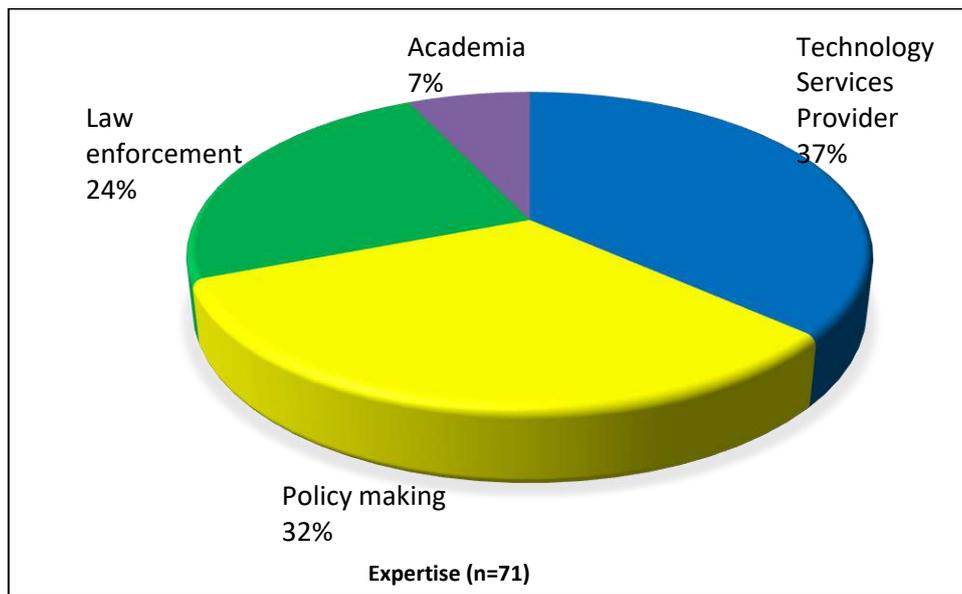
The study findings indicate that of the 71 participants, majority that is 38 per cent of the respondents fell within the age bracket of 32-38 years, this was followed by 28 per cent of the respondents who fell within the age bracket of 25-31 years. 15 per cent of the respondents fell within the age bracket of 39-45 years. Only 1 per cent of the respondents were over 50 years of age. These findings imply that the bulk of the study population for this research were young people in their late 20s and late 30s. This could also imply that the efficiency of Kenya's domestic data privacy legislation cannot be achieved without the participation of Kenya's youth. According to the 2019 Kenya national population and housing census, 75 per cent of Kenya's 47.6 million people are under the age of 35.

Figure 4: Frequency distribution of respondents by education level



The findings reveal that the highest number (46.5 per cent) of respondents had attained a bachelor's degree, followed by master's degree holders at 23.9 per cent. A sizeable number (21.1 per cent) of the respondents had a diploma, while PhD holders were 2.8 per cent, secondary school certificate (2.8 per cent), and primary school certificate (2.8per cent). The findings could mean that for effectiveness in data protection laws in Kenya, then merit is a vital aspect. Level of education was important to this study in that data protection and technology in general is a complex subject that is easier to understand for an individual who is more informed hence can confidently handle data/information and can influence the effectiveness of the domestic data protection law in Kenya.

Figure 5: Frequency distribution of respondents by field of expertise



The findings of the study show that the highest number (37 per cent) of respondents in the study area were drawn from technology services providers, followed by policy makers (32 per cent). A relatively sizeable number (24 per cent) of the respondents were from law enforcement, while 7 per cent of participants were drawn from the academia. The findings demonstrate that technology services providers are at the central point when it comes to data protection as they are the ones who primarily play the role of data processors, followed by policy makers who are responsible for developing the policies that create and enabling environment for data processors to work while at the same time respecting the rights of data owners. Whereas law enforces closely follow as they are the ones tasked with ensuring that data processors adhere to the laid down policies. Academia also has a role to play through incorporating the principles of data protection in academics and research for the benefit of all stakeholders.

Figure 6: Frequency distribution of respondents by number of years in the specific field

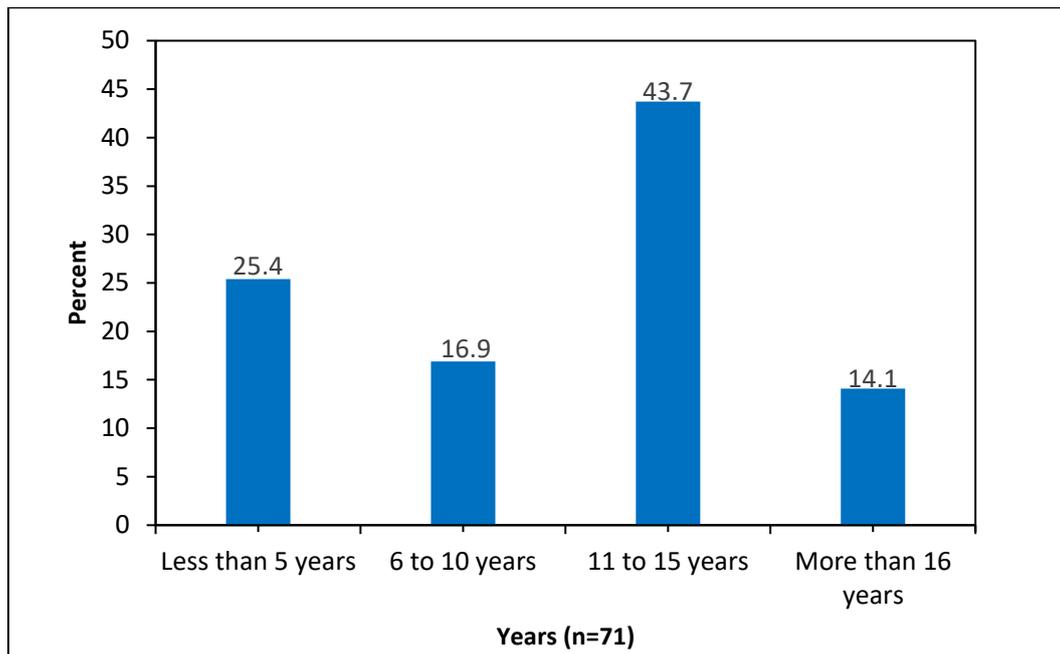
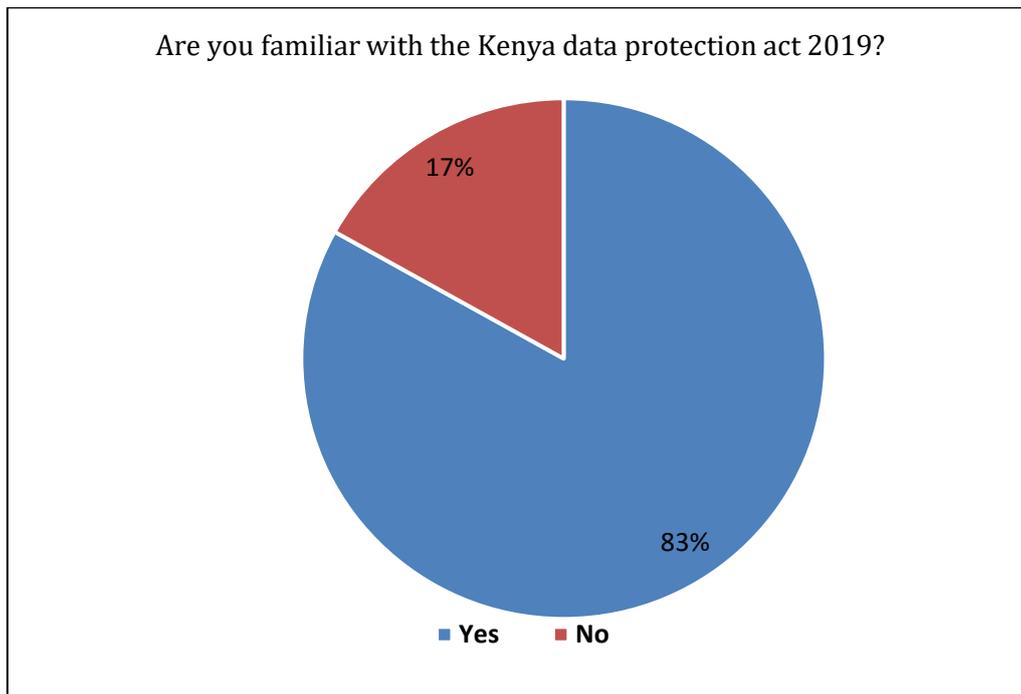


Figure 6 shows that 43.7 per cent of the participants interviewed had been involved in the ICT field for a period between 11-15 years, followed by 25.4 per cent (less than 5 years), while 16.9 per cent of the respondents indicated that they had been involved in ICT field for a period between 6-10 years. 14.1 per cent indicated more than 16 years. Going by these findings, it is clear from the results that the participants have sufficient experience in the field of ICT to be able to give their perspective on the domestic data protection law in Kenya. Whereas the concept of data protection is still new, individuals with a significant ICT background were in a better position to understand it as well as its implications and how it applies to this study seeking to assess the effectiveness of the domestic data protection law in Kenya.

4.4 Response on domestic data protection law enforceability

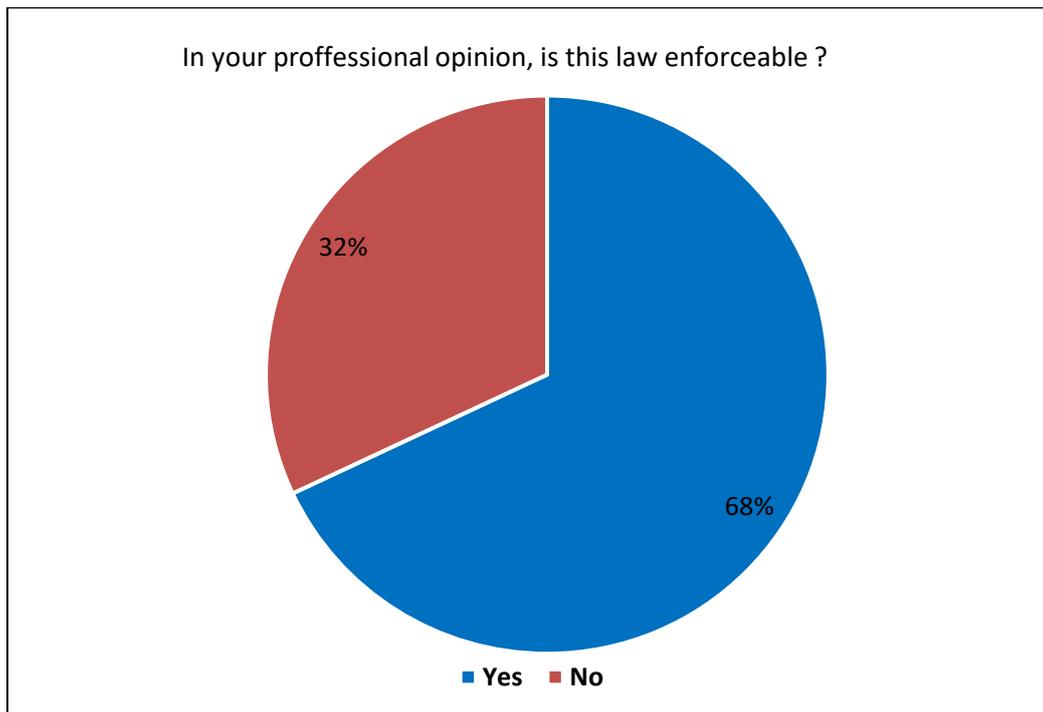
This section sought to analyze response on whether the domestic data protection law in Kenya is enforceable. The respondents were required to answer either *Yes* or *No* based on their understanding, experience, expertise or knowledge about the domestic data protection law in Kenya. The section also analyzed the opinions and suggestions from key informants engaged to give expert opinions.

Figure 7: Respondents familiarity with the Kenya Data Protection Act of 2019



The results in figure 7 indicate that majority of the participants (83 per cent) in the study area are familiar with Kenya data protection Act of 2019. This goes to mean that for laws to be effective, particularly Kenya’s domestic data protection law, there has to be a significant level of awareness and literacy around the contents of these laws among the population. This will therefore enable the various stakeholders involved, from the citizenry to service providers to law enforcers to policy makers better understand their respective roles in enhancing effective application of data protection legislation.

Figure 8: Respondents on domestic data protection law enforceability



From these findings, it is evident that majority of the respondents forming 68 per cent expressed confidence in the ability of Kenya to enforce its domestic data protection laws, whereas 32 per cent of the respondents were of a contrary opinion.

All respondents were fully aware that non-compliance to the Kenya Data Protection Act of 2019 was an offence which could lead to a fine or prison sentence or both. When asked to state the challenges Kenya was likely to face in the enforcement of the Kenya Data Protection Act 2019, respondents stated the following:

Economic issues - The respondents opined that Kenya’s economic landscape particularly as far as data is concerned, is not well defined. Emerging issues such as how to define the value of data, whether the Kenyan government has set up proper structures to support the data economy, the digital divide not only domestically in Kenya but also across the globe, issues of equity for micro, small and medium enterprises (MSMEs). Whereas data may have economic value, this value is usually not the same for all parties as its value is dependent on who the end user is and how they intend to utilize it whether as a resource for business intelligence, decision making for public service provision, national security, crime, and so on.

Fairness in data processing – The predominant issues raised here were the levels of awareness as well as informed consent by the owners of data, technologies that have automated data processing, highly opaque data management practices that are currently the norm among most data processors and practicality of handling sensitive personal data by data processors as required by the Kenya Data Protection Act of 2019.

Political data is particularly sensitive - respondents opined that when it comes to Government functions, collection of personal data of the citizenry is necessary for purposes of ease of identification of citizens and provision of government services. While this is noted, there is also potential for the government misusing this data particularly for political gain and suppression of democracy in the guise of promoting national security and improving service delivery. This is a thin line that will require a lot of trust to be built between the government and its citizenry.

Cross border transfer – With the world being a global village, there are no barriers to personal data being transferred across international borders. The impending challenge remains of how to handle situations where personal data belonging to Kenyan citizens will be exported to countries that do not have adequate data protection laws or have laws that do not conform to the Kenya Data Protection Act of 2019.

When asked to give any suggestions on how Kenya can mitigate the enforcement challenges, six issues were suggested:

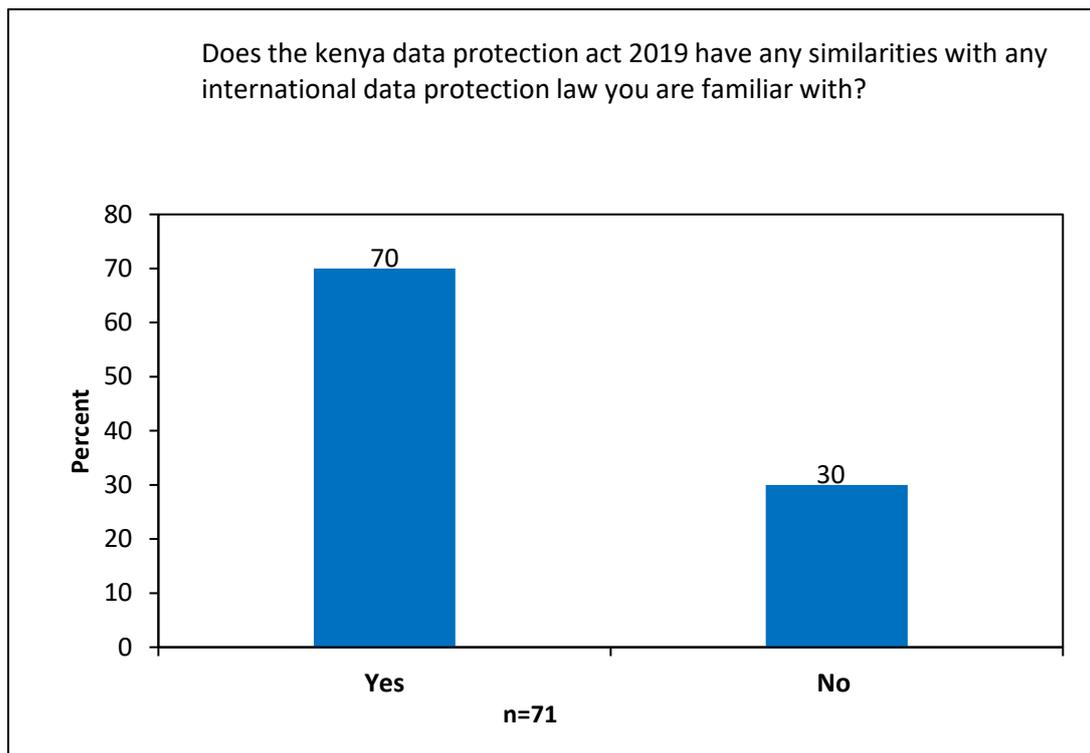
1. Creating more literacy among the citizenry on the data economy and rights of data subjects.
2. Sensitize both private and public entities on emerging issues in data protection.
3. Promote a friendly environment for data processors and data controllers.
4. Encourage data controllers and processors to adopt best practices in data protection.
5. Invest significantly in enforcement of data protection laws, including the ability to investigate and issue sanctions.
6. Promote and protect the rights of data subjects.

4.5 Similarities between Kenya’s domestic data protection law and international data protection laws

This section sought to establish whether Kenya’s domestic data protection law has any similarities with other international data protection laws. The respondents were asked to

indicate either *Yes* or *No* based on their understanding, experience, expertise or knowledge about whether the domestic data protection law in Kenya had any similarities with international data protection laws. The section also analyzed the opinions and suggestions from key informants engaged to give expert opinion.

Figure 9: Respondents on domestic data protection law similarities with international data protection laws



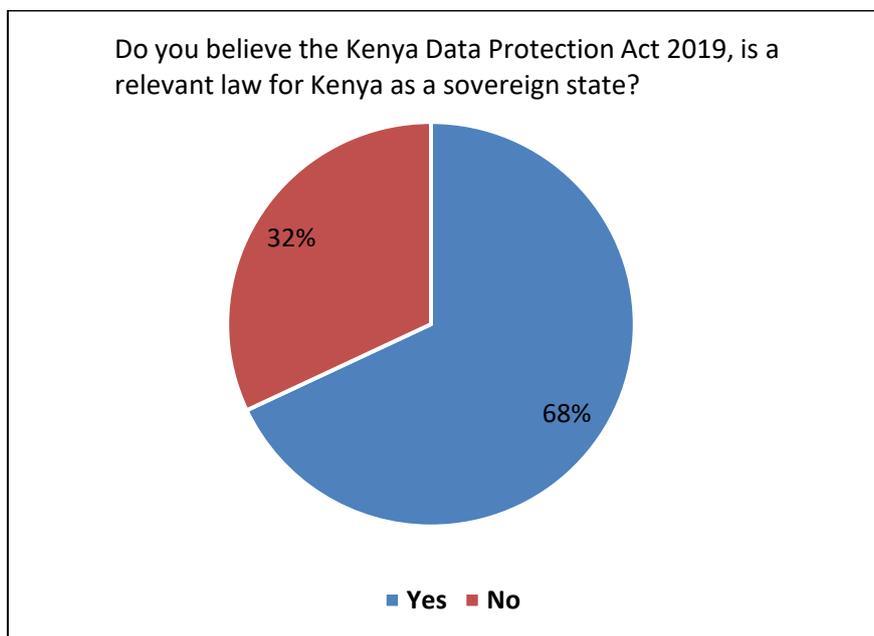
From the study findings, majority that is 70 per cent of the respondents concurred that the Kenya Data Protection Act of 2019 had similarities with other international data protection laws particularly the GDPR in which is in place in the EU. Whereas 30 per cent of the respondents were not aware of any international data protection laws that were similar to Kenya’s domestic data protection law.

One of the key informants during the interviews stated that “*The terms of the Domestic Data Protection Act 2019 closely resemble those of the European Union's General Data Protection Regulations (GDPR), thus businesses that have already made steps to comply with GDPR will be ahead of the game*”. This goes to mean that Kenya is taking comprehensive measures to ensure the effective of its domestic data protection law by borrowing heavily from global

best practices particularly the EU which has the gold standard when it comes to data protection legislation.

Other key informants also highlighted the similarity in definitions of key terms as highlighted in both the Kenya Data Protection Act of 2019 and other international data protection laws. One of the key informants noted that, “*The Kenya Data Protection Act has a lot in common with the General Data Protection Regulation (GDPR), as evidenced by the text. The terms 'personal data,' 'controllers,' and 'processors' are all defined the same way in the Kenyan law.*” One Key informant from the Ministry of ICT stated that, “*In my view, there is probably a 90 per cent overlap between the two laws.*” This goes to indicate that the Kenya Data Protection Act of 2019 is a comprehensive law that borrows heavily from the proven and tested GDPR hence has the potential to impose obligations onto organizations anywhere, so long as they target or collect data related to the Kenyan citizenry.

Figure 10: Respondents on relevance of Kenya Data Protection Act for Kenya as a sovereign state



Majority of the respondents that is 68 per cent concur that the Kenya Data Protection Act of 2019 is a relevant legislation to Kenya as a sovereign state, whereas 32 per cent of the respondents were of the contrary opinion. These findings generally indicate a high level of confidence among the target population on the ability of the country to enforce this law domestically, and on the huge need and timeliness of this law.

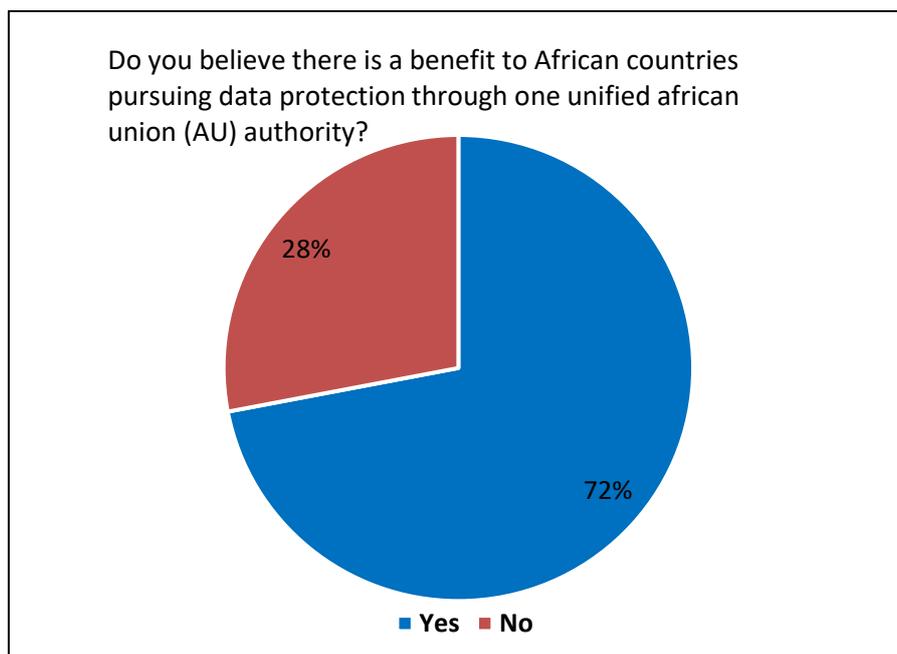
When asked which key areas of the Kenya Data Protection Act they like most, a relatively sizeable number of key informants highlighted the fact that the Kenyan citizenry who are mostly referred to as data subjects, stand a real risk of having their data privacy rights violated, and this is actually something that has been going on for years because of lack of regulation for data controllers and data processors. The silver lining today is that there exists the Office of the Data Protection Commissioner (ODPC) that has the mandate of handling data subjects' complaints on data breaches by data controllers and processors.

4.6 Techniques that can be employed to strengthen the domestic data protection law in Kenya

Respondents were asked to suggest ways in which Kenya can strengthen its domestic data protection laws. Three suggestions stood out from the key informants:

- Active involvement of all stakeholders in the development of the data protection legislation.
- Development of a mechanism to enable auditing of personal data in the custody of private entities.
- Parliament should legislate a registration and identification of person's bill, which is fully subjected to the public participation process.

Figure 11: Respondents on Benefit to African Countries Pursuing Data Protection through one unified African Union (AU) Authority



Majority of the respondents that is 72 per cent concurred that there was a benefit in African countries pursuing data protection through a unified AU authority, whereas a minority that is 28 per cent were of the contrary opinion. The results go to show that data is an essential resource, which necessitates strong legislation supported by strong institutions to protect it. Therefore, there is value and merit in African countries pursuing data protection through a unified AU authority in order to enhance effectiveness in enforcing data protection laws domestically. With the challenges of globalization, strong multinational corporations and the threats of cyber security, a unified approach for AU member states will enhance data protection both within and across intracontinental and intercontinental borders to ensure that data belonging to Africans can be used to meet the utility aspirations of Africans.

During an interview with one member of the National ICT Steering Committee who was one of the key informants in the study, stated that, “*The cross-border flow of personal data, which will be exacerbated by the digital economy's growth, necessitates intra-African collaboration in enforcing data protection legislation. The African Union has made judgments about the secure use of Africa's digital economy*”. This goes to show the necessity of protecting personal data of the African citizenry even as it is transferred across borders so as to ensure that Africans are in a position to assert their rights to their personal data.

4.7 Inferential Statistics

In order for the researcher to be able to accept or reject the null hypothesis, the chi square test of independence was carried out.

Hypothesis 1:

H₁: Kenya will have difficulty enforcing its domestic data protection law especially when non-compliance is by a multinational corporation.

Table 4: Case processing summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
difficulty enforcing domestic data protection law * YES/NO	8	100.0%	0	0.0%	8	100.0%

Table 5: Difficulty enforcing domestic data protection law * YES/NO Cross tabulation

		YES/NO		Total
		no	yes	
Difficulty enforcing domestic data protection law	Accuracy	0	1	1
	Adequacy	1	0	1
	Cross border transfer	0	1	1
	Fairness and lawfulness	1	0	1
	Retention	0	1	1
	Rights of data subjects	0	1	1
	Security of data	1	0	1
	Stated purpose	1	0	1
Total		4	4	8

Based on the results from this Chi square test, the p-value (0.333) is larger than the standard alpha value (0.05), based on this, the researcher therefore accepted the null hypothesis that asserts that Kenya will have difficulty enforcing its domestic data protection law especially when non-compliance is by a multinational corporation. Table 6 below shows the results of the Chi square test:

Table 6: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8.000 ^a	7	0.333
Likelihood Ratio	11.090	7	0.135
N of Valid Cases	8		

a. 16 cells (100.0%) have expected count less than 5. The minimum expected count is .50

Hypothesis 2:

H₁: Kenya’s domestic data protection law will conform to international standards as it is largely based on the EU’s GDPR

Table 7: Case processing summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
domestic data protection law conforms to international standards * YES/NO	8	100.0%	0	0.0%	8	100.0%

Table 8: Domestic data protection law conform to international standards * YES/NO Cross tabulation

		YES/NO		Total
		no	yes	
domestic data protection law conforms to international standards	Accuracy	0	1	1
	Adequacy	1	0	1
	Cross border transfer	0	1	1
	Fairness and lawfulness	0	1	1
	Retention	0	1	1
	Rights of data subjects	0	1	1
	Security of data	0	1	1
	Stated purpose	1	0	1
Total		2	6	8

Based on the results from this Chi square test, the p-value (0.333) is larger than the standard alpha value (0.05), based on this, the researcher therefore accepted the null hypothesis that asserts that Kenya’s domestic data protection law will conform to international standards as it is largely based on the EU’s GDPR. Table 9 below shows the results of the Chi square test:

Table 9: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8.000 ^a	7	0.333
Likelihood Ratio	8.997	7	0.253
N of Valid Cases	8		

a. 16 cells (100.0%) have expected count less than 5. The minimum expected count is .25

Hypothesis 3:

H₁: There are techniques available that Kenya can use to strengthen its domestic data protection law.

Table 10: Case processing summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
techniques available that Kenya can use to strengthen its domestic data protection law * YES/NO	8	100.0%	0	0.0%	8	100.0%

Table 11: Techniques available that Kenya can use to strengthen its domestic data protection law * YES/NO Cross tabulation

		YES/NO		Total
		no	yes	
Techniques available that Kenya can use to strengthen its domestic data protection law	Accuracy	0	1	1
	Adequacy	1	0	1
	Cross border transfer	1	0	1
	Fairness and lawfulness	1	0	1
	Retention	0	1	1
	Rights of data subjects	0	1	1
	Security of data	1	0	1
	Stated purpose	1	0	1
Total	5	3	8	

Based on the results from this Chi square test, the p-value (0.333) is larger than the standard alpha value (0.05), based on this, the researcher therefore accepted the null hypothesis that asserts that there are techniques available that Kenya can use to strengthen its domestic data protection law. Table 12 below shows the results of the Chi square test:

Table 12: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8.000 ^a	7	0.333
Likelihood Ratio	10.585	7	0.158
N of Valid Cases	8		

a. 16 cells (100.0%) have expected count less than 5. The minimum expected count is .38

4.8 Discussion

According to the findings, more than half of the respondents (83 per cent) said they were familiar with the Kenya Data Protection Act of 2019. This essentially shows that majority of the key stakeholders who formed a bulk of the study's target population had sufficiently interacted with the contents of Kenya's domestic data protection laws. It is noteworthy however that this may not be a representation of the level of knowledge among the wider Kenyan citizenry based on the results of a study released recently by Amnesty International (2020)⁶⁷ which found that only 54 per cent of Kenyans were aware they had the right to privacy. This is in spite of the fact that the Data Protection Act of 2019 had been in effect for

⁶⁷ Amnesty International (2021). Kenyans still unaware of data protection and right to privacy.

nearly a year and a half, as at the time of the study. The study by Amnesty found that 70 per cent of people are still unaware of it. The North-Eastern (79 per cent), Central (72 per cent), and Rift Valley (72 per cent) regions of Kenya had the greatest lack of awareness. Furthermore, as noted by 70 per cent of respondents in the study region, the Kenya Data Protection Act of 2019 shares similarities with international data protection regulations. This implies that not a single country, including Kenya, can claim to have achieved data protection success on its own, as these laws need to be interoperable globally due to globalization which has resulted in inevitable need to transfer personal data across international borders. The findings are backed up by Grudz (2018)⁶⁸ who reported that African countries are slowly but steadily enacting data privacy legislation, thanks in large part to the EU's GDPR. According to Grudz, about half of Africa's 53 countries have enacted legislation aimed at protecting personal data.

The findings also reveal that Kenya's domestic data protection law is a comprehensive piece of legislation that has the potential to sufficiently protect the personal data of the Kenyan citizenry, owing to the fact that it heavily borrows from the tried and tested GDPR. Results indicated that more than half (68 per cent) of the respondents in the study area believe the Kenya Data Protection Act of 2019 is a relevant law for Kenya as a sovereign state. The findings are in line with Makulilo (2012)⁶⁹, who noted that the Kenya Data Protection Act of 2019 is a local data protection legislation modeled on the GDPR, which is Kenya's primary data protection statute and is anchored on the Kenyan constitution promulgated in 2010 thus giving effect to Article 31 c) and d) which guarantee the individual's right to privacy. The law is intended to establish a legal framework for both government and commercial organizations to collect, process, store, and use personal data belonging to Kenyan citizens.

According to the findings, Africa needs a coordinated plan for trusted data interchange both within and beyond borders in order to ensure that data belonging to Africans is respected and privacy rights entitled to the African citizenry are unconditionally granted and respected by both states and multinational corporations who mostly utilize this data in their operations. This is based on the fact that 72 per cent of those polled thought that African countries would benefit from pursuing data protection through a single African Union (AU) authority. The

⁶⁸ Grudz (2018). Social Media Marketing: Who is watching the Watchers? *Journal of Retailing and Consumer Services* 53: 1-12

⁶⁹ Makulilo, A.B. (2012). Privacy and data protection in Africa: a state of the art. *International Data Privacy Law*, 2, 163-178.

findings are in line with Makulilo (2012)⁷⁰ who stated that a unified data protection regime for the AU may be a more successful path in the ability of Kenya and other AU members to enforce adherence to their domestic data protection policies.

From the study findings, the respondents expressed confidence in Kenya's ability to enforce its domestic data protection policies. This was based on the fact that the law clearly stipulated sanctions for non-compliance with this law, with offenses punishable through a fine, imprisonment, or both. However, UNCTAD (2016) highlights the difficulty of defining jurisdiction as a major issue in law, particularly when it comes to data protection. Because data travels across international borders and there is currently no one universal data protection agreement thus, defining jurisdiction can be difficult. This was a perspective that the researcher shared prior to the study hence the emphasis in approaching data protection through a unified AU authority that will have an expanded jurisdiction.

When asked what obstacles Kenya is likely to experience in enforcing the Kenya Data Protection Act of 2019, the following issues emerged as the most significant:

- The fact that Kenya's economic landscape particularly as far as data is concerned, is not well defined. Emerging issues such as how to define the value of data, whether the Kenyan government has set up proper structures to support the data economy, the digital divide not only domestically in Kenya but also across the globe, issues of equity for micro, small and medium enterprises (MSMEs). Whereas data may have economic value, this value is usually not the same for all parties as its value is dependent on who the end user is and how they intend to utilize it whether as a resource for business intelligence, decision making for public service provision, national security, crime, and so on.
- The levels of awareness as well as informed consent by the owners of data, technologies that have automated data processing, highly opaque data management practices that are currently the norm among most data processors and practicality of handling sensitive personal data by data processors as required by the Kenya Data Protection Act of 2019.

Makulilo, A.B. (2012). Privacy and data protection in Africa: a state of the art. *International Data Privacy Law*, 2, 163-178.

- When it comes to Government functions, collection of personal data of the citizenry is necessary for purposes of ease of identification of citizens and provision of government services. While this is noted, there is also potential for the government misusing this data particularly for political gain and suppression of democracy in the guise of promoting national security and improving service delivery. This is a thin line that will require a lot of trust to be built between the government and its citizenry.
- With the world becoming a global village, there are no barriers to personal data being transferred across international borders. The impending challenge remains of how to handle situations where personal data belonging to Kenyan citizens will be exported to countries that do not have adequate data protection laws or have laws that do not conform to the Kenya Data Protection Act of 2019.

When asked for thoughts on how Kenya should address the enforcement concerns, six issues were raised:

- Creating more literacy among the citizenry on the data economy and rights of data subjects.
- Sensitize both private and public entities on emerging issues in data protection.
- Promote a friendly environment for data processors and data controllers.
- Encourage data controllers and processors to adopt best practices in data protection.
- Invest significantly in enforcement of data protection laws, including the ability to investigate and issue sanctions.
- Promote and protect the rights of data subjects.

Chi square results found evidence for null hypothesis and therefore the three null hypotheses are accepted, that is to say:

H₁: Kenya will have difficulty enforcing its domestic data protection law especially when non-compliance is by a multinational corporation;

H₁: Kenya's domestic data protection law will conform to international standards as it is largely based on the EU's GDPR; and

H₁: There are techniques available that Kenya can use to strengthen its domestic data protection law.

These are perspectives that the researcher concurs with as they clearly highlight the shortcomings of pursuing data protection mechanisms from a domestic lens as opposed to a unified AU authority. The silver lining is that stakeholders in this field express significant knowledge on the subject and there is optimism that Kenya and African states in general will pursue unity in data protection provided there is sufficient information and evidence available to advice policy makers.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This formed this study's final chapter, which detailed the summary of the primary study's findings, drew inferences from the findings and offered conclusions and recommendations from the researcher's perspective as well as insight into potential areas for future research. The chapter was guided by the following questions: Is Kenya's domestic data protection law enforceable? Does Kenya's domestic data protection law conform to international standards? Are there strategies that may be used to strengthen Kenya's domestic data protection law?

5.2 Summary of Findings

The first question aimed at finding out whether Kenya's domestic data protection legislation was enforceable. Whereas the findings reveal that the law has mechanisms to sanction non-compliance through punitive measures such as a fine, jail, or both, this law does not address issues of jurisdiction especially in situations where violations will be committed by entities outside of Kenya's jurisdiction, which will be an inevitability taking into account the challenge of globalization which necessitates cross border transfer of personal data. Whereas this law may prescribe punitive measures for non-compliance, the practicality of enforcing this law is what the researcher seeks to bring into question and is not convinced was sufficiently addressed by the respondents. As things stand, multinational corporations run platforms such as email, social media, e-commerce, banking and many more that make use of personal data. Majority of this multinational corporations do not have a physical presence in Kenya as well as in a majority of other African countries. It will therefore present a challenge, sanctioning such organizations for violations of domestic data protection legislation when they are not subject to a state's jurisdiction.

The second question aimed at ascertaining whether Kenya's domestic data protection policy was in conformity with international standards. This was answered in the affirmative as both the respondents as well as the researcher's own comparison of Kenya's law and the GDPR which is the premier law in the EU and currently the global gold standard, showed glaring similarities. According to the analysis, Kenya's domestic data protection law enacted in 2019 is largely influenced by the EU's GDPR. It is also noteworthy that Kenya is among the few states in Africa to adopt the Malabo Convention that gave birth to the African Union

Convention on Cyber Security and Personal Data Protection. Experts have touted this convention as a visionary pact that came before its time, taking into consideration that it was conceptualized long before the GDPR came into effect in Europe. This convention creates room for a unified data protection AU regime that is interoperable with other international data protection regimes. The Kenya Data Protection Act of 2019 is in full conformity with these two international legal regimes.

The final inquiry was to see whether there were any measures that could be used to strengthen Kenya's domestic data protection legislation. The following recommendations emerged from the study's findings:

1. Active involvement of all stakeholders in the development of the data protection legislation.
2. Development of a mechanism to enable auditing of personal data in the custody of private entities.
3. Develop a mechanism for enforcement of data privacy rules, including the capacity to conduct investigations and apply penalties.
4. Parliament should legislate a registration and identification of person's bill, which is fully subjected to the public participation process.
5. More civic education on the data economy and data subjects' rights.

Whereas the researcher concurred with these recommendations from the respondents, and believes if adhered to, they will help strengthen Kenya's domestic data protection policies, a glaring omission from these responses was evident. This primarily entails setting up mechanisms to ensure this domestic law is interoperable with other international laws as well as operationalizing the Malabo Convention.

5.3 Conclusion

Based on the findings of this study, there is no doubt that domestically, the Kenya Data Protection Act of 2019 is an effective law that can be enforced, meets international standards and has the potential to be strengthened to make it more effective. The challenge comes in when nonconformity is by a party whether they are a state or non-state actor that does not fall within the Kenya's jurisdiction. With globalization, international transfer of personal data is an inevitability hence the need for states to develop laws that are interoperable with other international legal regimes so as to broaden jurisdiction for enforceability. In noting so, it is

important to highlight the fact that data protection cannot be the subject of a single state, global treaty or accord, and that Africa's and Kenya's success in guaranteeing personal data protection for its citizenry can be secured through approaching data protection through a unified AU authority as was envisioned in the Malabo Convention.

The study also recognizes the awareness gap on matters of data protection which affects each individual as their data is utilized by both government and private sector players from within and outside of the country's borders, often without due consideration to the individual data subject's rights. The onus is on respective governments and industry stakeholders to conduct sufficient civic education on this subject, to ensure that there is a citizenry that is knowledgeable enough on this subject so that they can contribute adequately to policy decisions that affect them. One of the key policy decisions is on whether to retain sovereignty in domestic data protection or cede this power to a unified AU authority.

According to the researcher, the liberalism theory still holds and has merit in this study in that whereas there is a strong call to anchor data protection to a unified AU authority, the composition of this authority should have representation from key stakeholders from states as well as non-state actors. This is meant to ensure that the interests of all parties are looked into and protected even as states look to end anarchy in the way in which personal data is currently handled with plenty of disregard to the rights of the data subjects. The GDPR as applied in the EU has already provided a roadmap and potential picture on how this can be achieved, the question remains, does the AU have sufficient political goodwill to follow in the steps of the EU?

5.4 Recommendation

In as much as phrases such as “data is the new oil,” have been coined and have been used by experts in the recent past to create a picture of how valuable data is, and how it is the vehicle that will drive international trade and economics for decades to come, there just do not seem to have sufficient information on this subject particularly for individual citizens who are mostly the owners of this data. The researcher therefore recommends as a starting point, for policymakers, lawmakers, and other key stakeholders who are sufficiently conversant with this subject, to engage in civic education in order to raise public knowledge on the same. In noting so, before African countries such as Kenya can begin approaching data protection from a unified AU authority, it is important for their respective citizenry to fully understand this subject of data protection.

Kenyan citizens for instance need to all understand what the Kenya Data Protection Act of 2019 is, what it entails, what it seeks to achieve and what the citizenry stands to benefit from it. With a more informed citizenry, any efforts to strengthen such legislation through a unified approach as what has been done through the GDPR in the EU, is likely to bear more fruit, as the citizenry will be enlightened enough to see the value of what is being presented to it. All in all, the EU has set a precedent through the GDPR, and this provides the perfect case study for the African continent to make reference to as opposed to trying proverbially to reinvent the wheel.

5.5 Limitations of the study

This study sought to evaluate the effectiveness of domestic data protection laws in African countries, using Kenya's domestic data protection law as a case study. The study population was further narrowed down to Kenya's capital Nairobi, as this is where the researcher was confident of finding respondents with sufficient knowledge on the subject owing to its highly specialized nature. The scope therefore posed a problem in terms of empirical evidence availability, and this therefore necessitates the consideration of a broader scope. For a more thorough coverage, it may be necessary to conduct a similar study in a number of other African states so as to compare study findings. Despite the limitations mentioned above, the conclusions provided in this research concurs to some extent with other similar studies that are already in the public domain and have been referenced in this study.

5.6 Suggestions for further research

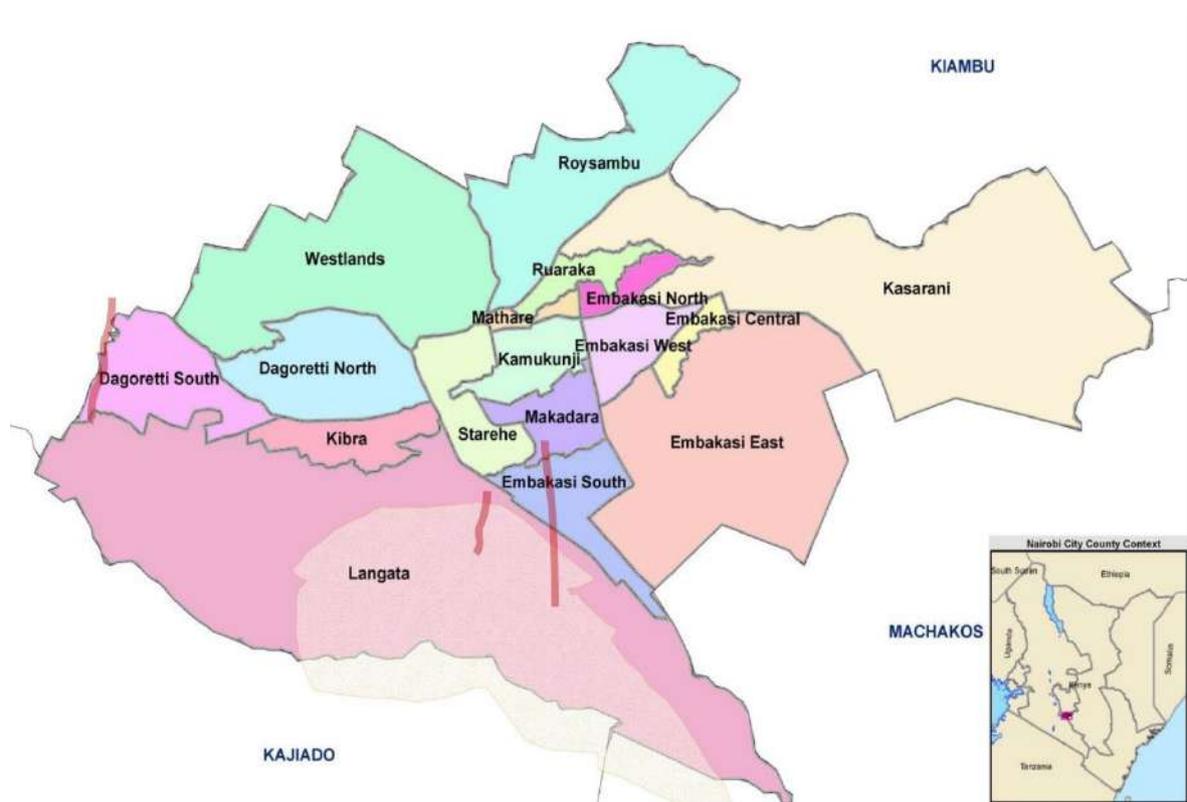
The study sample size was 85 participants from four different ICT fields that interact with data on a daily basis, are familiar with the subject of data protection and are key stakeholders in this sector. These include members of the National ICT Steering Committee, members of Nairobi's top ten ICT companies, members of Nairobi's main internet distributors, and the Ministry of ICT in Nairobi County. Based on the information obtained from these respondents who were highly specialized, it may not be possible to generalize the findings. The study therefore proposes a broader scope for assessing the performance of domestic data protection laws in not only Kenya but also in other Africa states.

References

- African Union (2019), *African union convention on cyber security and personal data protection* e.pdf, p. 13.
- African Union (2020). 'List of countries which have signed, ratified/acceded to the AU Convention on Cyber Security and Personal Data Protection'.
- Ainley, Kirsten and Brown (2005). Chris. *Understanding international relations, 3rd Edition*. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan.
- AU (2014). *African Union Convention on Cyber-security and Personal Data Protection*. Intergovernmental report, Malabo: African Union.
- Brzezinski, Z. (2017). 'Moving into a technetronic society,' in *Information Technology in a Democracy*, Harvard University Press. Cambridge, Mass, pp. 161–7.
- Chander, A. and Uyen, P. (2017) 'Data nationalism', *Emory Law Journal*, 3rd Edition, Pg. 64.
- Consumers International (2018). *The state of data protection rules around the world: A briefing for consumer organizations*. Industry report, London: Consumers International.
- Deloitte (2017). *Privacy is Paramount: Personal Data Protection in Africa*. Industry report, Johannesburg: Deloitte.
- Doninioni, S. (2019). 'The geopolitical meaning of Europe's Cybersecurity Act', Istituto per gli Studi di Politica Internazionale (ISPI).
- Foss, K. (2017). *Rhetorical criticism: Exploration and practice*. Waveland Press. Behavioral Sciences, 6th ed. Pyrczak Publishing.
- Gruzd, A. (2018). 'Multi-Stakeholder Initiatives: Lessons Learned'. SAIIA Research Paper.
- Hunt, N. and Tyrrell, S. (2001). *Coventry University Probability Sampling Techniques*.
- Kenya Gazette (2019). *The Kenya Data Protection Act*. Nairobi: Kenya National Assembly.
- Kenya National Bureau of Statistic (KNBS, 2019), *Kenya Population and Housing Census Results Report*.
- Kenya: The Constitution of Kenya [Kenya], 27 August 2010, available at: <https://www.refworld.org/docid/4c8508822.html> [accessed 1 September 2021]
- Kothari, C. R. (2006). *Research Methodology: Methods & Techniques (2nd Ed.)*. New Delhi: Age International Publishers.
- Kurbalija, J. (2019). *An Introduction to Internet Governance (6th ed)*, pg. 4
- Mugenda, O. & Mugenda, A. (2003). *Research methods: Qualitative and quantitative Approaches, Africa Center for technology studies*, Nairobi, Kenya.

- Makulilo, A.B. (2012). Privacy and data protection in Africa: a state of the art. *International Data Privacy Law*, 2, 163-178.
- Murithi, T. (2012). ‘*The African Union at ten: An appraisal*’, *African Affairs*, 111, 445, p. 663.
- Neuman, L. (2016). *Understanding research*. Pearson.
- Nikkei Asian Review (2019). ‘*Beijing exports “China-style” internet across Belt and Road*’.
- Orji, U. J. (2018). ‘The African Union Convention on Cybersecurity: A regional response towards cyber stability?’ in *Masaryk University Journal of Law and Technology*, 12th Edition, Vol2, pp. 92.
- Park, N. (1992). *Fundamental Applications of Statistics* Sage Publications. 1992.
- Parshotam, A. (2018). ‘*Can the African Continental Free Trade Area Offer a New Beginning for Trade in Africa?*’ Johannesburg: SAIIA (South African Institute for International Affairs), Occasional Paper no. 280.
- Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.).
- Schwab, K. (2016). *The Fourth Industrial Revolution*, New York: Crown Business.
- Scott Burchill, Andrew Linklater, Richard Devetak, Jack Donnelly, Matthew Paterson, Christian Reus-Smit and Jacqui True (2005). *Theories of International Relations, 3rd Edition*. Basingstoke: Palgrave Macmillan.
- Snedecor, G. (1997). *Design of Sampling Experiments in the Social Sciences*
- The Kenya Data Protection Act (2019). Available at: <https://www.odpc.go.ke/dpa-act/> [accessed 1 September 2021]
- Turianskyi, Y. (2018). ‘*Balancing Cyber Security and Internet Freedom In Africa*’, Johannesburg: SAIIA (South African Institute for International Affairs). Occasional Paper no. 275.
- UNCTAD (2016). *Data protection regulations and international data flows: Implications for trade and development*. Pg 4

Appendix 1: Map of Nairobi County



Appendix 2: Research Authorization University of Nairobi



UNIVERSITY OF NAIROBI
College of Humanities and Social Sciences
Institute of Diplomacy and International Studies

Tel : (02) 318262
Telefax : 254-2-245566
Fax: : 254-2-245566
Website : www.uonbi.ac.ke
Telex : 22095 Varsity Ke Nairobi, Kenya
E-mail : director-idis@uonbi.ac.ke

P.O. Box 30197
Nairobi
Kenya

August 23, 2021

TO WHOM IT MAY CONCERN

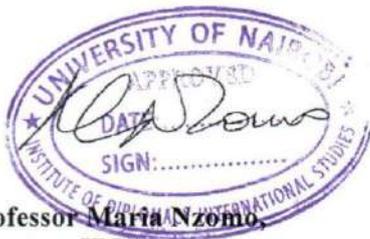
RE: MUKOKO EUGENE WANEKEYA– R50/33958/2019

This is to confirm that the above-mentioned person is a bona fide student at the Institute of Diplomacy and International Studies (IDIS), University of Nairobi pursuing a **Master of Arts Degree in International Studies**. He is working on a research project titled, **“EFFECTIVENESS OF DOMESTIC DATA PROTECTION LAWS IN AFRICAN COUNTRIES: A CASE STUDY OF THE DATA PROTECTION LAW IN KENYA”**.

The research project is a requirement for students undertaking Masters programme at the University of Nairobi, whose results will inform policy and learning.

Any assistance given to him to facilitate data collection for his research project will be highly appreciated.

Thank you in advance for your consideration.



Professor ~~Maria Nzomo~~,
Director, IDIS
&
Professor of International Relations and Governance

Appendix 3: Research Authorization National Commission for Science, Technology and Innovation (NACOSTI)


REPUBLIC OF KENYA


**NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY & INNOVATION**

Ref No: **345532** Date of Issue: **08/September/2021**

RESEARCH LICENSE



This is to Certify that Mr.. Eugene Mukoko Wanekeya of University of Nairobi, has been licensed to conduct research in Nairobi on the topic: EFFECTIVENESS OF DOMESTIC DATA PROTECTION LAWS IN AFRICAN COUNTRIES: A CASE STUDY OF THE DATA PROTECTION LAW IN KENYA for the period ending : 08/September/2022.

License No: **NACOSTI/P/21/12685**

345532
Applicant Identification Number


Director General
**NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY &
INNOVATION**

Verification QR Code



**NOTE: This is a computer generated License. To verify the authenticity of this document,
Scan the QR Code using QR scanner application.**

Appendix 4: Questionnaire



UNIVERSITY OF NAIROBI

INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES

RESEARCH STUDY CONDUCTED IN PARTIAL FULFILLMENT FOR THE AWARD OF MASTER OF ARTS IN INTERNATIONAL STUDIES

Research Questionnaire

Dear respondent,

I am Eugene Wanekeya, a student at The University of Nairobi pursuing a Master of Arts in International Studies – Student no. R50/33958/2019 Institute of Diplomacy and International Studies (IDIS). As part of the requirements for my Master of Arts in International Studies, I am conducting a survey as part of my research project on **“Effectiveness of domestic data protection laws in African countries: A case study of the data protection law in Kenya.”**

I would therefore appreciate if you could spare a few minutes to complete this questionnaire, as your professional perspective will go a long way in helping me prove or disprove my study hypothesis.

The data collected in this survey will strictly be used for academic and research purposes therefore your participation is completely voluntary and any information you provide will be kept confidential.

Researcher,

Eugene Wanekeya Mukoko

Please read each question carefully and respond to the best of your ability

1. What is your field of expertise?

Technology Services Provider	
Policy making	
Law enforcement	
Academia	

2. How many years have you been involved in this field

Less than 5 years	
6 to 10 years	
11 to 15 years	
More than 16 years	

3. Are you familiar with Kenya Data Protection Act 2019?

Yes	
No	

4. In your opinion, do you believe the Kenya Data Protection Act is a relevant law for Kenya as a sovereign state?

a.

Yes	
No	

b. Why?

5. What four key areas of this law do you like most?

a. _____

b. _____

- c. _____
- d. _____

6. What four key areas of this law do you have reservations about?

- a. _____
- b. _____
- c. _____
- d. _____

7. In your professional opinion, is this law enforceable?

a.

Yes	
No	

b. Why?

8. What four challenges do you foresee Kenya will face in the enforcement of the Kenya Data Protection Act 2019

- a. _____
- b. _____
- c. _____
- d. _____

9. Do you have any suggestions on how Kenya can mitigate the four enforcement challenges you have pointed out in question 8 above?

10. Does the Kenya Data Protection Act 2019 have any similarities with any international data protection law you are familiar with?

a.

Yes	
No	

b. Which one?

c. In what ways?

11. Do you believe the Kenya Data Protection Act 2019 can be seamlessly integrated with other international data protection laws

a.

Yes	
No	

b. Why do you believe so?

12. In what ways can Kenya strengthen its domestic data protection laws?

- a. _____
- b. _____
- c. _____
- d. _____

13. Do you believe there is a benefit to African countries pursuing data protection through one unified African Union (AU) authority?

a.

Yes	
No	

b. What are the reasons for your above answer?

Thank you for participating in this survey