KENYA'S DATA PROTECTION ACT AND ITS JURISDICTIONAL REACH: GOVERNING CROSS-BORDER DATA TRANSFERS.

Submitted in partial fulfilment of the requirements of the Bachelor Degree of Laws Degree.

Strathmore University Law School.

By

Mureithi Rachael Ivy Njoki

121309.

Prepared under the supervision of:

Mrs. Agnes Andeso

DATE: 13 JANUARY 2025.

Word Count: 11995.

DECLARATION

I, **Rachael Ivy Njoki Mureithi,** do hereby declare that this research is my original work and that to the best of my knowledge and belief, it had not been previously, in its entirety or in part, been submitted to any other university for a degree or a diploma. Other works cited or referred to are accordingly acknowledged.

Signed: 

Date: 13TH JANUARY 2025.

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

Signed: 

Mrs. Agnes Andeso.

VT OMNES VNVM SINT

ABSTRACT

This dissertation examines the jurisdictional reach of Kenya's DPA in regulating cross border transfers, focusing on its extraterritorial enforcement and compliance. The study evaluates whether the DPA adequately addresses the risks and challenges posed by international data transfers, emphasizing its role in safeguarding the right to privacy. The dissertation also takes a step at critically assessing the Data Protection Act's extraterritorial jurisdiction. Furthermore, the study outlines Kenya's current legal framework. Evidence of gaps in enforcement and compliance is presented, alongside risks associated with inadequate regulation of cross-border data transfers. The findings underscore the need for policy and legal reforms to enhance the DPA's efficacy. This research offering insights into enhancing the DPA's jurisdictional reach and fostering data privacy in a globalized digital environment.

VT OMNES VNVM SINT

ACKNOWLEDGEMENTS

I am deeply grateful to God who has been a great source of strength during this process. I believe that I would not have made it this far without the support He has offered me all the way. I am also grateful to my supervisors Madam Agnes Andeso my supervisor. Lastly, I am heavily indebted to my parents who have supported me and encouraged me since first year. They supported a dream that sometimes seemed too big for me and kept me from giving up on it.

DEDICATION

This dissertation is dedicated to my late grandmother, Rachel Njoki Mithamo. I still remember how ecstatic she was when my parents told her I had been accepted to join Strathmore Law School. Unfortunately, she did not get to see me get to the end. Dedicating this is an effort to include her in the end of a journey we began together. She has and will always be a role model and source of strength to me. She played a key role in instilling in me the values of hard work and perseverance.

List of Abbreviations

DPA – The Data Protection Act of Kenya, 2019.

DPIA- Data Protection Impact Statement.

GDPR - General Data Protection Regulation.

NIIMS- National Integrated Identity Management System.

ODPC- The Office of the Data Protection Commissioner.

List of Statutes

The Data Protection Act 2019.

The Data Protection (General) Regulations 2021.

The General Data Protection Regulations 2016.

List of Cases

Federation of Kenya Employers v Cabinet Secretary, Ministry of Foreign Affairs and International Relations & 4 others, 2023.

Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR.

Table of Contents

CHAPTER 1: INTRODUCTION TO THE STUDY

1.1 Background

Kenya enacted the Data Protection Act in 2019 (DPA) is the primary statute regulating data protection in Kenya.[1] It defines some key terms that are integral to data protection. To begin with, personal data is defined as any information relating to a natural person. Data subjects are the natural people that are the subject of personal data.[2] Consent is an informed indication by a data subject, that shows their acceptance to have their data processed. It is to be express, unequivocal, free, specific, and informed.[3] Acceptance should be communicated in a statement or by a clear affirmative action.[4] Data controllers handle the purpose and means of processing personal data.[5] While a data processor does the processing on behalf of a data controller.[6] However, to perform their duties they need to be registered by the Data Protection Commissioner as per Part III of the DPA.

DPA confers upon the controllers the power to transfer data to third parties.[7] Transfer of data is the process of exchanging large files of data between systems or organizations.[8] It is the act that collects, replicates, and transmits data.[9] Transfers happen between organizations that are

[1] --< https://www.dlapiperdataprotection.com/index.html?t=law&c=KE>-- on 5 November 2024.
[2] Section 2, Data protection act (2019).
[3] Section 2, Data protection act (2019).
[4] Section 2, Data protection act (2019).
[5] Section 2, Data protection act (2019).
[6] Section 2, Data protection act (2019).
[7] Section 2, Data protection act (2019).
[8] --https://www.informatica.com/services-and-training/glossary-of-terms/data-transfer-definition.html—on 5 November 2024.
[9] --https://www.informatica.com/services-and-training/glossary-of-terms/data-transfer-definition.html—on 5 November 2024.

business partners or have a contract between them obligating them to share the data.[10] They may be aimed at sharing, analyzing, or retaining data for storage.[11]

To transfer data to third parties, there are certain conditions that ought to be met. At the collection of personal data, they ought to inform data subjects of the third parties that will receive their personal data and what safeguards have been adopted.[12] Sometimes, the third parties may be based outside Kenya. The DPA has also provided for conditions for transfer of data out of Kenya in section 48, and the safeguards that exist and are to be adopted prior to the transfer in section 49. The study will delve deeper into these provisions in later chapters of the study.

Based on the specific purpose, the information collected may vary between low-risk data to high-risk data. Low-risk data can be used for explicit use by the public.[13] High-risk data cannot be shared to the public as it exposes data subjects to risks like identity theft.[14] The transfer of such data could expose it to unauthorized and unconsented exposure and/or loss. When transferring, it is important to ensure that data that is transferred is in line with the purpose of processing, reason for transfer, or performance of the contract with the third party.[15] However, since data is heavily dependent on each other, it then becomes challenging to decide what data to transfer and the data to leave behind.[16] This could lead the data controller or processor to transferring high-risk data to the third party when it is not in line with the purpose of transfer and processing that the third party is in control of.

In the case of ***Federation of Kenya Employers v Cabinet Secretary, Ministry of Foreign Affairs and International Relations & 4 others,*** a question on the conditions of transfer of data outside Kenya is raised.[17] This case arose from legal proceedings being carried out in Scotland between James Finlay's Company and its workers. The workers were aggrieved over issues of employment and work injuries. The Kenyan courts had issued injunctions stopping the

[10] --https://www.cyber.gc.ca/en/guidance/data-transfer-upload-protection-itsap40212- on 5 November 5 2024.
[11] --https://www.cyber.gc.ca/en/guidance/data-transfer-upload-protection-itsap40212- on 5 November 5 2024.
[12] Section 29 (d), Data protection act (2019).
[13] --https://it.cornell.edu/security-and-policy/data-types-high-risk-moderate-risk-low-risk#:~:text=High%2DRisk%20%2D%20Data%20that%20should,Credit%20card%20numbers—on November 2024.
[14] --https://it.cornell.edu/security-and-policy/data-types-high-risk-moderate-risk-low-risk#:~:text=High%2DRisk%20%2D%20Data%20that%20should,Credit%20card%20numbers—on November 2024.
[15] Section 48 (c), Data protection act (2019).
[16] --https://www.montecarlodata.com/blog-data-migration-risks-checklist/-- on 5 November 2024.
[17] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] KEELRC 3067 eKLR.

collection of evidence that was inconsistent with the laws of Kenya for the proceedings in Scotland.[18] While the case between the workers and James Finlay's Company was ongoing in Scotland, Federation of Kenya Employers filed this petition as they were apprehensive that the suit would involve transfer of sensitive personal data of employees in Kenya to the Scottish court.[19] They needed to ensure that the transfers adhered to Kenyan laws regulating data transfers.[20]

The data subjects had consented to the transfer of their data to the Scottish Court.[21] This raised an issue because, though they had consented, the transfer was without the approval from Kenya's Data Commissioner.[22] The petitioner sought to have this court decide whether this was in violation of section 48 of the DPA, even if the data subjects had consented and no complaint had been raised.[23]

1.2: STATEMENT PROBLEM

The Data Protection Act provided for its extraterritorial reach when it deals with data processors or controllers that are neither established nor resident in Kenya but process personal data of data subjects that are resident in Kenya. However, in the case of cross-border transfers, data controllers and processors engage with foreign entities that are often, not recognized as data controllers or processors in Kenya. In this case, these foreign entities receive sensitive personal data of data subjects protected by the DPA. The DPA has provisions that seek to mitigate the risks that arise from data transfers outside Kenya. However, it fails to determine whether it will be involved in regulating the processing of data once data leaves the country and how it will do so. This raise concerns on whether data collected from data subjects in Kenya is adequately protected once it leaves the country. The DPA should be able to regulate the processing, protect the rights of the data subject, and provide remedies to the data subjects even when the data leaves the country.

[18] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] eKLR.
[19] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] eKLR.
[20] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] eKLR.
[21] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] eKLR.
[22] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] eKLR.
[23] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] eKLR.

1.3: HYPOTHESIS

The DPA's failure to extensively provide for its extraterritorial reach creates a legal and institutional gap that brings about various limitations and challenges. It limits the access of justice for Kenyan data subjects and the protection of their personal data. The gap further creates a challenge in the understanding and knowledge data controllers and data subjects have on how to navigate data transfers outside Kenya. To fill these gaps and take control of the limitations and challenges, there is a need for the DPA to have extraterritorial reach. It ought to have the power to protect the rights of data subjects and regulate the processing of their data if it was regulating the processing of that data before it was transferred. This will allow data subjects to enjoy the same rights, protections and means of redress in respect of their personal data regardless of the location of the organization processing their data.

1.4: RESEARCH OBJECTIVES

1. To examine the challenges that arise in implementing and enforcing the DPA's provisions when data is transferred outside the country to be processed by a foreign entity.
2. To examine the current legal framework that regulates the transfer of personal data outside Kenya.
3. To examine the comparison between the Data Protection Act borrow from the General Data Protection Regulations.
4. To make policy or legal reforms that could be implemented to strengthen the DPA's extraterritorial enforcement mechanisms.

1.5: RESEARCH QUESTIONS

1. What challenges arise in implementing and enforcing the DPA when data transferred outside the country is being processed by a foreign entity?
2. What is the current legal framework regulating the transfer of personal data outside Kenya?
3. What is the comparison between the Data Protection Act borrow from the General Data Protection Regulations?
4. What policy or legal reforms could be implemented to strengthen the DPA's extraterritorial enforcement mechanisms?

1.6: JUSTIFICATION OF THE STUDY

This study is important because as the world gets more digitalized, data has become critical assets for businesses. Even as we view it critical for businesses to run, it is important to ensure that laws and regulations cover grounds that would lead to the misuse of data. The relevance of this study is to reveal an existing gap in law that is created by the lack of clarity in the Data Protection Act's extraterritorial reach and further provide solutions on how to fill the gap. It will take a keen look at the process and measures that the DPA has set out for transfer of data outside Kenya and how effective the processes and measures are. It will also look at whether the DPA has control over how data is processed and provides remedies for data subjects where contraventions happen. It aims at contributing to the existing literature on how effective the DPA is in protecting the rights of data subjects and ensuring that data controllers and processors comply with its provisions. By addressing these issues, it seeks to offer practical insights and recommendations that can aid policymakers and regulatory bodies in fostering a more robust and effective data protection environment.

1.7: THEORETICAL FRAMEWORK

1.7.1: Restricted Access/Limited Control theory

This theory was adopted by Tavani Herman. He aimed at articulating a definition of privacy that would serve as a foundation for an adequate theory of privacy and enable us to frame clear, transparent, and consistent online privacy policies.[24] Through this theory, Tavani defines privacy as the protection from intrusion, interference, and information access by others in whatever situation a person is in.[25] The situation could be a relationship, location, or access or storage of information.[26]

This study focuses on the aspect of normative privacy that Tavani differentiated from natural privacy.[27] The former can be violated and invaded and to prevent this, it provides a baseline for creating policies, laws, and practices that respect individual privacy while balancing other societal needs.

[24] Spreeuwenberg L, "Justifying a right to privacy," unpublished LLM thesis, Tilburg University, Tilburg, 2016, 11.
[25] Spreeuwenberg L, "Justifying a right to privacy," unpublished LLM thesis, Tilburg University, Tilburg, 2016, 11.
[26] Spreeuwenberg L, "Justifying a right to privacy," unpublished LLM thesis, Tilburg University, Tilburg, 2016, 11.
[27] Spreeuwenberg L, "Justifying a right to privacy," unpublished LLM thesis, Tilburg University, Tilburg, 2016, 11.

This theory is applicable to the study because data subjects enter contractual relationships with data controllers and processors, where the former allows the latter to process their personal data. This exposes the data subjects' data to risks like intrusion, interference, and unauthorized access. This theory reveals that for data subjects to enjoy their privacy, it needs to be protected from the risks. The Data Protection Act having an extraterritorial reach would enable its provisions to protect the data subject's data from these risks.

1.7.2: Stakeholder theory

This theory has been used in various contexts. It has been used to show the interconnection of relationships between an organization and its customers, suppliers, employees, investors, communities, and all that have a stake in the organization.[28] It can be dated back to Wagner Mainardes and Richard Edward Freeman.[29]

In the context of this study, stakeholders are people or groups that have legitimate interests in procedural and substantive aspects of privacy.[30] This includes data subjects, data controllers, data processors, and the regulating body. These stakeholders are pivotal to the success of the data protection legal framework.[31] This is because, through their interests the aspects of privacy, they are responsible for shaping, implementing, and adhering to the policies that govern the use and processing of data.[32] Each stakeholder has an interest, and these interests connect the stakeholders, creating a relationship among them. In data protection, the supreme goal is protecting the right to privacy that data subjects hold. To achieve this goal, there is a need to balance the needs and interests of the parties involved.[33]

---

[28] Introna L & Poloudi N, "Privacy in the information age: Stakeholders, interests, and values," Journal of business ethics, 1999, 34, --< https://www.researchgate.net/publication/226528834_Privacy_in_the_Information_Age_Stakeholders_Interests_and_Values?enrichId=rgreq-7b2715d03fa6a2abe40b6c64a6706621-XXX&enrichSource=Y292ZXJQYWdlOzIyNjUyODgzNDtBUzoxNTA3MjgxNDAxMzY0NTFAMTQxMjk0Nzc5NzE2Mg%3D%3D&el=1_x_2&_esc=publicationCoverPdf>-- on 19 December 2024.

[29] Introna L & Poloudi N, "Privacy in the information age: Stakeholders, interests, and values," Journal of business ethics, 1999, 34, --< https://www.researchgate.net/publication/226528834_Privacy_in_the_Information_Age_Stakeholders_Interests_and_Values?enrichId=rgreq-7b2715d03fa6a2abe40b6c64a6706621-XXX&enrichSource=Y292ZXJQYWdlOzIyNjUyODgzNDtBUzoxNTA3MjgxNDAxMzY0NTFAMTQxMjk0Nzc5NzE2Mg%3D%3D&el=1_x_2&_esc=publicationCoverPdf>-- on 19 December 2024.

[30] Introna L & Poloudi N, "Privacy in the information age: Stakeholders, interests, and values," Journal of business ethics, 1999, 34, --< https://www.researchgate.net/publication/226528834_Privacy_in_the_Information_Age_Stakeholders_Interests_and_Values?enrichId=rgreq-7b2715d03fa6a2abe40b6c64a6706621-XXX&enrichSource=Y292ZXJQYWdlOzIyNjUyODgzNDtBUzoxNTA3MjgxNDAxMzY0NTFAMTQxMjk0Nzc5NzE2Mg%3D%3D&el=1_x_2&_esc=publicationCoverPdf>-- on 19 December 2024.

[31] --https://www.secoda.co/blog/stakeholder-roles-in-data-governance--, on 19 December 2024.

[32] --https://www.secoda.co/blog/stakeholder-roles-in-data-governance--, on 19 December 2024.

[33] --https://www.secoda.co/blog/stakeholder-roles-in-data-governance--, on 19 December 2024.

1.8: LITERATURE REVIEW.

Ryngaert and Taylor M. begin by stating that the internet has brought about deterritorialization of the internet and international communications technology.[34] They say that this has brought about questions on who may regulate the activities on the internet.[35] This is justified by a territorial link between the GDPR and an activity or a person triggers its impact.[36] Meaning the activity being done within the European Union (EU) or its effects felt in the same region triggers jurisdiction.[37] Additionally, the person involved in the activities is in the EU. Foreign entities monitoring parties in the EU trigger the GDPR's jurisdiction.[38] Another ground is that of a person's affiliation with the EU.

With a specific look at health data sharing, Annelize McKay et al, emphasize the need for the improvement of regulatory frameworks that seek to promote health data sharing while addressing privacy concerns.[39] They highlight various privacy concerns that data sharing brings about. They show that there is a need to strike a balance between the advantages of data sharing and the protection of personal data.[40] They highlight that cross-border data sharing raises concerns about varying levels of data protection laws in different countries and the need for safeguards like Data Transfer Agreements.[41]

Stein A. says that the mobility of people and transactions has strained jurisdiction's dependence on the current location of the defendant.[42] Stein also talks about how the concept of corporate entities poses a challenge for the traditional notions of jurisdiction. The only place a corporation could be located would be the state where it is registered as a legal entity.[43] However, in this digital age, corporations extend their services and activities outside the territories of the states where they are incorporated. This then challenges the traditional territorial jurisdiction that assumes that power is tied to the physical presence within a state's borders.[44] Stein speaks on

[34] Ryngaert C. and Mistale T, "The GDPR as global data protection regulation?" Symposium on the GDPR and international law by the Cambridge University Press, 2019, 5.
[35] Ryngaert C. and Mistale T, "The GDPR as global data protection regulation?" 2019, 5.
[36] Ryngaert C. and Mistale T, "The GDPR as global data protection regulation?" 2019, 6.
[37] Ryngaert C. and Mistale T, "The GDPR as global data protection regulation?" 2019, 6.
[38] Ryngaert C. and Mistale T, "The GDPR as global data protection regulation?" 2019, 6.
[39] McKay A, Brand D, et al, "The regulation of health data sharing in Africa: A comparative study," Journal of law and biosciences, 11(1), 2024, 6.
[40] McKay A, Brand D, et al, "The regulation of health data sharing in Africa: A comparative study," 6
[41] McKay A, Brand D, et al, "The regulation of health data sharing in Africa: A comparative study," 6
[42] Stein A, "The unexceptional problem of jurisdiction in cyberspace," 32 (4), International lawyer, 1998, 1169.
[43] Stein A, "The unexceptional problem of jurisdiction in cyberspace," 1169.
[44] Stein A, "The unexceptional problem of jurisdiction in cyberspace," 1169.

a need for states to compromise or abandon their sovereign claims when it comes to matters related to cyberspace activities.[45]

Mistale T brings forward the idea that the EU's data protection laws' extraterritorial reach is because of its need to protect its citizens who are data subjects.[46] This is because the laws place focus on protecting the citizens. They set out that data transfers and processing of data outside the EU exposes citizens to the risk of having their right to personal data protected.[47]

Czerniawski M. and Svantesson state that extraterritoriality of the data protection laws is justified since failure to extend states' data protection laws is a failure to protect the rights of their citizens.[48] However, they argue that it is unreasonable as it is impossible for every internet user to adjust their conduct in alignment with data protection laws of all states that they come into contact with and it would make it difficult for businesses to engage in cross-border trade.[49]

Numerous studies explore the application of national legal systems over international jurisdictions and the challenges posed by cyberspace. However, there is a gap in understanding how these principles apply to the DPA, particularly cross border transfers. While debates on extraterritoriality focus on territorial connections and citizens' rights, the protection of Kenyan data subjects when their data is transferred abroad has received little attention. This study seeks to fill this void. It also aims at outlining current limitations and proposing reforms that enhance data protection.

1.9: METHODOLOGY

The method used in the research will be doctrinal legal research. This will be the standard desktop method where data shall be drawn from a historical and descriptive evaluation of the DPA to determine its extraterritorial reach. To add on to this, the study shall rely on primary and secondary sources of data.

With regards to the primary sources, the study seeks to analyze the existing laws regulating data transfers outside Kenya to examine the intention of legislators. To aid this, the study shall

[45] Stein A, "The unexceptional problem of jurisdiction in cyberspace," 1170.
[46] Mistale T, "The EU's human rights obligations in relation to its data protection laws with extraterritorial effect," 247.
[47] Mistale T, "The EU's human rights obligations in relation to its data protection laws with extraterritorial effect,"247.
[48] Czerniawski M and Svantesson D, "Challenges to the extraterritorial enforcement of data privacy law – EU case ResearchGate, 2023, 128.
[49] Czerniawski M and Svantesson D, "Challenges to the extraterritorial enforcement of data privacy law – EU case," ResearchGate, 2023, 128.

also rely on policy analysis to show the current framework on the same, both domestic and international. On the other hand, it shall use secondary sources that have analyzed and interpreted the existing legislature to support my argument and reach my conclusion. The secondary sources shall also be relied upon to delve into to identify existing best practices for the data transfers.

2.0: Chapter breakdown

Chapter one details the introductory part of this chapter. It sets out the background of the study, research questions and objectives. It also provides for the foundations of the subsequent chapters, like the statement problem, hypothesis, justification of the study, literature review, the study's methodology, and chapter breakdown.

Chapter two will examine the challenges that arise in implementing and enforcing the DPA's provisions when data that is transferred outside the country is being processed by a foreign company. This is from the lens of case studies. It will examine the bases of jurisdiction and the role of extraterritoriality in data protection laws. It will also make an analysis of case studies.

Chapter three seeks to delve into the existing legal framework on data protection as it looks at the importance that has been placed on data protection through the key developments leading up to the adoption of the Data Protection Act in 2019. It shall look at the provisions providing for data transfers and their effectiveness.

Chapter four will then provide legal and institutional reform in Kenya, that would strengthen the mechanisms, safeguards and provisions that cater to data transfers. It will also set out the study's conclusion,

CHAPTER 2: THE CHALLENGES OF CROSS BORDER TRANSFERS

Introduction

This chapter relies on case studies with the aim of outlining the difficulties and constraints of extraterritorial enforcement of Kenya's Data Protection Act (DPA). This analysis is based on a more general discourse of data protection vulnerabilities in the global context and their impact on Kenyan regulation.

2.1: Extraterritorial jurisdiction

2.1.1: Bases of jurisdiction

Jurisdiction varies depending on what it seeks to achieve. The different types of jurisdiction that exist are the jurisdiction to prescribe, jurisdiction to enforce, jurisdiction to function and jurisdiction to adjudicate.[50] Among these, attention has been more focused on the jurisdiction to prescribe.[51] Through the jurisdiction to prescribe, a state has the right to apply its laws to the activities, relations, interests, or status of persons.[52] A state could do this by legislation, executive order or act, administrative rule or regulation, or by the determination of a court.[53] To have grounding for jurisdiction, a state could have subjective territoriality, objective territoriality, nationality, protective principle, passive nationality, or universality.[54] A state does not need all of these bases to be present for their jurisdiction over a matter to be justified. They only need one base to be present.[55]

Subjective territoriality allows a state to have jurisdiction over matters that take place within its territory.[56] Where an act is committed outside the borders of a state, but its effects are felt within its state, objective territoriality allows the state to exercise their jurisdiction.[57] The nationality of the actor (one that causes the action in contention to occur) grants the actor's state the jurisdiction.[58] A state could feel threatened by the actions occurring in another state

[50] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 4(1), Michigan telecommunications law review, 1998, 71.
[51] Ryngaert C, "The concept of jurisdiction in international law," unpublished, Utrecht University, Utretcht, 5.
[52] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 71.
[53] Ryngaert C, "The concept of jurisdiction in international law," unpublished, Utrecht University, Utretcht, 5.
[54] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 71.
[55] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 71.
[56] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 71.
[57] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 71.
[58] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 71.

and based on this, they acquire jurisdiction through the protective principle.[59] Passive nationality is invoked where the nationality of the victim to the actor's actions is considered the basis for granting a state jurisdiction.[60] The universal jurisdiction, also known as the universal interest, gives states the right to capture and punish actors of crimes like slavery, genocide, and air piracy (hijacking).[61]

2.1.2: The role of extraterritoriality in data privacy laws

The need for data privacy laws to have extraterritorial reach arises for various reasons. To begin with, governments have an interest in providing for effective protection of their citizens' rights despite the existing territorial confines.[62] With the increased emphasis on the right to privacy as a human right, it would be undesirable to have governments not take extra steps to ensure that this right is protected. There is also an increased commercialization of data.[63] Data has become an asset that is sought after for various commercial reasons by commercial enterprises. There ought to be a balance between the commercial enterprises' need for the data and the protection of the personal data. An overreliance on the former at the expense of the latter would pose a risk to the right of privacy that data subjects should enjoy.

In this digital era, data subjects share their data voluntarily in their day-to-day interactions with the internet through social media platforms.[64] Because the internet blurs the geographical barriers, these interactions are not limited to the data subjects' territory of residence. This necessitates the extraterritoriality of data protection laws to ensure that even as they share their data voluntarily, their data is protected from data risks. Personal data has also been commodified.[65] This means that personal data has been turned into a form of currency where access to certain online services is paid for by accepting to provide the data.[66] This may mean that the services accessed are free, however, this may prevent parties looking at the security risks associated with sharing their data on such conditions.

---

[59] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 71.
[60] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 71.
[61] Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 71.
[62] Kuner C, Cate F, et al, "The extraterritoriality of data privacy laws- an explosive issue yet to detonate," 3(3), International Data Privacy Law, 2013, 147.
[63] Kuner C, Cate F, et al, "The extraterritoriality of data privacy laws- an explosive issue yet to detonate," 147.
[64] Kuner C, Cate F, et al, "The extraterritoriality of data privacy laws- an explosive issue yet to detonate," 147.
[65] Kuner C, Cate F, et al, "The extraterritoriality of data privacy laws- an explosive issue yet to detonate," 147.
[66] Kuner C, Cate F, et al, "The extraterritoriality of data privacy laws- an explosive issue yet to detonate," 147.

This goes to show that data protection laws ought to have an extraterritorial reach. This is not to seek for wide reach but solely with an aim of ensuring that data is secure even as it crosses borders.

2.2 Risks Involving International Transfer of Data

The risks emerging from cross-border data transfers are especially high when it comes to the categories of data that have high risks now, including biometric and financial data.[67] This is because when such data is mishandled or misused, it could cause significant harm to the data subjects. There is a heavy disregard and ignorance of corporations for their data protection obligations under the data protection laws. In 2021, a survey was done in Kenya where it was shown that while there exist strong data protection regulations, only 36% of the Kenyan businesses were aware of the existence of these privacy laws.[68] The survey further showed that among the 36%, 77% of them had data protection policies that catered to protection of customers' data. However, despite this knowledge, only 56% applies their policies strictly.[69] Monetization of personal data is a major priority to cooperations that they fail to pay due regard to the right to privacy that data subjects are entitled to with regards to their personal data.

In 2021, Ireland's Data Protection Commission (DPC) fined WhatsApp 29 billion Kenyan Shillings for its failure to explain its data processing practices in its privacy notice.[70] In 2022, the French Data protection Office fined Google with a KES 11.6 billion fine for its failure to deploy proper cookie consent procedures on YouTube.[71] In 2023, META, the Facebook owner, was fined KES 11.7 billion for mishandling data by the Irish Data Protection Commissioner. This was following an investigation into how passwords are stored.[72]

In this digital era, most Kenyans use WhatsApp, Facebook, and YouTube, in their quest to connect with the rest of the world, educate themselves, acquire services all around the world, and even work. This means that all the companies that are mentioned above that have been

---

[67] --https://itlawco.com/transfer-personal-data-out-of-kenya/#:~:text=Failure%20to%20comply%20with%20the,impact%20an%20organisation's%20financial%20standing—on 20 December 2024.
[68]--https://www.kictanet.or.ke/cross-border-data-transfers-safeguarding-privacy-in-a-data-monetisation-world/--, on 20 December 2024.
[69]--https://www.kictanet.or.ke/cross-border-data-transfers-safeguarding-privacy-in-a-data-monetisation-world/--, on 20 December 2024.
[70]--https://www.kictanet.or.ke/cross-border-data-transfers-safeguarding-privacy-in-a-data-monetisation-world/--, on 20 December 2024.
[71] --https://www.kictanet.or.ke/cross-border-data-transfers-safeguarding-privacy-in-a-data-monetisation-world/--, on 20 December 2024.
[72] --https://www.bbc.com/news/technology-65669839--, on 20 December 2024.

fined, are corporations that receive data from data subjects in Kenya. Their failure to uphold the data protection regulations poses a risk on the personal data that they receive. Despite the companies receiving fines, it is unclear that they took steps to ensure that the previous breaches were remedied. Prior to its name change, META was alleged to be involved in data mining and illegal sharing of data. It was also accused of deliberate data breaches such as selling private user information to advertisers.[73] This serves as a clear indication that there are actionable points that affected data subjects in Kenya but no clear action by the ODPC in this case or any other case affecting Kenyan subjects.

This shows that personal data is highly valued by commercial enterprises and that its monetization is growing. This has driven such enterprises to overlook protecting the data in their pursuit of following the current trend of digitization and e-commerce. This puts personal data at heavy risk. Due to this, special attention needs to be paid by Data Protection Agencies to ensure that proper balance is maintained despite the need to follow the digitization and e-commerce trends.

2.3: Case Study 1: Federation of Kenya Employers v Cabinet Secretary, Ministry of Foreign Affairs and International Relations & 4 others

2.3.1: Background

This case originates from an industrial court case in Scotland involving James Finlay's Company and its employees. The order by the Scottish courts compelling the transfer of employee data, which include information such as biometric data, identity numbers and other personal information could be in breach of Kenya's Data Protection Act.[74] Even though the data subjects provided their consent for the transfer, the ODPC approval was not obtained.[75] This led to a petition on whether such a transfer constitutes a breach of Section 48 of the DPA.

2.3.2: Analysis

The case highlights a critical gap in the DPA: that there is no specific legal provision that specifically assigns the ODPC with legal oversight and or regulation of data once it has been

[73] --https://www.kictanet.or.ke/cross-border-data-transfers-safeguarding-privacy-in-a-data-monetisation-world/--, on 20 December 2024.
[74] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] KEELRC 3067 eKLR.
[75] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] KEELRC 3067 eKLR.

transferred out of Kenya.[76] While the data subjects made their consent, ODPC non-interference was a departure from the Act's spirit of protecting their personal data.[77] Additionally, outsourcing data protection laws thereof to other nations which may not be at par with Kenya exposes data subjects to high risks in their privacy. It once again points to the question about the possibility of enforcing regional regulations at the international level.

2.3.3: Implications

This case shows why the extraterritorial application also needs to be addressed under the Kenyan DPA in order to safeguard the rights of Kenyan data subjects wherever their data is. It also specifies another aspect of cooperation between Kenya's ODPC and foreign control authorities in order to create the basis for compliance. Possible legal obstacles to future cross-border data transfers could be averted by demanding enhanced regulation.

2.4 Case Study 2: Huduma Namba Data Concerns

2.4.1: Background

The Huduma Namba introduced by Kenyan government to provide unique numbers to its citizens to organize their data collected in one place was a major concern for data privacy and security.[78] The National Integrated Identity Management System (NIIMS) enrollment form contained a disclaimer that data collected would be shared with third parties.[79] This raised concerns because collection as well as the possible disclosure of the personal information of the citizens of Kenya with the third-party service providers including those in the other countries posed certain risks of misuse as well as the violations of the privacy of the individuals.[80] Suspicion arose in 2020 as it was said that some information gathered under this campaign could be reportedly exempt from the purview of Kenya DPA.

---

[76] The National Council for Law Reporting. "Petition E085 of 2023." Kenya Law, 2023. -- http://kenyalaw.org/caselaw/cases/view/274776/--

[77] CMS. "Transfer Of Personal Data Outside Kenya." CMS Law.Tax, 2024. --https://cms.law/en/ken/news-information/transfer-of-personal-data-outside-kenya—on 14 December 2024.

[78] Kenya Human Rights Commission. "Judgement on NIIMS (Huduma Namba)," February 6 2020, -- https://khrc.or.ke/publication/judgement-on-niims-huduma-namba/--, on 14 December 2024.

[79] Nubian Rights Forum & 2 others v Atttorney General & 6 others; Children Welfare Society & 9 others (Interested Parties) [2020] eKLR.

[80] Business Daily. "Privacy, Data Safety Fears over Huduma Namba," April 7 2019, -- https://www.businessdailyafrica.com/bd/opinion-analysis/letters/privacy-data-safety-fears-over-huduma-namba-2245390—on 14 December 2024.

2.4.2: Analysis

This case portrays an existing tension between achieving national interests towards digitization and protecting individual rights on privacy. As for the enforcement, it pointed towards limitations such as absence of information whether the data shared with foreign service providers complied with the measures specified under Section 49 of the DPA.[81] Furthermore, the scarcity of comprehensive Data Protection Impact Assessments (DPIAs) before that type of transfers only amplified uncertainties on the correct use of information.[82] The Huduma Namba case is a perfect example of the consequences where transparency and enforcement measures are insufficient.

2.4.3: Implications

The controversy that surrounds Huduma Namba underscore the necessity of higher tolerance measures, stricter DPIAs requirements and more vigilant monitoring of the ODPC. It also underscores the need to develop trusting relations with the public and respect data protection laws that apply during cross-border data transfers through national activities. Preventive steps could help to reduce threats and provide people with more confidence about the protection of their information.

2.6: Challenges that arise in implementing and enforcing the DPA's provisions extraterritorially

The ODPC faces several challenges in enforcing the DPA's provisions for data transfers outside Kenya:

2.6.1: NEGATIVE – Extraterritorial jurisdiction

The DPA has extraterritorial applicability that is based on section 4. This means that it applies to data controllers and processors who are based in foreign countries, but they process the personal data of individuals located in Kenya.[83] It further provides for administrative, criminal, and civil remedies for non-compliance.[84] The issue that arises from this is that the DPA does

[81] Kenya Human Rights Commission. "Judgement on NIIMS (Huduma Namba)," February 6 2020 -- https://khrc.or.ke/publication/judgement-on-niims-huduma-namba/-- 14 December 2024.
[82] Bowmans. "Application of the Data Protection Act in Kenya: The 'Huduma Namba Decision,'" October 19, 2021, --https://bowmanslaw.com/insights/application-of-the-data-protection-act-in-kenya-the-huduma-namba-decision/-- on 14 December 2024.
[83] --< https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/TMT/technology-media-telecommunications-alert-6-september-The-foreign-applicability-of-the-Kenyan-Data-Protection-Act-.html#:~:text=The%20DPA%20has%20extraterritorial%20applicability,of%20individuals%20located%20in%20Kenya>-- on 15 December 2024.
[84] --< https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/TMT/technology-media-telecommunications-alert-6-september-The-foreign-applicability-of-the-Kenyan-Data-Protection-Act-

not furnish the ODPC with extraterritorial authority to supervise or enforce compliance with the law once data has left the country to a foreign entity that is not registered as a data processor or controller in Kenya. Such limitations expose data subjects to privacy invasion in countries that lack strong data protection laws. Their absence reduces the effectiveness of the DPA.

2.6.2: Resource Constraints

The founder of Africa Digital Rights' Hub, Teki Akuetteh, noted that for the successful and effective implementation of data protection laws, there is a need to address the issue of whether the data regulating authorities have adequate resources to do so.[85] There is inadequate funding, staff, and skill to monitor and ensure compliance with the set standards within the ODPC.[86] Challenges with regards to funding creates hurdles for the functioning of the ODPC.[87] It prevents the office from engaging in activities like recruiting, training staff, and investigating and further affects the effectiveness of their investigations and their capacity to carry out their responsibilities. They are further compounded in cases of cross border transfers as monitoring entails sophisticated technological and legal acumen[88]. Data protection laws are always trying to catch up with these advancements which increases the burden that exists on the ODPC to ensure that even with the advancements, the DPA provisions are complied with. These are some of the constraints that need to be overcome for proper enforcement.

2.7: Conclusion

In this chapter, the study has had the chance to bring out the importance of bestowing data protection laws with an extraterritorial reach. Using case studies, the difficulties and drawbacks related to the extraterritorial application of the DPA have been revealed and discussed. This goes to show that this is an existing problem in Kenya that needs to be tackled. Without the data protection laws' extraterritorial reach, data subjects are open to be preyed upon by commercial enterprises.

.html#:~:text=The%20DPA%20has%20extraterritorial%20applicability,of%20individuals%20located%20in%20Kenya>-- on 15 December 2024

[85] Adapt, "Understanding the challenges data protection regulators face: A global struggle towards implementation, independence, & enforcement,"17.

[86] KICTANET, "New Report Identifies Achievements, Challenges and Recommendations to Enhance Data Protection in Kenya." KICTANet Think Tank, 2024, --https://www.kictanet.or.ke/new-report-identifies-achievements-challenges-and-recommendations-to-enhance-data-protection-in-kenya/--

[87] Adapt, "Understanding the challenges data protection regulators face: A global struggle towards implementation, independence, & enforcement,"17.

[88] KICTANET, "New Report Identifies Achievements, Challenges and Recommendations to Enhance Data Protection in Kenya." KICTANet Think Tank, 2024, --https://www.kictanet.or.ke/new-report-identifies-achievements-challenges-and-recommendations-to-enhance-data-protection-in-kenya/--

CHAPTER 3: LEGAL FRAMEWORK

INTRODUCTION

This chapter delves into what the law prescribes with regards to the right to privacy in connection with data protection. It will analyze the provisions of the DPA and the Data Protection (General) Regulations. It will place special focus on what the law provides with regards to cross-border transfers and its jurisdictional reach

3.1: The right to privacy

This right is protected in the 2010 Constitution of Kenya.[89] It provides that no person ought to be subjected to arbitrary or unnecessary interference with their privacy, family, home, property, privacy of their communications, or information that relates to their family or private affairs.[90] It seeks to protect human dignity.[91]

3.2: The Data Protection Act, 2019

Due to the growth of technology and the internet, this right evolved to entail the obligation of the protection of personal data.[92] Before the enactment of the DPA , there was an attempt to regulate data protection through two bills in 2009 and 2012.[93] The 2009 bill did not intend to regulate data handled by the private sector.[94] They both only dealt with automated processing of data.[95] While the 2009 bill sought to create a data protection commission, the 2012 bill provided that duty to the existing government ombudsman.[96] The two bills failed to be introduced to the parliament because they were lacking.[97] They neither addressed the rights of data subjects nor did they address issues pertaining to consent.[98] They also failed to address data residency, portability, and cross border transfers.[99]

The lack of regulations on data protection placed a reliance of data protection on Article 31 of the Constitution of Kenya.[100] This is because, the right to privacy entails the right to

[89] Article 31, Constitution of Kenya (2010).
[90] Article 31, Constitution of Kenya (2010).
[91] Universal Periodic Review Stakeholder Report, "The right to privacy Kenya," 25 November 2024, 2.
[92] Universal Periodic Review Stakeholder Report, "The right to privacy Kenya," 25 November 2024, 2.
[93] --https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf—on 25 November 2024.
[94] --https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf—on 25 November 2024.
[95] --https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf—on 25 November 2024.
[96] --https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf—on 25 November 2024.
[97] --https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf—on 25 November 2024.
[98] --https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf—on 25 November 2024.
[99] --https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf—on 25 November 2024.
[100] Tavani H. "Philosophical theories of privacy: implications for an adequate online privacy policy," Metaphilosophy, volume 38, No.1, --https://www.jstor.org/stable/24439672--, on 22 January 2024.

information privacy.[101] This is the right to be protected from unsolicited interference and unnecessary revelation or acquisition of information that is tied to family or private affairs.[102] It is attached to the protection from the infringement of the privacy of communications.[103] Data protection entails the regulation of the handling and processing of personal data and the compliance of the safeguards of personal information.[104] Recognizing the need for a statute that catered to this regulation and providing safeguards, the DPA was adopted in 2019 giving effect to Article 31 of the 2010 Constitution of Kenya.[105]

3.2.1: Objectives of the Data Protection Act

The objectives are provided for in section 3. They reveal an effort to regulate the processing of personal data.[106] It limits the processors and controllers' power to control and process personal data by providing for their duties and creating the Office of the Data Commissioner, that is the regulating body. By setting out the principles of processing data in section 25, it seeks to ensure that any processing is guided and done within the confines of the principles.[107] It also seeks to provide protection to the right to privacy.[108] Though this right can be limited, significant efforts ought to be made to ensure that it is not unlawfully limited. To achieve this, it provides data subjects with rights and remedies, which is also an objective.[109] Lastly, it aims at establishing both legal and institutional mechanisms that will protect personal data.[110]

3.3: The Data Protection (General) Regulations 2021

In the exercise of the powers conferred to the Cabinet Secretary in section 71 of the DPA, the Data Protection (General) Regulations were enacted in 2021, 'the regulations.' They set out the procedures for the enforcement of the rights of the data subjects. They also elaborate on the duties and obligations of data controllers and data processors. Since they work to give effect to the DPA, it works in a similar scope to the act.

---

[101] Article 31 (c), The constitution of Kenya (2010).
[102] Tavani H. "Philosophical theories of privacy: implications for an adequate online privacy policy.
[103] Erforth B. and Martin-Shields, "EU-Kenya cooperation in data protection," *Where privacy meets politics,* 146.
[104] Nyaga B. et al, "Mediation and data protection law in Kenya: Appraising ADR for oprimac access to justice to justice under the DPA 2019," SSRN, 11.
[105] Vikram C. and Ruby N, "The data protection act 2019, Kenya," A.B Patel & Patel LLP, -- https://www.abpateladvocates.com/data_protection_act_2019_kenya.php—on 25 November 2024.
[106] Section 3 (a), Data Protection Act, 2019.
[107] Section 3 (b), Data Protection Act, 2019.
[108] Section 3 (c), Data Protection Act, 2019.
[109]Section 3 (e), Data Protection Act, 2019
[110] Section 3 (d), Data Protection Act, 2019

The regulations do not apply to civil registration entities.[111] Such entities are described as the public agencies that are responsible for processing of personal data relating to registration of births, adoptions, person, issuance of passports and other identity documents, registration of marriages, and/or deaths.[112]

In accordance with section 32 of the DPA that deals with the conditions of consent, section 4 speaks to the informed nature of consent. Controllers or processors ought to give a data subject certain information prior to processing their data like the identity of the data controller or processor, the purpose of each processing operations that consent is sought for, and the type of personal data that they seek to collect.[113] Also, informing them of the use of personal data for automated decision-making where relevant[114]. In addition to that, whether the personal data shall be shared with third parties, the right to withdraw consent, and the implication of providing, withholding, or withdrawing consent.[115] This information may be presented to the data subject through a written notice, an oral statement, audio message, or video message.[116]

It also provides for grounds in which a data subject may seek the restriction of the processing of their personal data.

3.4: Core provisions

Section 4 provides the DPA's provisions should be applied where a data controller or processor enters personal data that is meant to process in a record.[117] The personal data may be entered into the record through automated or non-automated means.[118] If entered through the latter means, it ought to form part of the filing system or the whole of it.[119] For the DPA to apply to the data controller or processor, they ought to be processing data of data subjects that are located in Kenya.[120] This is whether the data controller or processor is established or a resident in Kenya or not.[121]

[111] Section 3, Data Protection (General) Regulations (2021).
[112] Section 3, Data Protection (civil registration) Regulations (2020).
[113] Section 4 (1), Data Protection (General) Regulations (2021).
[114] Section 4 (1), Data Protection (General) Regulations (2021).
[115] Section 4 (1), Data Protection (General) Regulations (2021).
[116] Section 4 (2), Data Protection (General) Regulations (2021).
[117] Section 4 (a), Data Protection Act (2019).
[118] Section 4 (a), Data Protection Act (2019).
[119] Section 4 (a), Data Protection Act (2019).
[120] Section 4 (b), Data Protection Act (2019).
[121] Section 4 (b), Data Protection Act (2019).

Section 5 provides for the establishment of the Office of the Data Protection Commissioner.[122] Its functions and powers are provided for in section 9 of the act. Section 18 then provides that a person can only act as a data controller or processor if they are registered as one with the Data Commissioner.[123] It provides what the application ought to entail. Part III of the act provides the situations that may cause a data controller or processor to have their certificate cancelled after registration with the ODPC.[124]

Part IV of the act provides for the principles and obligations of personal data protection. With section 25 providing the principles of data protection and section 26 providing for the rights of a data subject. It also speaks to instances where the data subject is unable to carry out the rights conferred to them because of factors like mental capacity.[125] In such instances, it is provided that the rights of a data subject can be conferred on a third party.[126]

3.5: Jurisdictional reach of the Data Protection Act

3.5.1: Cross-border data transfers

Cross-border data transfers entail the transfer of personal data across international borders.[127] With the growth of the internet and endless technological innovations, data can be shared among international organizations seamlessly.[128]

Data controllers and processors are provided with the conditional power to transfer personal data outside Kenya. The DPA and the regulations provide for the measures to be taken prior to the transfer of personal data outside Kenya. This is in sections 48 and 49 of the DPA and Part VII of the regulations.

The DPA provides that data processors and controllers cannot transfer personal data out of Kenya without proving to the Data Commissioner that safeguards exist to ensure that personal data is secure and protected.[129] They also need to ascertain that an adequacy decision has been made by the data commissioner.[130] This is where the Data Commissioner makes a decision that

[122] Section 5(1), Data Protection Act (2019).
[123] Section 18 (1), Data Protection Act (2019).
[124] Section 22, Data Protection Act (2019).
[125] Section 27, Data Protection Act (2019).
[126] Section 27, Data Protection Act (2019).
[127] Akintola S, "Cross border transfer of personal data," Africa Legal Network, 25 July 2023, -- https://aln.africa/insight/cross-border-transfer-of-personal-data/-- on 25 November 2024.
[128] Akintola S, "Cross border transfer of personal data," Africa Legal Network, 25 July 2023, -- https://aln.africa/insight/cross-border-transfer-of-personal-data/-- on 25 November 2024.
[129] Section 48 (a), Data Protection Act (2019).
[130] Regulation 40, The Data Protection (General) Regulations (2021).

there is an adequate level of protection of personal data by the other country, territory, specified sectors in that territory, or the international organization.[131] Where this decision is made, the list of countries, territories, and organizations that have received its approval may be published on the ODPC's website to mark them 'safe' for transfer.[132]

They should also ascertain that the consent of the data subject has been given.[133] They also ought to prove that the recipient's territory has commensurate data protection laws.[134] These laws ought to be binding to the recipient.[135] If not, through an assessment, the data controller concludes that there exist appropriate safeguards to protect personal data.[136]

A country is deemed to have the appropriate safeguards if they have either of the following. Firstly, their ratification of the African Union Convention on Cyber Security and Personal Data Protection.[137] If not, the country ought to have a data protection agreement with Kenya that is reciprocal.[138] Lastly, if there are contractual binding corporate rules among a concerned group of undertakings or enterprises.[139]

The validity of the corporate rules relies on the following factors. Firstly, that every party to it is legally bound by it.[140] On top of that, that they apply to and are enforced by each member of the parties to the contract, including their employees.[141] That they provide data subjects enforceable rights with regards to how their data is processed.[142] Lastly, that they follow the requirements that the Data Protection (General) Regulations provide.[143]

On top of that, transfers have to be from a place of necessity.[144] As per the regulations, it ought to be ascertained prior to the transfers.[145] These necessities include the performance of a contract that a data controller or processor has with a data subject.[146] Where there was pre-contractual measure taken because of the data subject requests, if the transfer is necessary for

[131] Regulation 44 (1), The Data Protection (General) Regulations (2021).
[132] Regulation 44 (2), The Data Protection (General) Regulations (2021).
[133] Regulation 40, Data Protection (General) Regulations (2021).
[134] Section 48 (b), Data Protection Act (2019).
[135] Regulation 41 (1), Data Protection (General) Regulation (2021).
[136] Regulation 41 (1), Data Protection (General) Regulation (2021).
[137] Regulation 42 (a), Data Protection (General) Regulations (2021).
[138] Regulation 42 (b), Data Protection (General) Regulations (2021).
[139] Regulation 42 (c), Data Protection (General) Regulations (2021).
[140] Regulation 43 (1) (a), The Data Protection (General) Regulations (2021).
[141] Regulation 43 (1) (a), The Data Protection (General) Regulations (2021).
[142] Regulation 43 (1) (a), The Data Protection (General) Regulations (2021).
[143] Regulation 43 (1) (a), The Data Protection (General) Regulations (2021).
[144] Section 48 (c), Data Protection Act (2019).
[145] Regulation 40 (c), Data Protection (General) Regulations (2021).
[146] Section 48 (c) (i), Data Protection Act (2019).

the implementation of these measures, it qualifies as a ground for transfer.[147] It further provides that any matter pertaining to public interest qualifies as a necessity as it entails the public's well-being.[148]

Where there is a need to complete or perform a complete contract between the data controller and another party, personal data may be transferred.[149] However, this is only if the contract was performed or concluded in the interest of the data subjects.[150] In addition to that, data could be transferred if the data controller or processors needs to establish, exercise, or defend a legal claim.[151] A company can operate in various countries and process data of data subjects that are not in the country they are registered as legal entities increasing their chances of getting involved in legal procedures and claims in any of these countries. This provision creates room for these entities to cooperate with law enforcement officials of these countries.

The instances where the data can be transferred without the consent of the data subjects happen only when the data subject is incapable of giving consent physically or legally.[152] The data transfer ought to aim at protecting their vital interests.[153] Lastly, the necessity could be a compelling legitimate interest that the data controllers or processors pursue.[154] However, the interests, rights and freedoms of data subjects have priority.[155]

The DPA provides safeguards to be adopted prior to these transfers. Firstly, only a data subject's consent to the transfer of their data outside Kenya can effect the transfer.[156] A data subject ought to be informed of the data transfer, the company or institution that will receive their data, why their data is being transferred, whether it is necessary, the risks connected to the transfers, and the safeguards adopted to curb the risks. There is also a need for the confirmation of appropriate safeguards that have been adopted.[157]

The Data Commissioner may also request the data controller or processor to demonstrate how effective the safeguards adopted to ensure the data is secure and protected during the transfer

[147] Section 48 (c) (i), Data Protection Act (2019).
[148] Section 48 (c) (iii), Data Protection Act (2019).
[149] Section 48 (c) (ii), Data Protection Act (2019).
[150] Section 48 (c) (ii), Data Protection Act (2019).
[151] Section 48 (c) (iv), Data Protection Act (2019).
[152] Section 48 (c) (v), Data Protection Act (2019).
[153] Section 48 (c) (v), Data Protection Act (2019).
[154] Section 48 (c) (vi), Data Protection Act (2019).
[155] Section 48 (c) (vi), Data Protection Act (2019).
[156] Section 49 (1), Data Protection Act (2019).
[157] Section 49 (1), Data Protection Act (2019).

are.[158] They may also request a demonstration of the existence of the compelling legitimate interests that the data controllers or processors deem necessitates the transfers.[159]

To protect the rights and freedoms of the data subjects, the Data Commissioner may prohibit or suspend cross-border transfers.[160] They can further provide conditions the data controllers or processors need to meet for the transfers to happen.[161]

3.5.3: The Data Protection Act's extraterritorial reach

Extraterritorial jurisdiction may be understood as a state's extension of its legal powers outside its territory.[162] These legal powers may include an attempt to impose, apply, or enforce the state's national legislation.[163] Traditionally, the territory of a state defined the limits of its jurisdiction.[164] However, we are in an era of digital businesses and transnational companies because of the advent of the internet.[165] Such companies are registered as legal entities in one state; however, they operate beyond the territory of the said state. This, and the flow of data transnationally has presented a significant challenge to the jurisdictional boundaries that once existed.[166]

To factor this in, countries have included extraterritorial application clauses in their privacy laws. [167] The inclusion of such clauses reveals a state's need and desire to protect the personal data of its citizens despite it being processed outside their borders.[168] They aim to protect the data from harmful conduct by multinational entities that are in other states.[169]

We see this move being taken up by the DPA through section 4. The DPA reveals its power to govern and regulate the processing of personal data by a data controller or processor that may

[158] Section 49 (2), Data Protection Act (2019).
[159] Section 49 (2), Data Protection Act (2019).
[160] Section 49 (3), Data Protection Act (2019).
[161] Section 49 (3), Data Protection Act (2019).
[162] --< https://globalnaps.org/issue/extraterritorial-jurisdiction/>-- , on 26 November 2024.
[163] --< https://data-privacy-office.eu/navigating-the-jurisdictional-chaos-an-international-law-perspective-on-the-extraterritorial-application-of-data-protection-laws/>-- , on 27 November 2024.
[164] --< https://data-privacy-office.eu/navigating-the-jurisdictional-chaos-an-international-law-perspective-on-the-extraterritorial-application-of-data-protection-laws/>-- , on 27 November 2024.
[165] --< https://data-privacy-office.eu/navigating-the-jurisdictional-chaos-an-international-law-perspective-on-the-extraterritorial-application-of-data-protection-laws/>-- , on 27 November 2024.
[166] --< https://data-privacy-office.eu/navigating-the-jurisdictional-chaos-an-international-law-perspective-on-the-extraterritorial-application-of-data-protection-laws/>-- , on 27 November 2024.
[167] --< https://data-privacy-office.eu/navigating-the-jurisdictional-chaos-an-international-law-perspective-on-the-extraterritorial-application-of-data-protection-laws/>-- , on 27 November 2024.
[168] --< https://data-privacy-office.eu/navigating-the-jurisdictional-chaos-an-international-law-perspective-on-the-extraterritorial-application-of-data-protection-laws/>-- , on 27 November 2024.
[169] --< https://data-privacy-office.eu/navigating-the-jurisdictional-chaos-an-international-law-perspective-on-the-extraterritorial-application-of-data-protection-laws/>-- , on 27 November 2024.

not be established or have an ordinary residence in Kenya.[170] The processing may not even be done within the country.[171] What links these controllers and processors to the DPA's regulation is the processing of data subjects' data who are in Kenya.[172] However, for this section to have power over a transnational company, the institution ought to be recognized as a data controller or processor in Kenya. Meaning, they ought to be registered as data controllers or processors.[173]

Through this provision, the Data Protection Act takes up the prescriptive type of jurisdiction. This is because it seeks to have its provisions applicable to govern the processing done by an institution that is not located in Kenya but is recognized as a data processor or controller in Kenya. It draws its basis from the fact that the data subject is a citizen of Kenya. Through this we find that the jurisdictional bases are objective territoriality because the effects of unlawful processing of the data subjects' data will be felt in Kenya and when that happens, passive nationality will be invoked because the victims of the unlawful processing are Kenyan nationals.

3.6: Conclusion

It is important to understand that the DPA applies to processing that is done by data controllers and processors recognized in Kenya by the ODPC. This recognition is earned only by registration through the ODPC. The DPA and the regulations provide for safeguards and mechanisms meant to ensure that data transfers outside the country is safe. This chapter has provided insight into what the law prescribes on the matter.

VT OMNES VNVM SINT

[170] Section 4 (b), Data Protection Act (2019).
[171] Section 4 (b), Data Protection Act (2019).
[172] Section 4 (b), Data Protection Act (2019).
[173] Section 18 (1), Data Protection Act (2019).

Chapter 4: Comparative analysis between the General Data Protection Regulations and the Kenyan Data Protection Act.

4.1: Introduction.

The General Data Protection Regulations (GDPR) is known for the strictness of its provisions on the processing of personal data. This is because it seeks to ensure that the EU citizens' fundamental right to privacy is protected. Due to both the GDPR and DPA having similar aims, this chapter seeks to draw a comparison between both. This aims at revealing their strengths, weaknesses, and what the DPA could borrow from the GDPR with a key focus on cross-border data transfers.

4.2: HISTORICAL CONTEXT OF THE GENERAL DATA PROTECTION REGULATIONS

Leaders of the EU held talks on how they could ensure that peace and prosperity prevailed.[174] They found that the solution was to encourage international cooperation and reconstruction.[175] This brought about the birth of Organization for Economic Cooperation and Development (OECD).[176] In 1980, the OECD issued data privacy and protection guidelines called, "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data."[177] The principles that the guidelines set out continue to be relevant today and are seen in data protection laws and regulations today.

OECD member states continued to pass individual privacy laws, some which were conflicting, leading to confusion with regards to compliance.[178] The European Commission (EC) promulgated a new directive, "Data Protection Directive," in 1995, that was binding upon the member states of the EU.[179] Directives were not enforced on all members. They acted as a goal that the EU set for its member states, which they tried to achieve by setting up their laws and regulations that aligned with the directive and were equivalent to one another.[180]

---

[174] Kramer J & Hoar S, "GDPR, part 1: History of European data protection law," Lewis Brisbois Bisgaard & Smith LLP --https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf/-- on 12 March 2025.

[175] Kramer J & Hoar S, "GDPR, part 1: History of European data protection law," Lewis Brisbois Bisgaard & Smith LLP --https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf/-- on 12 March 2025.

[176] Kramer J & Hoar S, "GDPR, part 1: History of European data protection law," Lewis Brisbois Bisgaard & Smith LLP --https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf/-- on 12 March 2025.

[177] Kramer J & Hoar S, "GDPR, part 1: History of European data protection law," Lewis Brisbois Bisgaard & Smith LLP --https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf/-- on 12 March 2025.

[178] Kramer J & Hoar S, "GDPR, part 1: History of European data protection law," Lewis Brisbois Bisgaard & Smith LLP --https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf/-- on 12 March 2025.

[179] Kramer J & Hoar S, "GDPR, part 1: History of European data protection law," Lewis Brisbois Bisgaard & Smith LLP --https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf/-- on 12 March 2025.

[180] --< https://www.ihasco.co.uk/blog/brief-history-of-the-gdpr>--, on 12 March 2025.

Each country setting its own laws and regulations caused problems when it came to sharing data across borders.[181] A gap in law was created as there was no way of guaranteeing the safety of data once it was transferred outside the EU.[182] As a result, the GDPR was born. It aimed at harmonizing the data protection laws that existed in the EU, making sure that the data transferred abroad was safeguarded, and provide data subjects with more control over their personal data.[183]

4.2: Comparison between the provisions of the GDPR and the DPA

4.2.1: Key principles

Core principles in the DPA are found in Section 25 while in the GDPR they are provided for in Article 5. Both the GDPR and DPA provide for lawfulness, fairness, and transparency in the handling of personal data. They both provide that personal data should be collected for a specified purpose and should not be used beyond the necessary purpose that it was collected for.[184] They further provide that only data that is necessary for the purpose of processing should be collected.[185] That collecting excessive and unnecessary data should be avoided.[186] On top of that, they provide that the data that is collected should be accurate.[187] That inaccuracies should be corrected and the data subjects have the right to bring them up and seek their correction.[188] The GDPR further specifies that processing should be in a manner that ensures that personal data is secure which matches with section 25 (1) of the DPA. They both seek that personal data should be protected against unauthorized or unlawful processing and against accidental loss, destruction, or damage.[189]

Nonetheless, there are principles that the GDPR adds. It provides data should only be retained for as long as it is necessary for the specified purpose.[190] It provides that it is important for data controllers and processors to implement retention periods.[191] Exemption to this is where the data is kept for the purpose of public interest, scientific or historical research, or statistical purposes.[192] Lastly, it adds that

[181] --< https://www.ihasco.co.uk/blog/brief-history-of-the-gdpr>--, on 12 March 2025.
[182] --< https://www.ihasco.co.uk/blog/brief-history-of-the-gdpr>--, on 12 March 2025.
[183] --< https://www.ihasco.co.uk/blog/brief-history-of-the-gdpr>--, on 12 March 2025.
[184] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[185] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[186] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[187] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[188] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[189] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[190] Article 5, *General data protection regulations*, 2016, 2016/679.
[191] Article 5, *General data protection regulations*, 2016, 2016/679.
[192] Article 5, *General data protection regulations*, 2016, 2016/679.

the data controllers and processors are held accountable and should be able to demonstrate that they are complying with the GDPR provisions.[193]

The DPA also has extra principles like the data collected should only be used for the purpose it was collected.[194] It should not be processed further for a purpose the data subject did not provide consent for.[195] On top of that, it would be best if personal data were anonymized.[196]

4.2.2: Scope and jurisdiction

The DPA provisions apply to registered data processors and controllers whether they are resident in Kenya or not.[197] The GDPR jurisdictional reach goes beyond the data controllers and processors.[198] It also applies to the entities offering goods or services to European residents or those monitoring the behavior of European residents occurring in Europe.[199] Both the GDPR and the DPA both apply to the processing where personal data is entered into the record through automated or non-automated means.[200] If entered through the latter means, it ought to form part of the filing system or the whole of it.[201]

4.2.3: Legal bases and jurisdiction

The DPA provides for the legal bases in section 30 while in the GDPR they are found in Article 6.

They both provide that data can only be processed where the data subject has provided consent.[202] Data could be processed due to the need to perform a contract that the data subject is a party to.[203] The requests of a data subject provided before entering the contract also necessitate processing.[204] Further, compliance with a legal obligation that controllers are subject to necessitates processing.[205] On top of

[193] Article 5, *General data protection regulations*, 2016, 2016/679.
[194] Section 25 (d), Data Protection Act, 2019.
[195] Section 25 (d), Data Protection Act, 2019.
[196] Section 25 (g), Data Protection Act, 2019.
[197] Section 4 (b), Data Protection Act, 2019.
[198] Kramer J & Hoar S, "GDPR, part 1: History of European data protection law," Lewis Brisbois Bisgaard & Smith LLP --https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf/-- on 12 March 2025.
[199] Article 3, *General data protection regulations*, 2016, 2016/679.
[200] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[201] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[202] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[203] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[204] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[205] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.

that, processing is necessary to protect the vital interests of a data subject or another natural person.[206] Processing is also necessitated by the need to perform a controller's task that is required for public interest or in the exercise of the official authority.[207] In addition to these, a controller's or third party's legitimate interests provide a legal basis for processing.[208] This however does not override the rights and freedoms of data subjects.

On top of these, the DPA provides that historical, statistical, journalistic, literature and art, or scientific research would amount to a legal basis for processing personal data.[209] It also adds that the performance of a task carried out by a public authority necessitates processing.[210]

4.2.4: Enforcement mechanisms and sanctions

The DPA provides for the Office of the Data Protection Commissioner as the regulatory body.[211] As for the GDPR, each state has one or more supervisory authorities.[212] Each authority then gets to have a seat on the European Data Protection Board.[213] The authorities in both the GDPR and DPA monitor the application of their provisions and act independently in the performance and exercise their functions and powers.[214]

The GDPR provides for a fine of 10 million euros or 2% of their total worldwide annual turnover of the preceding financial year for infringements pertaining to children's data and special categories of data.[215] The fine is 20 million euros or 4% of their total worldwide annual turnover of the preceding financial year, where the infringement pertains to basic processing principles, rights of data subjects, failure to comply with an order limiting processing or suspension of data flows, and failure to provide access.[216]

In the DPA, the enforcement provisions are provided for in Part VIII of the act. The ODPC investigates all the complaints and orders necessary for the investigation are made as set out in section 57. Where there is a failure to comply with the DPA, the data commissioner serves the party with an enforcement notice requiring them to take certain steps to comply.[217] Failure to comply with the enforcement notice

[206] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[207] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[208] --https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--, on 20 March 2025.
[209] Section 30, Data Protection Act, 2019.
[210] Section 30, Data Protection Act, 2019.
[211] Section 5, Data Protection Act, 2019.
[212] Article 51, *General data protection regulations*, 2016, 2016/679.
[213] Article 51, *General data protection regulations*, 2016, 2016/679.
[214] Article 51, *General data protection regulations*, 2016, 2016/679.
[215] Article 83, *General data protection regulations*, 2016, 2016/679.
[216] Article 83, *General data protection regulations*, 2016, 2016/679.
[217] Section 58 (1), Data Protection Act, 2019.

leads to the service of a penalty notice. It will require the party to pay a certain amount to the ODPC.[218] The DPA provides for conditions that lead the data commission to serve a penalty notice.[219] The maximum amount that may be imposed should be 5 million Kenyan Shillings or a 1% of an undertaking's annual turnover of the preceding financial year.[220]

Not only are the fines in the GDPR higher, but also, between the fines and the percentage of the annual turnover that is sought, it provides that the one that is higher is what should be enforced on the party. In the DPA, it provides that whichever is lower is what should be enforced on the party.

4.3: Comparison of the provisions on cross border data transfers

4.3.1: GDPR and DPA.

Cross-border transfers can only happen where the GDPR's standards are met. There ought to be an adequate level of protection for the transfers to happen. This could be assessed through adequacy decisions made by the European Commission and appropriate safeguards.

Determination of adequate levels of protection by the commission is based on elements like the rule of law, respect for fundamental human rights and freedoms, and the relevant legislation existing in the third country, territory, sector, or international organizations.[221] On top of that, the existence of supervisory authorities that function effectively is looked at.[222] It also checks the commitments that the third country or international organizations are party to or the obligations that arise for them with regards to legally binding conventions or instruments they are party to.[223]

Even after the decision, periodical reviews should be done on the third countries and organizations that are approved.[224] The commission should also monitor the developments in third countries and international organizations.[225] Based on this, it could repeal, amend, or suspend the decision of adequacy.

Transfers could occur where no adequacy decision is sought. This is only applicable if the controller or processor and the country receiving the data adopt appropriate safeguards that will ensure the safety of transferred personal data.[226] These include binding corporate rules that are used to internally transfer personal data, standard contractual clauses, and certification mechanisms and code of conduct that is

[218] Section 62 (1), Data Protection Act, 2019.
[219] Section 62 (2), Data Protection Act, 2019.
[220] Section 63, Data Protection Act, 2019.
[221] Article 45, *General data protection regulations*, 2016, 2016/679.
[222] Article 45, *General data protection regulations*, 2016, 2016/679.
[223] Article 45, *General data protection regulations*, 2016, 2016/679.
[224] Article 45, *General data protection regulations*, 2016, 2016/679.
[225] Article 45, *General data protection regulations*, 2016, 2016/679.
[226] Article 46, *General data protection regulations*, 2016, 2016/679.

approved. These must be binding to the parties.[227] Binding corporate rules shall be approved if they also expressly confer enforceable rights on data subjects.[228] GDPR also provides for what they should mention.[229]

On top of that, transfers or disclosures based on a third country's court decision will not be recognized or enforced unless it is based on an international agreement between the third country and the Union or a member state, that is in force.[230] Conditions that would allow cross border data transfers in the absence of adequacy decisions and binding corporate rules include a data subject's consent, transfer is necessary for legal claims, or transfer is made from a register that is intended to provide information to the public.[231] Further conditions are those that provide for the legal bases for processing.

It also calls for international cooperation between the Commission, supervisory authorities, and the third countries and international organizations.[232] This could be by developing international cooperation mechanisms, providence of international mutual assistance, engaging in discussions and activities with stakeholders aimed at the same, and promotion of the exchange and documentation of personal data protection legislation and practice.[233]

This study has delved into the provisions on cross-border data transfers in Kenya in Chapter 3. The comparison reveals that DPA's provisions on cross-border data transfers are lacking as they only provide for adequacy decisions, consent of data subjects, transfers out of necessity, and adequate safeguards. Even in the case of safeguards, it does not go into the depth of what such would entail. However, this gap is covered by the Data Protection (General) Regulations which are read together with the DPA.

4.4: Conclusion.

This chapter reveals that there exists a great similarity between the rules in the GDPR and the provisions in the DPA. However, some differences are revealed. Based on the provision of fines due to contraventions, the GDPR is stricter than the DPA. The chapter also reveals that the DPA is not a weak legislation. Its provisions reveal its aim of seeking to regulate the processing of personal data. There are provisions that the DPA could borrow from the GDPR like its extraterritorial reach. This provision shows the stark difference between the DPA and the GDPR.

[227] Article 46, *General data protection regulations*, 2016, 2016/679.
[228] Article 46, *General data protection regulations*, 2016, 2016/679.
[229] Article 46, *General data protection regulations*, 2016, 2016/679.
[230] Article 48, *General data protection regulations*, 2016, 2016/679.
[231] Article 49, *General data protection regulations*, 2016, 2016/679.
[232] Article 50, *General data protection regulations*, 2016, 2016/679.
[233] Article 50, *General data protection regulations*, 2016, 2016/679.

Chapter 5: FINDINGS AND RECOMMENDATIONS

5.1 Introduction

This chapter shall outline the research findings. In response to the outlined research questions and objectives, the chapter presents a systematic approach to the details of the DPA's jurisdictional application, enforcement challenges, and risks when transferring data across borders.

5.2 Findings on Cross-Border Data Transfers

Cross-border data transfer is well regulated through the Kenya Data Protection Act providing a broad legal framework for regulating the global transfer of data. Transfer of data is allowed outside Kenya if the processor or controller provides sufficient data protection safeguards.[234] Nevertheless, evidence suggests that the provisions have not been followed consistently.

In the case of *Federation of Kenya Employers v. Cabinet Secretary, Ministry of Foreign Affairs*, data subjects transferred their data voluntarily to the Scottish court without the approval of the ODPC as required by section 48.[235] Their personal data was required as evidence by the Scottish Courts. This court failed to liaise with the ODPC.[236] This shows a disregard of the Kenyan DPA and ODPC by this court and a disregard of the laws and the regulating body. This causes one to doubt how well it would have protected that data. Though remedial measures are well spelled in the DPA, actionable remedies have no guarantee of being instituted because there was no action from the ODPC.

The Scottish Court also prohibited James Finlay's Kenya from setting up a case in the Kenyan Courts undermining the jurisdiction of the latter courts. This shows that despite the existence of a strong framework that provides for requirements to be met prior to cross-border transfers, parties not regulated by the DPA fail to see the need to comply with these provisions. This incapacitates the DPA in its own mandate to protect personal data and thus harm the data subjects.

---

[234] Masibo, Meshack. "What Does The Data Protection Act Say About Cross Border Data Transfers." KICTANet Think Tank, 2023. https://www.kictanet.or.ke/what-does-the-data-protection-act-say-about-cross-border-data-transfers/.

[235] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] eKLR.

[236] Federation of Kenya Employees v Cabinet secretary, Ministry of foreign affairs and international relations & 4 others; Law Society of Kenya (Interested Party) [2023] eKLR.

Section 25 (h) of the DPA provides the condition of either proving to the ODPC that adequate safeguards exist or obtaining consent from the data subjects to create a legal basis for the transfer of personal data. Looking at the case mentioned above it brings out the confusion that this section brings about. Section 25 (h) and section 48 clash. The Scottish court could have relied on section 25 (h) in their defense, arguing that they followed the provisions of the DPA. This confusion creates room for controllers and processors to carry out processing of personal data that puts data subjects and their data at risk.

5.3 Summary of Findings

This study focuses on the loopholes in enforcing and implementing the DPA concerning transfers across borders. Although it contains clear rules for securing data subjects, in practice, compliance is still questionable, as seen in the case studies presented in chapter 2. The study has shown that the transfers involve great risks. A big percentage of processors and controllers do not apply their policies strictly. This creates room for the lack of proper protection of personal data shared and improper processing of this data. Resource limitations and issues of jurisdiction hamper the performance of the ODPC leading to inadequate regulatory supervision. Besides, the transfer of high-risk data categories encounters more risks due to weak protection measures and low user consciousness. The recommendations shall utilize these findings to address the gaps posted above.

Chapter 4 compares the DPA to the GDPR revealing stark differences between them. Unlike the DPA, the GDPR has extraterritorial jurisdiction which it to protect the EU citizen's right to privacy. It also reveals that periodical reviews are carried out to see how data is being processed in the third countries or international companies and reviewing if the laws of the third countries are still able to protect the privacy of the data subjects' transferred data. On top of that, the GDPR has higher fines compared to the DPA.

5.4 Recommendations for Policy and Legal Reforms

To strengthen the DPA's extraterritorial enforcement mechanisms, the following reforms are proposed:

5.4.1 Amendments to the DPA

There is a need to amend section 4 (b) of the Data Protection Act, for the act's provisions to apply to entities that process the personal data of Kenyan residents, outside the Kenyan jurisdiction. This amendment will allow it to achieve its objective of regulating the processing

of personal data and the protection of the privacy of individuals, stretching its jurisdictional reach extraterritorially. It will act as a basis for the ODPC to play its role of supervising and overseeing the processing of data of individuals in Kenya by foreign organizations. The amendment of section 25 (h) of the DPA is needed. It should provide that both conditions ought to be met for data to be transferred outside Kenya. This removes the confusion that comes from its current clash with section 48 of the DPA.

The study also suggests the adoption of the GDPR rules on the periodical reviews done by the supervisory authorities after cross border data transfers. This adoption would empower the ODPC to enforce the provisions of the DPA on foreign companies that receive the personal data of Kenyan residents. This would also stretch the jurisdictional reach of the DPA.

As proven by chapter 2, cooperations prioritize their businesses and profits over the protection of data subjects' personal data. This poses a great risk to the personal data that they process. There is a need to balance the risk where the cooperations will see that they will have a lot to lose in an instance of a contravention with the provisions of the DPA. This could be done by increasing the fines that would be imposed on them in such an instance. In chapter 4, the study has revealed that in comparison with the GDPR, the DPA has lower fines. The former's fines are either 10 million, 20 million, or 2% or 4% of the cooperation's worldwide annual turnover, depending on the contravention. Section 63 of the DPA provides for 2 million or 1% of their annual turnover, which is significantly lower than the GDPR fines. Increasing the fines allows an increase in stakes and will force cooperations to comply and to strictly apply their data privacy notices.

5.4.2 Improved Resources for the ODPC

The government should increase its budgetary support to the ODPC to strengthen it to effectively conduct monitoring and enforcement activities. These are for instance; resources required for enhancing technological features, manpower development, and educational outreach[237]. Bolstering resource endowment could enhance improved regulatory capacity and co-ordination.

[237] --https://www.kictanet.or.ke/new-report-identifies-achievements-challenges-and-recommendations-to-enhance-data-protection-in-kenya/--, on 20 December 2024.

5.4.3 International Agreements

It is important for Kenya to pursue bilateral and multilateral legal treaties with other countries for the purpose of cooperation and enforcement of data protection laws. These agreements should explicitly address the equivalence in data protection standards between Kenya and its partner countries, ensuring mutual recognition of safeguards and compliance mechanisms. The treaties should include clearly defined procedures for the settlement of disputes arising from cross-border data transfers. There should be a clause in the treaties that mandates the institutions that receive data through cross-border data transfers to submit periodic compliance reports with regards to how the data of Kenya data subjects is processed and is protected. Thus, there is a potential to address some of the issues arising from different regulations through collaboration.

5.5: Conclusion

This dissertation analyses the jurisdictional reach of the DPA and its effectiveness in regulating cross-border data transfers. The research reveals that while the DPA represents significant progress in data protection in Kenya, it faces substantial challenges in achieving its objectives, particularly in the context of extraterritorial enforcement.

The case studies examined reveal data privacy concerns, the gaps in the current framework, and the need for stronger regulatory mechanisms. It underscores that, the lack of clear enforcement provisions and operational capacity weakens the DPA's ability to safeguard Kenyan citizens' data once transferred internationally.

It reveals the need for reforms to enhance the DPA's capacity and effectiveness. The amendments aim to clarify jurisdictional authority and streamline processes for handling cross-border data transfers. Enhanced international collaboration can provide a more robust framework for addressing global data privacy concerns. Furthermore, allocating adequate resources to the ODPC is essential for effective implementation and oversight.

In conclusion, the DPA has laid the groundwork for Kenya to assert its role in data protection within the global digital economy. However, achieving its full potential requires strategic reforms, stronger enforcement mechanisms, and international cooperation. By addressing the identified gaps, Kenya can ensure that its citizens' privacy rights are preserved in an increasingly interconnected world.

BIBLIOGRAPHY

Books.

Stein A, "The unexceptional problem of jurisdiction in cyberspace," 32 (4), International lawyer, 1998.

Menthe D, "Jurisdiction in cyberspace: A theory of international spaces," 4(1), Michigan telecommunications law review, 1998.

JOURNALS

Introna L & Poloudi N, "Privacy in the information age: Stakeholders, interests, and values," Journal of business ethics, 1999, 34, --< https://www.researchgate.net/publication/226528834_Privacy_in_the_Information_Age_Stakeholders_Interests_and_Values?enrichId=rgreq-7b2715d03fa6a2abe40b6c64a6706621-XXX&enrichSource=Y292ZXJQYWdlOzIyNjUyODgzNDtBUzoxNTA3MjgxNDAxMzY0NTFAMTQxMjk0Nzc5NzE2Mg%3D%3D&el=1_x_2&_esc=publicationCoverPdf>-- .

Mulwa M,& Ndeti N, "Integrated marketing communication and technology adoption: A case of Safaricom's M-PESA mobile money transfer services in Kenya." 5 (5), *African Journal of Science, Technology, Innovation and Development*, 2013.

Kuner C, Cate F, et al, "The extraterritoriality of data privacy laws- an explosive issue yet to detonate," 3(3), International Data Privacy Law, 2013.

McKay A, Brand D, et al, "The regulation of health data sharing in Africa: A comparative study," Journal of law and biosciences, 11(1), 2024.

THESES

Spreeuwenberg L, "Justifying a right to privacy," unpublished LLM thesis, Tilburg University, Tilburg, 2016.

Ryngaert C, "The concept of jurisdiction in international law," unpublished, Utrecht University, Utretcht.

Online sources.

--https://www.dlapiperdataprotection.com/index.html?t=law&c=KE%3e

--https://www.informatica.com/services-and-training/glossary-of-terms/data-transfer-definition.html—

--https://www.cyber.gc.ca/en/guidance/data-transfer-upload-protection-itsap40212-

--https://it.cornell.edu/security-and-policy/data-types-high-risk-moderate-risk-low-risk#:~:text=High%2DRisk%20%2D%20Data%20that%20should,Credit%20card%20numbers

--https://www.secoda.co/blog/stakeholder-roles-in-data-governance--,

Masibo M, "What does the data protection act say about cross border data transfers," KICTANet Think Tank, --https://www.kictanet.or.ke/what-does-the-data-protection-act-say-about-cross-border-data-transfers/--

Musau B. "The Kenya data protection act, 2019," 2019, --https://www.bmmusau.com/the-kenya-data-protection-act-2019/--

The National Council for Law Reporting. "Petition E085 of 2023." Kenya Law, 2023. --http://kenyalaw.org/caselaw/cases/view/274776/--

CMS. "Transfer Of Personal Data Outside Kenya." CMS Law.Tax, 2024. --https://cms.law/en/ken/news-information/transfer-of-personal-data-outside-kenya—

Kenya Human Rights Commission. "Judgement on NIIMS (Huduma Namba)," February 6 2020, --https://khrc.or.ke/publication/judgement-on-niims-huduma-namba/--

Business Daily. "Privacy, Data Safety Fears over Huduma Namba," April 7 2019, --https://www.businessdailyafrica.com/bd/opinion-analysis/letters/privacy-data-safety-fears-over-huduma-namba-2245390—

Bowmans. "Application of the Data Protection Act in Kenya: The 'Huduma Namba Decision,'" October 19, 2021, --https://bowmanslaw.com/insights/application-of-the-data-protection-act-in-kenya-the-huduma-namba-decision/--

Kramer J & Hoar S, "GDPR, part 1: History of European data protection law," Lewis Brisbois Bisgaard & Smith LLP --https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf/--

McCallum S "Meta settles Cambridge Analytica scandal case for $725m." BBC News, December 23, 2022, --https://www.bbc.com/news/technology-64075067—

Bareebe R, “The Cambridge Analytica scandal and its impact on Meta.” unknown, May 3, 2022, -http://dx.doi.org/10.13140/RG.2.2.19583.69285-

--< https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/TMT/technology-media-telecommunications-alert-6-september-The-foreign-applicability-of-the-Kenyan-Data-Protection-Act-.html#:~:text=The%20DPA%20has%20extraterritorial%20applicability,of%20individuals%20located%20in%20Kenya>--

--https://www.kictanet.or.ke/new-report-identifies-achievements-challenges-and-recommendations-to-enhance-data-protection-in-kenya/--

--https://www.datahubconsulting.co.uk/articles/kenya-data-protection-act-2019-compared-to-eu-gdpr/#--

--< https://www.ihasco.co.uk/blog/brief-history-of-the-gdpr>--

WORKING PAPERS

Ryngaert C. and Mistale T, “The GDPR as global data protection regulation?” Symposium on the GDPR and international law by the Cambridge University Press, 2019, 5.

INTERNATIONAL SOURCES

SELF PUBLISHED ARTICLES.

Czerniawski M and Svantesson D, “Challenges to the extraterritorial enforcement of data privacy law – EU case ResearchGate, 2023.

REPORTS.

Adapt, “Understanding the challenges data protection regulators face: A global struggle towards implementation, independence, & enforcement.”