Protection of Data Sovereignty and Cybersecurity: A Study of Cross-Border Data Transfer Regulations in Kenya

Submitted in partial fulfilment of the requirements of the Bachelor of Laws Degree, Strathmore University Law School

By

Mathenge Tess Wanjiku

134382

Prepared under the supervision of

Dr. Josephat Kilonzo

February 2025

Word count (10165)

Table of Contents

ACKNOWLEDGEMENT ..... **iv**

DECLARATION ..... **v**

LIST OF LEGAL INSTRUMENTS ..... **vi**

LIST OF ABBREVIATIONS ..... **vi**

LIST OF CASES ..... **vii**

ABSTRACT ..... **viii**

CHAPTER ONE: INTRODUCTION **1**

1.1. Background 1
1.2. Statement of Problem 3
1.3. Research Objectives 3
1.4. Research Questions 3
1.5. Hypothesis 4
1.6. Justification of the Study 4
1.7. Theoretical Framework 4
1.8. Literature Review 7
1.9. Research design and Methodology 9
1.10. Limitations 9
1.11. Chapter Breakdown 9

CHAPTER TWO: CURRENT LEGAL FRAMEWORK GOVERNING CROSS-BORDER DATA TRANSFERS IN KENYA **11**

2.1. Introduction 11
2.2. Constitutional Framework 11
2.3. Legislative Framework 12
2.4. Complementary Legislative Frameworks, Regulations and Guidelines 14
2.5. Conclusion 16

CHAPTER THREE: KEY CHALLENGES AND GAPS IN KENYA'S LEGAL FRAMEWORK ON CROSS-BORDER DATA TRANSFERS **18**

3.1. Introduction 18
3.2. Challenges in Kenya's Legal Framework on Cross-Border Data Transfers 18
3.3. Gaps in Kenya's Legal Framework on Cross-Border Data Transfers 20
3.4. Impact of Gaps and Challenges 21
3.5. Conclusion 22

CHAPTER FOUR: CROSS-BORDER DATA TRANSFERS IN THE NETHERLANDS: LESSONS FOR KENYA **23**

4.1. Introduction 23
4.2. The Netherlands' Legal Framework for Cross-Border Data Transfers 23
4.3. The Netherlands' Practical Approaches and Enforcement Mechanisms 24
4.4. Comparative Analysis: Netherlands vs. Kenya 26
4.5. Lessons and Best Practices for Kenya 28
4.6. Conclusion 29

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS **30**

5.1. Introduction 30
5.2. Conclusion 30
5.3. Recommendations 31

BIBLIOGRAPHY 34
Books 34
Journals 34
Reports 34
Online sources 34

ACKNOWLEDGEMENT

First and foremost, I extend my deepest gratitude to God for granting me the strength, wisdom, and perseverance to complete this dissertation. His guidance has been my source of motivation throughout this academic journey. I am profoundly grateful to my supervisor, Dr. Josephat Kilonzo, for his invaluable support, insightful feedback, and continuous encouragement. His guidance has played a crucial role in shaping my research and ensuring its academic rigor.

To my family, your unwavering support, patience, and belief in me have been my greatest source of strength. Your encouragement during the most challenging moments of this journey has meant the world to me. I also extend my appreciation to my friends, who have stood by me throughout this process. Your encouragement and moral support have been invaluable.

To everyone who contributed in one way or another to this research, whether through guidance, inspiration, or simply being a pillar of support, I sincerely thank you.

DECLARATION

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

Signed: 

Date: 26th February 2025.

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

Signed:  .....

DR. JOSEPHAT KILONZO.

Date: 26th February 2025.

LIST OF LEGAL INSTRUMENTS

The Constitution of Kenya (2010).
Data Protection Act (Act No 24 of 2019).
The Data Protection (General) Regulations (Kenya Subsidiary Legislation) 2021.
Computer Misuse and Cybercrimes Act (Act No 5 of 2018).
General Data Protection Regulation (GDPR) (EU) 2016/679.
African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014.

LIST OF ABBREVIATIONS

DPIAs	Data Protection Impact Assessments
GDPR	General Data Protection Regulation
EU	European Union
SCCs	Standard Contractual Clauses
CIGI	Centre for International Governance Innovation
DPA	Data Protection Act 2019 and accompanying Kenya Subsidiary Legislation 2021
ODPC	Office of the Data Protection Commissioner
SMEs	Small and Medium Enterprise
AP	Dutch Data Protection Authority
TIAs	Transfer Impact Assessments

LIST OF CASES

Okiya Omtatah Okoiti v. Communication Authority of Kenya & 8 Others (2018) eKLR.

Kenya Human Rights Commission v. Communications Authority of Kenya & 2 Others (2017) eKLR.

R v Joe Mucheru (2021) eKLR.

Nubian Rights Forum & Others vs. Attorney General (2020) eKLR.

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (2020), Court of Justice of the European Union.

ABSTRACT

As the global economy digitizes, data flow across borders becomes vital for trade, communication, and innovation. However, this brings challenges in privacy, cybersecurity, and regulation. In Kenya, cross-border data transfer regulations like the Data Protection Act, its accompanying Kenya Subsidiary Legislation, 2021 and the Computer Misuse and Cybercrimes Act aim to address these issues and protect privacy rights. Yet, their effectiveness remains uncertain, amid concerns about data sovereignty, jurisdictional conflicts, and rapid technological change. This study examines the adequacy of these regulations, using a doctrinal research approach. Through legal analysis and policy evaluation, it explores the regulatory landscape, identifies challenges, and assesses implications for businesses, government, and individuals. The study aims to highlight strengths and weaknesses, inform policy reforms, and contribute to the discourse on data governance and digital rights in Kenya and globally. By shedding light on cross-border data transfer regulations in Kenya, this research advances understanding of data governance dynamics in the digital age. It emphasizes the need to balance privacy protection, cybersecurity, and regulatory flexibility to foster innovation, economic growth, and social progress in Kenya and beyond.

CHAPTER ONE: INTRODUCTION

1.1. Background

In today's digital economy, the flow of data across borders is a fundamental aspect of international business, technological innovation, and economic growth. Countries like Kenya are recognizing the importance of regulating cross-border data transfers to ensure that personal data is protected, no matter where it travels. Kenya's Data Protection Act 2019 and its accompanying Kenya Subsidiary Legislation 2021 are a significant legislative step towards safeguarding personal data, yet a notable gap exists in the regulation of cross-border data transfers. The Data Protection Commissioner, who assumed office after the Act was passed, has published a variety of guidelines for different sectors and activities on the regulator's website. However, there are no specific guidelines addressing cross-border data transfers, leaving a regulatory void in this critical area.[1]

Kenya's Constitution, under Article 31, guarantees the right to privacy, which includes protecting individuals from the unnecessary disclosure of their private information.[2] This provision forms the constitutional foundation for Kenya's data protection regime, establishing that any legislation governing personal data must hold this fundamental right. The Data Protection Act 2019 builds on this constitutional dictate by setting out clear principles for the processing of personal data. These principles include provisions for transparency, data minimization, and accountability, among others.[3] The Act also lays out obligations for data controllers and processors, ensuring that they take responsibility for safeguarding personal information throughout its lifecycle.[4]

The Data Protection Act requires organizations to undertake Data Protection Impact Assessments (DPIAs) under Article 31 of the Act when processing operations are likely to result in a high risk to data subjects' rights and freedoms.[5] It also introduces mandatory data breach notifications, enabling individuals and regulators to respond quickly to potential breaches.[6] While the Act provides robust protections for personal data processed within Kenya, it lacks clarity and depth regarding cross-border data transfers.[7] This creates a critical gap, as the transfer of personal data across borders is a common practice in today's digital economy. The absence of clear regulations or guidelines on managing these transfers leaves the privacy of Kenyan citizens vulnerable, especially when their data leaves the country's jurisdiction.

---

[1] Office of the data protection commissioner, 'Guidelines' Kenya data protection regulator's website, https://www.odpc.go.ke/guidelines-2/ on 12 September 2024.
[2] Article 31, *Constitution of Kenya* (2010).
[3] Article 25, *Data Protection Act* (Act No. 24 of 2019).
[4] Part IV, *Data Protection Act* (Act No. 24 of 2019).
[5] Article 31, *Data Protection Act* (Act No. 24 of 2019).
[6] Article 43, *Data Protection Act* (Act No. 24 of 2019).
[7] Part VI, *Data Protection Act* (Act No. 24 of 2019).

In contrast, the General Data Protection Regulation (GDPR) of the European Union (EU) is widely regarded as the most comprehensive data protection law globally. It establishes stringent rules for the processing of personal data, including provisions that regulate data transfers to non-EU countries.[8] The GDPR ensures that personal data leaving the EU remains protected, regardless of the destination. One of the key mechanisms for achieving this is through the use of Standard Contractual Clauses (SCCs), which are legal agreements designed to ensure that data transferred to third countries meets the high standards set by the GDPR.[9] SCCs are particularly important for businesses that operate across borders, as they provide a structured, compliant framework for managing international data transfers.

Since the SCCs were modernized in 2021, they have become more flexible and better suited to today's data transfer realities. These updated clauses offer a comprehensive approach, ensuring that personal data remains protected in jurisdictions outside the EU, even if those jurisdictions do not have laws equivalent to the GDPR.[10] Kenya, which seeks to become a regional hub for digital innovation, could benefit greatly from adopting a similar framework. Without specific regulations for cross-border data transfers, businesses and individuals in Kenya face uncertainty, particularly when interacting with international entities.

On the African continent, the African Union's Malabo Convention—formally known as the African Union Convention on Cyber Security and Personal Data Protection—serves as a crucial international framework. The Malabo Convention was adopted in 2014 to harmonize data protection laws across Africa. Several African nations, including Senegal, Mauritius, and Ghana, have signed and ratified the convention, demonstrating their commitment to aligning with global data protection standards.[11] However, Kenya has yet to ratify this convention, further emphasizing the gap in its legal framework for handling international data transfers.[12]

Alongside international frameworks like the GDPR and the Malabo Convention, Kenya's Computer Misuse and Cybercrimes Act 2018 complements the Data Protection Act by criminalizing various cyber offenses, including unauthorized access to computer systems, identity theft, and cyber espionage.[13] This Act plays a vital role in protecting Kenyan citizens

[8] Chapter V, *General Data Protection Regulation (GDPR) ((EU) 2016/679).*
[9] European Commission, 'Standard Contractual Clauses' Official website of the European union, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en on 12 September 2024.
[10] European Commission, 'Standard Contractual Clauses' Official website of the European union, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en on 12 September 2024.

[11] Kaaniru J, 'The African union convention on cyber security and personal data protection: key insights' Strathmore university, 24 July 2023 https://cipit.org/the-african-union-convention-on-cyber-security-and-personal-data-protection-key-insights/ on 12 September 2024.

[12] 'List of countries which have signed, ratified/acceded to the African union convention on cyber security and personal data protection' African union, https://dataprotection.africa/wp-content/uploads/2305121.pdf on 12 September 2024.
[13] Part III, *Computer Misuse and Cybercrimes Act*, (Act No. 5 of 2018).

from cyber threats, but it does not address the specific regulatory needs of cross-border data transfers, which remain a significant blind spot in Kenya's legal framework.

For Kenya to position itself as a competitive player in the global digital economy, its Data Protection Act must evolve to include structured regulations for cross-border data flows, mirroring best practices set by the GDPR. By introducing specific guidelines on cross-border data transfers, Kenya can ensure that personal data remains secure even when it moves beyond national borders. Moreover, ratifying international instruments like the Malabo Convention would demonstrate Kenya's commitment to harmonizing its laws with global data protection standards, thereby fostering trust with international partners. The absence of clear cross-border data transfer rules presents a significant challenge to the country's growing digital economy, and closing this gap is critical for promoting responsible data sharing and privacy protections for Kenyan citizens.

1.2. Statement of Problem

Kenya's Data Protection Act 2019, while advancing the protection of personal data, fails to provide clear and in-depth guidelines for cross-border data transfers, leaving a critical gap in the legal framework. This omission creates uncertainty for businesses and exposes individuals' personal information to potential privacy risks when data is transferred internationally. In contrast, frameworks like the GDPR offer robust mechanisms to regulate such transfers, ensuring data protection across borders. Without similar provisions, Kenya's growing digital economy and its citizens' privacy rights are at risk. This research investigates the adequacy of Kenya's data protection laws regarding cross-border data transfers.

1.3. Research Objectives

1. Examine the current legal framework governing cross-border data transfers in Kenya.
2. Examine the key challenges and gaps in Kenya's legal framework on cross-border data transfers.
3. Analyse the lessons Kenya can learn from The Netherlands' regulation of cross-border data transfers.

1.4. Research Questions

1. To what extent does the current legal framework in Kenya regulate cross-border data transfers?
2. What are the key challenges and gaps in Kenya's legal framework on cross-border data transfers?
3. What lessons can Kenya learn from The Netherlands on regulating cross-border data transfers?

1.5. Hypothesis

Kenya's current legal framework on data protection may not be sufficient to provide the safeguards for proper regulation of cross-border data transfers. This may have an implication on individuals' rights including the right to privacy.

1.6. Justification of the Study

In today's digital age, regulating cross-border data transfers is crucial for governments, businesses, and individuals. This study on Kenya's data transfer regulations is vital in addressing key concerns, particularly the protection of privacy rights in the digital era. As people increasingly rely on online services, ensuring the privacy and security of personal data is paramount. Additionally, the study assesses cybersecurity implications, identifying regulatory gaps that could expose Kenya to cyber threats and data breaches. By evaluating existing frameworks, it contributes to enhancing both privacy protections and cybersecurity measures.

The study also holds significant implications for businesses, the economy, and legal frameworks.[14] As cross-border data flows drive global trade and innovation, understanding Kenya's regulatory landscape is crucial for local and international businesses. By examining Kenya's legal framework, this study adds value to ongoing legal scholarship, highlighting the need for legislative reforms. Furthermore, it emphasizes the importance of aligning Kenya's regulations with international data protection standards, promoting international cooperation and ensuring seamless data flows across jurisdictions.

1.7. Theoretical Framework

1.7.1. Regulatory Compliance Theory

The theory of regulatory compliance comes from studies in legal and organizational frameworks. Michael Lipsky (Street-level bureaucracy) and John Braithwaite (Responsive regulation) are scholars who are major contributors to regulatory compliance theory. Lipsky introduced the idea of "street-level bureaucrats" for example police officers and inspectors who directly implement and enforce laws.[15] Braithewaite explored the concept of "responsive regulation," which balances regulation enforcement with flexibility, giving room for more cooperative compliance mechanisms.[16]

Regulatory compliance focuses on how legal rules and regulations are followed. It explores the mechanisms, incentives, and retributions that ensure compliance with laws, as well as the

[14] *The African continental free trade area (AfCFTA) agreement,* 21 March 2018, 36437 AfCFTA.
[15] Lipsky M, *Street-level bureaucracy,* 30th ed, 2020, 169.
[16] Braithewaite J, *Responsive regulation, original ed, 1992, 4.*

interpretation of these laws by various stakeholders.[17] In the context of cross-border data transfers, this means studying how businesses, governments, and organizations adhere to data protection laws such as Kenya's Data Protection Act. However, while compliance theory addresses the enforcement of regulations, it can miss the broader cultural or technological factors that influence how laws are applied.[18] For instance, in Kenya, technological literacy and institutional capacity can impact how well data protection regulations are enforced. Additionally, regulatory compliance heavily depends on the availability of resources for enforcement, such as trained personnel and technological infrastructure,[19] which might be limited in developing countries like Kenya.

In conclusion, regulatory compliance theory allows me to explore how Kenya's Data Protection Act, the Computer Misuse and Cybercrimes Act, and other relevant regulations are implemented in practice and the challenges that arise in enforcing them. For example, I can examine the capacity of the Office of the Data Protection Commissioner to enforce data protection standards and analyse how Kenyan businesses comply with these regulations when managing international data transfers.

1.7.2. Technology and Innovation Theory

Thorstein Veblen, one of the earliest proponents of the theory technological determinism, argued that technology drives societal changes and influences how economic and social institutions function. His work paved the way for our current understanding of how technology affects social structures and human behaviour. Karl Marx also embraced a version of technological determinism, suggesting that the means of production (technology) shapes societal relations and governance structures. His focus on how technology influences economic systems and social power dynamics is relevant in understanding how data technologies affect governance.[20]

---

[17] 'What is regulatory compliance?' metricstream, https://www.metricstream.com/learn/comprehensive-guide-to-regulatory-compliance.htm#:~:text=Regulatory%20compliance%20focuses%20on%20aligning,at%20streamlining%20internal%20business%20requirements. on 13 September 2024.

[18] What is regulatory compliance?' metricstream, https://www.metricstream.com/learn/comprehensive-guide-to-regulatory-compliance.htm#:~:text=Regulatory%20compliance%20focuses%20on%20aligning,at%20streamlining%20internal%20business%20requirements. on 13 September 2024.

[19] What is regulatory compliance?' metricstream, https://www.metricstream.com/learn/comprehensive-guide-to-regulatory-compliance.htm#:~:text=Regulatory%20compliance%20focuses%20on%20aligning,at%20streamlining%20internal%20business%20requirements. on 13 September 2024.

[20] Finley T, 'A look through technological determinism, social constructivism, modernity and social media.' 2021, https://scholarworks.arcadia.edu/cgi/viewcontent.cgi?article=1552&context=showcase on 13 September 2024.

Technological determinism asserts that the main force behind societal change is technological innovation. According to this theory, institutions, laws, and regulations change as technology advances.[21] For example, global data governance systems have changed as a result of cloud computing and mobile technologies. Technological determinism in Kenya would contend that the country's cross-border data transfer regulations need to change to keep up with technology advancements or risk becoming antiquated and ineffectual.

Critics of this theory however argue that technological determinism overemphasizes the role of technology and overlooks human agency, social norms, and political factors. Technology alone does not drive legal changes; rather, it works in tandem with societal, cultural, and economic forces.[22] It also neglects social responsibility in the sense that focusing too much on technology can obscure important ethical and social responsibilities.[23] For example, in cross border data transfers, issues of privacy rights and personal autonomy are often moral and ethical considerations, not just technological challenges.

Eric Trist and Fred Emery are pioneer scholars of sociotechnical systems theory which emerged from the Tavistock Institute of Human Relations in the 1950s. They argued that technology and social systems interact in complex ways, and technological advancements can only be understood in the context of social, political, and organizational dynamics.[24] This theory emphasizes that technology and society co-evolve. It implies that understanding how data protection laws interact with organizational structures, political systems, and societal needs is just as important to their efficacy as keeping up with technological advancements.[25] Data protection laws in Kenya need to take into account the local environment, which includes economic realities, governmental structures, and technological literacy.

While more holistic than technological determinism, sociotechnical systems theory can be difficult to apply because it involves many interacting factors. In data governance, trying to account for every societal, political, and technological variable might make the analysis too broad or scattered.[26] Moreover, The theory is more difficult to implement in policy-making because it does not offer straightforward solutions. It emphasizes understanding the interplay

[21] Adler P, 'Technological determinism' International encyclopaedia of organization studies, 7 July 2006 https://faculty.marshall.usc.edu/Paul-Adler/research/revisingTechnological%20Determinism.pdf on 13 September 2024.
[22] https://sites.psu.edu/natalieharp/writings/technological-determinism-a-critique-based-on-several-readings-in-adult-education/ on 13 September 2024.
[23] Tessema D, 'Technological determinism versus social determinism, a critical discussion' SCISPACE, 2021 https://typeset.io/papers/technological-determinism-versus-social-determinism-a-3jwstdltqs on 13 September 2024.
[24] Kaminski J, 'Theory applied to informatics: Socio-technical theory' 17 Canadian journal of nursing informatics 3-4, 2022, 1-4.
[25] https://business.leeds.ac.uk/research-stc/doc/socio-technical-systems-theory#:~:text=Socio%2Dtechnical%20theory%20has%20at,parts%20of%20a%20complex%20system. On 13 September 2024.
[26] Gorejena K, 'A critique and potency of socio-technical systems theory: a quest for broadband growth and penetration' 5 Public and municipal finance 2, 2016, 12.

between technology and society, which can be challenging when trying to create clear and enforceable regulations.[27]

Technological determinism helps in understanding how the proliferation of technologies like cloud computing, mobile data platforms, and internet-connected devices are reshaping Kenya's regulatory landscape. This theory provides a framework for discussing why Kenya needs to adapt its data protection laws to keep pace with technological innovations. For example, as cloud computing technologies grow, data localization requirements may become increasingly important.

On the other hand, sociotechnical systems theory adds depth by highlighting the interaction between technology, society, and law. In Kenya, data protection regulations cannot simply respond to technological advancements—they must also consider local societal dynamics. For instance, the enforcement of these laws might depend on factors like public awareness of privacy rights and the institutional capacity to implement regulations. By using sociotechnical systems theory, I can take a more nuanced approach to understanding how Kenya can craft effective, context-sensitive regulations for cross-border data transfers.

1.8. Literature Review

The increasing prevalence of cross-border data transfers and the movement of personal data across national borders raises crucial questions about privacy protection, cybersecurity, and the effectiveness of regulatory frameworks. This literature review explores the existing scholarship on cross-border data transfer regulations and their implications for the Kenyan digital environment. It examines key research findings, identifies relevant theoretical frameworks, and highlights a crucial research gap within the Kenyan context. The intricate relationship between data transfer regulations, privacy protections, and cybersecurity has become a pressing issue for researchers. Here, I will explore key findings from diverse academic perspectives, showcasing how they shed light on these complex issues within the unique context of Kenya's digital landscape.

Samuel Abu, in his work on cross-border data transfer, emphasizes the need for clear, consistent, and enforceable legal frameworks to navigate the complexities of data flows. He argues for harmonization across jurisdictions to address conflicts and ensure consistent applications of regulations.[28] This resonates with concerns raised by Kijirah and Thuo, who highlight potential challenges posed by data sovereignty regulations in Kenya, where requiring data storage within national borders may create trade barriers and hinder economic growth.[29]

---

[27] Gorejena K, 'A critique and potency of socio-technical systems theory: a quest for broadband growth and penetration' 5 Public and municipal finance 2, 2016, 13.

[28] Abu S, 'Right to privacy, data protection and IOTS: An appraisal of legal issues covering cross border data transfer' Published LLB Thesis, University of Lagos, Lagos, 2019, 33-39.

[29] Kijirah M, *Data protection and data localisation in Kenya: Potential economic impact and effect on Kenya's commitments in various regional treaty frameworks*, Mandela Institute, School of Law, Johannesburg, 2021.

Striking a balance between data security and economic benefits remains a complex issue for policymakers, requiring careful consideration within the Kenyan context.

Enforcement of these regulations presents further challenges. Mwangi S.N. examines the difficulties of enforcing data protection regulations in developing countries, focusing on Kenya. He identifies limitations in institutional capacity, resource constraints, and public awareness as key hurdles that weaken enforcement efforts.[30] As Kenya navigates these challenges, it faces the additional pressure of adapting to rapid technological advancements. The Centre for International Governance Innovation (CIGI) explores the impact of technologies such as cloud computing and mobile technologies on data governance practices. The need for regulatory frameworks to evolve in tandem with these technological developments is critical for ensuring robust privacy and cybersecurity protections. Jerameel Owuor and Kibet Brian similarly note the ongoing efforts in Kenya to strengthen its legal framework in alignment with international best practices, such as the European Union's GDPR.[31]

Governance mechanisms and compliance also play a pivotal role in the effectiveness of data protection regulations. Green emphasizes the importance of governance structures that promote transparency, accountability, and stakeholder engagement in shaping a data governance ecosystem that respects individual privacy rights.[32] This perspective aligns with Taylor M., who argues that the effectiveness of data protection regulations relies heavily on institutional capacity, political will, and the cooperation of various stakeholders, including government agencies, businesses, and civil society organizations.[33]

In conclusion, while existing literature provides significant theoretical insights into cross-border data transfer regulations, there is a gap in addressing how these regulations specifically apply to the Kenyan context. Most studies have focused on global or regional perspectives, but there is limited scholarly work exploring the practical challenges and opportunities these regulations present for Kenyan businesses, government agencies, and individuals. This study aims to contribute to the literature by critically analysing the Kenyan regulatory framework, highlighting areas of improvement, and offering insights based on theoretical and comparative analysis. Rather than conducting empirical research, this study focuses on addressing the conceptual and policy-related gaps, thereby advancing the discourse on data governance and digital rights in Kenya.

---

[30] Mwangi S.N, 'The Challenges of Enforcing Data Protection Legislation in Developing Countries: A Case Study of Kenya' International Journal of Law and Information Technology, 2018— https://academic.oup.com/ijlit/search-results?page=1&q=The%20Challenges%20of%20Enforcing%20Data%20Protection%20Legislation%20in%20Developing%20Countries%3A%20A%20Case%20Study%20of%20Kenya&fl_SiteID=5171&SearchSourceType=1&allJournals=1 on 14 September 2024.

[31] Owuor J, 'Defining Data Protection in Kenya: Challenges, Perspectives and Opportunities' SSRN, 7 November 2022— https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4270712 on 14 September 2024.

[32] Green T, *The Role of governance mechanisms in effective data protection*, Oxford university press, 2017.

[33] Taylor M, *Institutional dynamics and compliance with data protection standards,* International review of law, computers & technology, 2020, 269-288.

1.9. Research design and Methodology

This research is doctrinal in nature and mainly adopts a desktop research. The research relies on primary and secondary sources. The primary sources include the Constitution, legislation, treaties, and regulations. The secondary sources include books, book chapters, journal articles, and reports. The research also conducts a comparative study on The Netherlands to draw lessons for Kenya on regulation of cross-border data transfer.

1.10. Limitations

Legal analysis may be limited by the interpretation and ambiguity inherent in legal texts, potentially overlooking informal practices or regulatory gaps. This can be mitigated by supplementing legal analysis with expert consultations, comparative assessments or empirical data. Engaging diverse perspectives and critically analysing legal frameworks can enhance the strength of findings.

1.11. Chapter Breakdown

Chapter One: This chapter will provide essential details such as the background of the study, statement of problem, research objectives and questions, hypothesis, justification of the study, theoretical framework and the literature review. This chapter serves as the basis for the following chapters.

Chapter Two: This chapter addresses the first research question by providing a detailed analysis of the current legal framework governing cross-border data transfers in Kenya. It examines the Data Protection Act 2019 in depth, alongside complementary regulations that establish the guidelines, obligations, and protections relevant to data transfers.

Chapter Three: This chapter answers the second research question by identifying the key challenges and gaps in Kenya's legal framework concerning cross-border data transfers. It addresses specific areas where the regulatory framework falls short, as well as potential vulnerabilities related to privacy and cybersecurity.

Chapter Four: This chapter addresses the third research question by analysing the Netherlands' approach to regulating cross-border data transfers, particularly under the GDPR. It explores how the Netherlands' legal and regulatory framework ensures data protection across borders. Furthermore, the chapter compares the Dutch regulatory approach with Kenya's legal framework, identifying valuable lessons and best practices that Kenya can adopt to strengthen its own regulations governing cross-border data transfers.

Chapter Five: The final chapter summarizes the key findings of the research and provides recommendations for improving Kenya's cross-border data transfer regulations. It highlights areas where Kenya's legal framework can be strengthened and offers practical solutions for

addressing identified gaps, such as adopting international best practices and harmonizing with global data protection standards. This chapter concludes the study and outlines potential areas for future research.

CHAPTER TWO: CURRENT LEGAL FRAMEWORK GOVERNING CROSS-BORDER DATA TRANSFERS IN KENYA

2.1. Introduction

Cross-border data transfers have become integral to modern digital interactions, yet they pose significant legal and ethical challenges. Chapter two explores the legal framework governing these transfers within Kenya, answering the first research question by critically examining constitutional provisions, legislation, regulations, and case law. This chapter highlights how Kenya's regulatory approach seeks to protect individuals' right to privacy as guaranteed in the Constitution while enabling data-driven innovation in an interconnected world. The analysis underscores the interplay between constitutional principles and legislative efforts in establishing safeguards for data transfers, ensuring that privacy rights are upheld even when personal data crosses national borders.

Central to this discussion is the Data Protection Act 2019, which sets the legislative foundation for regulating data processing and transfers in Kenya. Complementary statutes such as the Data Protection (General) Regulations 2021 and the Computer Misuse and Cybercrimes Act 2018 further strengthen this framework by addressing specific aspects of cross-border data governance. In addition, guidance issued by the Office of the Data Protection Commissioner (ODPC) provides clarity on compliance obligations, such as securing data subject consent and conducting Data protection impact assessments. By integrating case law and regulatory measures, this chapter evaluates the extent to which Kenya's legal framework addresses the unique challenges posed by cross-border data flows.

2.2. Constitutional Framework

The Constitution of Kenya, 2010, is the foundational basis for its legal framework and explicitly guarantees the right to privacy under Article 31. This provision recognizes every individual's right not to have their personal, family, or private affairs unnecessarily intruded upon or their private communications infringed.[34] This constitutional guarantee forms the foundation for all data protection laws in Kenya, including the regulation of cross-border data transfers. It has thus recognized privacy as an inviolable human right, whose protection requires proactive legislation in the face of evolving technological and global challenges.

Article 31(c) and (d) directly address data protection by prohibiting the unwarranted disclosure or infringement of personal information. These clauses have been interpreted as imposing a duty on the state and private entities to implement mechanisms that protect individuals' data

[34] Article 31, *Constitution of Kenya* (2010).

from misuse, particularly in contexts involving transnational data flows.[35] This constitutional right supports the Data Protection Act 2019, which was enacted to actualize these protections in a legislative framework, detailing obligations for data controllers and processors involved in handling personal data.

Kenyan courts have also significantly shaped the interpretation and application of privacy rights in the context of data protection. For instance, in the landmark case of *Okiya Omtatah Okoiti v. Communication Authority of Kenya & 8 Others,* the court emphasized that privacy rights under Article 31 extend to the protection of personal data and communications. This case involved the Communications Authority's directive requiring telecommunications service providers to install a device management system capable of accessing subscribers' private data. The High Court found the directive unconstitutional, emphasizing the need for any action affecting personal data to comply with constitutional safeguards.[36]

Similarly, in *Kenya Human Rights Commission v. Communications Authority of Kenya & 2 Others,* the High Court addressed the constitutionality of surveillance measures. The Court reiterated that the right to privacy includes the right to control one's personal data and communications. It ruled against surveillance mechanisms that lacked adequate safeguards for protecting personal data, reinforcing the constitutional limits on data processing and surveillance in both domestic and international contexts.[37]

These cases illustrate the Judiciary's role in interpreting the Constitution to safeguard privacy rights. They also highlight the necessity for legal and procedural safeguards when handling cross-border data transfers to ensure compliance with constitutional mandates. Through these interpretations, the Kenyan legal framework has evolved to recognize privacy as central to individual autonomy and democratic governance. The integration of constitutional principles into legislative and judicial frameworks highlights the interplay between privacy rights and the need for a secure, regulated approach to cross-border data handling.

2.3. Legislative Framework

The Data Protection Act 2019 and accompanying Kenya Subsidiary Legislation (DPA) present a general regulatory framework that assists in ensuring transfers of personal data beyond Kenya's borders, observe strict standards concerning privacy and security. One of the most important provisions applicable in the context of cross-border transfers is the principle of explicit consent, under which the data controller is under obligation to obtain clear and informed consent from data subjects before their personal data can be moved out of Kenya.[38] It has to be voluntary and specific to enable the subjects to understand what happens to their

[35] Article 31, *Constitution of Kenya* (2010).
[36] *Okiya Omtatah Okoiti v. Communication Authority of Kenya & 8 Others (2018) eKLR.*
[37] *Kenya Human Rights Commission v. Communications Authority of Kenya & 2 Others (2017) eKLR.*
[38] Section 49, *Data Protection Act* (Act No. 24 of 2019).

information.[39] Data controllers are thus required to communicate the purpose and potential implications of the transfer transparently, thereby enabling the data subjects to make an informed decision about their data while entrenching a culture of privacy in Kenyan personal data management. By mandating explicit consent, the DPA ensures that individuals retain a primary role in deciding whether or not their data is transferred internationally,[40] reflecting a commitment to preserving data subject rights as central to data governance.

Additionally, the DPA addresses the adequacy of data protections in receiving countries, a key provision that safeguards Kenyan citizens' data when it crosses borders. According to this principle, personal data transfer shall only be effected with those countries whose laws provide a level of protection of equivalent standards to the Kenyan law, aligning with global data protection standards.[41] This implies that the country to which data is being exported must, on its part, also have measures in place regarding data protection, as would be adequate according to the Data Commissioner. This means that if the data protection laws or practices of the country of destination fall short, the transfer may be restricted unless alternative safeguards, such as agreements or contracts on data protection, are established to bridge the gap in protection.[42] Through this provision on adequacy, the DPA effectively restricts data transfers to countries that have robust privacy laws, reducing the risk that Kenyan data could be mishandled or exposed to inadequate protections. This measure also aligns Kenya with international best practices, similar to mechanisms in the EU's GDPR, ensuring that data protections extend beyond Kenya's borders while upholding high privacy standards.

However, the DPA also recognizes the need for flexibility in cross-border data transfers, hence it provides for certain key specific exemptions. These exemptions permit data transfers under particular sets of circumstances even when the recipient country lacks adequate protections. For instance, if the transfer is necessary for the performance of a contract involving the data subject, the data may be shared across borders, provided that adequate safeguards are in place to protect it.[43] This would particularly apply to a multi-national company or business associates who need to share data in order to perform contractual requirements. Other exemptions include when the transfer is necessary for a legitimate interest in business or for public interest,[44] enabling organizations to operate within practical bounds while still prioritizing data protection. Nonetheless, these exemptions are not without oversight. Data controllers are still obligated to implement sufficient safeguards, such as encryption and contractual agreements,[45] to minimize risks associated with cross-border transfers under exempted conditions. This balanced approach within the Data Protection Act ensures that while Kenya upholds the highest standards with respect to data protection, it remains adaptable to functional needs concerning international data transfer.

[39] Section 46, *The Data Protection (General) Regulations* (2021).
[40] Section 25h, *Data Protection Act* (Act No. 24 of 2019).
[41] Section 44, *The Data Protection (General) Regulations* (2021).
[42] Section 44, *The Data Protection (General) Regulations* (2021).
[43] Section 48c , *Data Protection Act* (Act No. 24 of 2019).
[44] Section 48c , *Data Protection Act* (Act No. 24 of 2019).
[45] Section 48a and b , *Data Protection Act* (Act No. 24 of 2019).

The interpretation and enforcement of Kenya's data protection laws have been significantly shaped by various judicial decisions. These cases provide clarity on the application of constitutional and statutory provisions concerning data privacy and cross-border data transfers. One of the most notable rulings is the *Huduma Namba Decision,* where the High Court declared the implementation of the National Integrated Identity Management System (NIIMS) unlawful due to the government's failure to comply with the Data Protection Act 2019. Central to this case was the absence of a DPIA, a requirement for ensuring that large-scale data processing initiatives adhere to privacy and security safeguards. The court underscored that adherence to the DPA's provisions is mandatory, even for government entities, thus reaffirming the Act's application to both private and public data controllers and processors.[46] This case sets a precedent for enforcing the law in projects involving extensive data collection and cross-border transfers.

Similarly, the *Nubian Rights Forum & Others vs. Attorney General* case addressed the collection of biometric data without adequate safeguards. The court's decision emphasized the need for comprehensive regulations governing sensitive data processing, especially in cases with potential cross-border implications.[47] The judgment highlighted the importance of DPIAs, secure data transfer protocols, and explicit consent mechanisms to ensure compliance with constitutional and statutory privacy protections.[48] This case echoes the Huduma Namba ruling in demanding rigorous oversight for data governance practices involving sensitive personal data.

Together, these provisions create a multi-faceted framework in law binding data controllers and processors to scrutinize the necessity, destination, and safeguards of any cross-border data transfer they initiate. Compliance obligations for data handlers in Kenya are therefore significant; they must demonstrate full adherence to consent requirements, ensure adequate protection standards in receiving countries, and carefully assess the applicability of any exemptions. By setting these rules, the DPA not only protects Kenyan data subjects but also holds data processors and controllers accountable for maintaining the integrity and security of data in cross-border contexts. This protective stance not only underscores Kenya's commitment to aligning with international data privacy standards but also enhances the country's ability to engage in international digital business securely. In sum, the provisions for cross-border data transfer within the DPA reflect a balanced interest in individual privacy rights with the functional requirements of a connected world economy.

2.4. Complementary Legislative Frameworks, Regulations and Guidelines

In addition to the regulatory framework for cross-border data transfers, Kenya has implemented complementary laws and guidelines alongside the DPA. These additional measures work together with the DPA to create a strong governance ecosystem that emphasizes privacy,

[46] *R v Joe Mucheru (2021) eKLR.*
[47] *Nubian Rights Forum & Others vs. Attorney General (2020) eKLR.*
[48] *Nubian Rights Forum & Others vs. Attorney General (2020) eKLR.*

security and accountability. The Computer Misuse and Cybercrimes Act of 2018 is one of these complementary frameworks. It mainly targets cyber offenses such as unauthorized access,[49] interception,[50] and misuse of data, outlining legal consequences for cyber-related offenses that could compromise the integrity of personal data, both domestically and internationally. It also plays a crucial role in reinforcing data protection measures. By addressing issues such as data breaches, cyber hacking, and unauthorized data disclosure,[51] the Act helps safeguard personal data from potential misuse as it moves across borders. For instance, penalties for data breaches under this Act discourage both domestic and foreign actors from engaging in practices that could jeopardize the privacy and security of Kenyan data subjects.[52] In doing so, the Computer Misuse and Cybercrimes Act indirectly supports the secure transfer of data across borders by ensuring that stringent legal consequences are in place for data-related offenses, thus adding an extra layer of protection for data handlers engaged in cross-border exchanges.

The ODPC has also played a role in setting the framework of Kenya's cross-border data transfer through a series of practical guidelines and advisories. This guidance represents detailed interpretations of requirements under the DPA, especially regarding cross-border data processing, and hence provides an operational framework for data controllers and processors. For example, the ODPC has provided guidelines that require entities that transfer data across borders to perform DPIAs which are a core procedure when it comes to analysing and mitigating risks with cross-border data transfers, as such allows an organization to consider the implications that cross-border data transfers will have on data privacy.[53] These assessments also provide organizations mechanisms that identify vulnerabilities and address data handling processes before the data leaves Kenya's jurisdiction to ensure that personal data remains secure and compliant with Kenyan standards.

Moreover, secure transfer protocols in guidelines issued by the ODPC insists that data handlers are required to apply specific technical and organizational measures when protecting integrity and confidentiality during cross-border data transfers. These include encryption and secure data storage practices, which are instrumental in securing data moving across different digital channels into possibly less-regulated international environments.[54] In enforcing such protocols, the ODPC guidelines reduce the risks of unauthorized access or interception of data during transfers, further consolidating Kenya's adherence to the highest standards of security. Furthermore, the ODPC has standardized the requirements for obtaining consent from data subjects before their information can be transferred abroad. According to these guidelines, data handlers must use clear, easily understandable consent forms that fully inform individuals

[49] Section 14, *Computer Misuse and Cybercrimes Act*, (Act No. 5 of 2018).
[50] Section 17, *Computer Misuse and Cybercrimes Act*, (Act No. 5 of 2018).
[51] Part III, *Computer Misuse and Cybercrimes Act*, (Act No. 5 of 2018).
[52] Part III, *Computer Misuse and Cybercrimes Act*, (Act No. 5 of 2018).
[53] Office of the data protection commissioner, 'Guidance note on data protection impact assessment' Kenya data protection regulator's website, https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-on-Data-Protection-Impact-Assessment-1.pdf on 4 November 2024.
[54] Office of the data protection commissioner, 'Guidance note on registration of data controllers and data processors' Kenya data protection regulator's website, https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-on-Registration-of-Data-Controllers-and-Data-Processors.pdf on 4 November 2024.

about the nature, purpose, and implications of the cross-border data transfer.[55] This requirement enhances transparency, giving data subjects greater control over their personal information and aligning Kenya's practices with international norms for informed consent in data protection.

Together, the Computer Misuse and Cybercrimes Act and the ODPC guidelines form a cohesive set of complementary frameworks that enhance the DPA's provisions on cross-border data transfers. These laws and guidelines not only address direct concerns over data privacy and security but also establish a comprehensive framework that deters unauthorized data access, encourages secure transfer protocols, and mandates the informed consent of data subjects. By working in together with the DPA, these regulations create a multi-layered approach to data protection that balances regulatory compliance with practical enforcement mechanisms. This synergy is crucial for establishing Kenya as a regional leader in data governance, as it provides businesses and citizens with a clear, structured framework for data protection, even as data crosses international borders.

The implementation of these complementary measures highlights Kenya's proactive stance in creating a robust and adaptable data protection ecosystem. As cross-border data transfers become increasingly integral to global trade and digital economy interactions, the combined efforts of the DPA, Computer Misuse and Cybercrimes Act, and ODPC guidelines ensure that Kenya is equipped to handle the challenges of data privacy in a globalized world. These complementary regulations thus serve not only as practical extensions of the DPA's core provisions but also as essential components of a holistic data protection strategy that prioritizes the privacy, security, and rights of Kenyan data subjects in a rapidly evolving digital landscape.

2.5. Conclusion

In conclusion, Kenya's legal framework for cross-border data transfers provides an essential foundation for ensuring data protection in an increasingly digital and interconnected world. The Data Protection Act along with its supporting regulations, establishes key principles and obligations for data controllers and processors.

However, while the provisions mentioned above establish a foundation for cross-border data protection, they are not as comprehensive as those found in other frameworks. The DPA's consent requirements and adequacy provisions lack detailed guidelines, and standardized mechanisms are notably absent. Similarly, while the Act allows exemptions for essential transfers, it does not fully clarify the boundaries of such exemptions, potentially leaving room for varying interpretations.

As a result, Kenya's cross-border data transfer regulations, though present, fall short of providing a robust, consistent framework for international data protection. In the following

[55] Office of the data protection commissioner, 'Guidance notes on consent' Kenya data protection regulator's website, https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Notes-on-Consent.pdf on 4 November 2024.

chapter, an examination of the challenges and regulatory gaps within the DPA will provide a deeper understanding of these limitations and offer insights into areas where Kenya's data protection laws could be strengthened to support a more secure and privacy-centric digital economy.

CHAPTER THREE: KEY CHALLENGES AND GAPS IN KENYA'S LEGAL FRAMEWORK ON CROSS-BORDER DATA TRANSFERS

3.1. Introduction

This chapter critically examines the limitations and obstacles within the existing legal and regulatory framework governing the international flow of personal data. While Kenya's Data Protection Act 2019 and its complementary regulations provide a robust foundation for data protection, challenges in enforcement, awareness, and alignment with global standards present significant hurdles. This chapter seeks to dissect these issues to better understand their implications on data sovereignty, privacy rights, and Kenya's position in the global digital economy.

The analysis will explore gaps that hinder the efficacy of Kenya's framework, such as the lack of comprehensive enforcement mechanisms, limited clarity on emerging technologies, and insufficient public and institutional capacity to manage data-related challenges. Additionally, the discussion highlights how these gaps expose individuals and organizations to privacy risks and cybersecurity threats. By identifying and contextualizing these challenges, the chapter sets the stage for proposing viable recommendations in subsequent sections of this study.

3.2. Challenges in Kenya's Legal Framework on Cross-Border Data Transfers

Kenya's legal framework for cross-border data transfers faces several challenges that hinder its effectiveness in protecting personal data while accommodating the demands of global data flows. One of the primary challenges is the complexity and ambiguity surrounding compliance requirements for data controllers and processors.[56] While the Data Protection Act 2019 establishes conditions for cross-border transfers, such as requiring data subjects' consent and ensuring adequacy of protection in the receiving country, the operationalization of these provisions is often unclear. For example, businesses may struggle to determine what constitutes "adequate protection" in the absence of a comprehensive list of countries deemed adequate by the ODPC. An example of a country that has published a whitelist of countries that are deemed "safe" to transfer data to is Nigeria,[57] which is something Kenya should adopt to avoid lack of clarity which creates compliance uncertainty for multinational corporations and small businesses alike, potentially discouraging foreign investment and limiting Kenya's integration into the global digital economy.

Another significant challenge lies in the enforcement capacity of the ODPC. Although the ODPC has made progress in issuing guidelines and engaging stakeholders, its ability to monitor,

[56] Kageni M, 'Strengthening Data Protection in Kenya: Opportunities and the Way Forward' The Kenya institute for public policy research, 30 June 2024 https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/ on 27 November 2024.
[57] Annexure C, *Nigeria Data Protection Regulation*, November 2020.

investigate, and enforce compliance is constrained by limited resources and expertise.[58] Cross-border data transfers involve sophisticated technical systems and complex international legal arrangements, which require specialized skills to regulate effectively.[59] The ODPC's limited reach hampers its ability to identify non-compliance, particularly among multinational entities operating across multiple jurisdictions.[60] This lack of enforcement not only undermines the credibility of Kenya's data protection framework but also exposes data subjects to the risk of unauthorized or insecure data transfers.

Kenya also faces the challenge of harmonizing its domestic laws with international standards and frameworks.[61] While the Data Protection Act attempts to align with global best practices, such as those set forth by the European Union's GDPR, there remain gaps in interoperability and recognition. For example, the GDPR requires robust accountability mechanisms, such as Standard Contractual Clauses,[62] which are not explicitly defined in Kenyan law. This misalignment complicates cross-border collaborations and data-sharing agreements, as organizations are forced to navigate overlapping and sometimes conflicting legal requirements. The absence of mutual recognition agreements with major trading partners further exacerbates this challenge, limiting the seamless exchange of data necessary for international business operations.

Moreover, the rapid evolution of technology presents a continuous challenge to Kenya's legal framework. Emerging technologies such as artificial intelligence are generating unprecedented volumes of data that often flow across borders instantaneously. These developments outpace the legislative process, leaving regulators struggling to address new data protection risks.[63] For instance, real-time cross-border data processing in cloud computing environments raises

---

[58] Immaculate Kassait, 'Data Commissioner Urges Humanitarian Organizations to Prioritize Dignity of Data Subjects at Privacy Symposium Conference 2024' Office of the Data Protection Commissioner, 15 June 2024 https://www.odpc.go.ke/data-commissioner-urges-humanitarian-organizations-to-prioritize-dignity-of-data-subjects-at-privacy-symposium-conference-2024/#:~:text=The%20Data%20Commissioner%20also%20acknowledged,copy%20of%20citizens'%20data%20locally. On 28 November 2024.

[59] https://www.privacyengine.io/resources/glossary/cross-border-data-transfer/#:~:text=Cross%2Dborder%20data%20transfer%20involves,virtual%20private%20networks%20(VPNs). On 28 November 2024.

[60] Immaculate Kassait, 'Data Commissioner Urges Humanitarian Organizations to Prioritize Dignity of Data Subjects at Privacy Symposium Conference 2024' Office of the Data Protection Commissioner, 15 June 2024 https://www.odpc.go.ke/data-commissioner-urges-humanitarian-organizations-to-prioritize-dignity-of-data-subjects-at-privacy-symposium-conference-2024/#:~:text=The%20Data%20Commissioner%20also%20acknowledged,copy%20of%20citizens'%20data%20locally. On 28 November 2024.

[61] Kipkoech D, 'Navigating the Crossroads: The Challenges of Cross-Border Data Flows under Domestic Laws in Africa' Strathmore University, 23 November 2023 https://cipit.strathmore.edu/navigating-the-crossroads-the-challenges-of-cross-border-data-flows-under-domestic-laws-in-africa/ on 28 November 2024.

[62] European Commission, 'Standard Contractual Clauses' Official website of the European union, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en on 28 November 2024.

[63] Kageni M, 'Strengthening Data Protection in Kenya: Opportunities and the Way Forward' The Kenya institute for public policy research, 30 June 2024 https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/ on 28 November 2024.

questions about data localization and jurisdiction that current laws do not adequately address.[64] This lag in legal adaptation creates vulnerabilities that malicious actors can exploit, undermining both data security and privacy.

3.3. Gaps in Kenya's Legal Framework on Cross-Border Data Transfers

Despite the progress made by the Data Protection Act 2019 and related regulations, significant gaps remain in Kenya's legal framework for cross-border data transfers, undermining its effectiveness in safeguarding personal data. One critical gap is the absence of specific mechanisms for assessing and determining data protection adequacy in foreign jurisdictions. Unlike the GDPR, which provides a clear framework for adequacy decisions, Kenya's DPA does not specify the criteria or processes for evaluating whether a receiving country meets the required standards. This omission leaves data controllers and processors without clear guidance, increasing the likelihood of non-compliance and exposing data subjects to privacy risks. This is echoed by the fact that the ODPC has published several guidelines for various sectors/ activities on the Kenya Data Protection Regulator's website, but none on cross-border data transfers.[65]

Another notable gap is the limited scope of exemptions for cross-border transfers. While the DPA allows for transfers necessary for contractual performance, public interest, or legitimate business interests, it provides little detail on what constitutes these exceptions or the safeguards required to protect data under such circumstances.[66] This vagueness opens the door to potential misuse or over-reliance on exemptions, diluting the protections intended by the Act. For example, a company might justify a transfer disguised as legitimate business interests without implementing adequate security measures, placing personal data at risk.

The framework also lacks robust provisions for accountability and oversight in cross-border data transfers. While the law requires DPIAs for high-risk activities, including cross-border transfers, there is no detailed guidance on such assessments' content, methodology, or review process.[67] Without standardized DPIA templates or enforcement mechanisms, organizations may adopt inconsistent approaches, undermining the effectiveness of this safeguard.

Kenya's framework is also insufficiently integrated with regional data protection initiatives. For instance, while the African Union's Malabo Convention encourages member states to adopt harmonized data protection standards, Kenya has yet to fully implement its provisions.[68] This

---

[64] Kijirah M, *Data protection and data localisation in Kenya: Potential economic impact and effect on Kenya's commitments in various regional treaty frameworks*, Mandela Institute, School of Law, Johannesburg, 2021.
[65] Office of the data protection commissioner, 'Guidelines' Kenya data protection regulator's website, https://www.odpc.go.ke/guidelines-2/ on 29 November 2024.
[66] Office of the data protection commissioner, 'Guidelines' Kenya data protection regulator's website, https://www.odpc.go.ke/guidelines-2/ on 29 November 2024.
[67] Office of the data protection commissioner, 'Guidelines' Kenya data protection regulator's website, https://www.odpc.go.ke/guidelines-2/ on 29 November 2024.
[68] 'List of countries which have signed, ratified/acceded to the African union convention on cyber security and personal data protection' African union, https://dataprotection.africa/wp-content/uploads/2305121.pdf on 29 November 2024.

isolation not only limits opportunities for international cooperation but also weakens Kenya's position as a competitive player in the global digital economy.

Lastly, there is a notable gap in public awareness and stakeholder engagement regarding cross-border data transfers.[69] Many Kenyan citizens and businesses remain unaware of their rights and obligations under the DPA, reducing the effectiveness of its provisions. For instance, data subjects may consent to transfers without fully understanding the risks or implications,[70] while data handlers may fail to implement adequate safeguards due to a lack of knowledge. This gap underscores the need for targeted education and capacity-building initiatives to enhance compliance and empower individuals to exercise their data protection rights effectively.

3.4. Impact of Gaps and Challenges

The gaps and challenges within Kenya's legal framework for cross-border data transfers have profound implications, affecting not only compliance with data protection norms but also the broader socio-economic landscape. From an economic perspective, the ambiguity and lack of harmonization with international standards pose significant barriers for Kenyan businesses engaging in cross-border trade.[71] For instance, Kenyan companies interacting with jurisdictions like the EU may struggle to comply with the stringent GDPR. The GDPR requires data transfers to meet adequacy requirements or rely on mechanisms such as SCCs.[72] The lack of a Kenyan adequacy decision from the EU implies that companies must undertake costly legal arrangements or technical adaptations, placing small and medium enterprises (SMEs) at a distinct disadvantage. This reduces the competitiveness of Kenyan businesses in the global digital market, limiting their opportunities for innovation and growth.

In addition, the legal and regulatory gaps negatively impact Kenya's attractiveness as an investment destination in the digital economy.[73] Multinational companies and tech giants often prioritize jurisdictions with robust, predictable data protection frameworks to minimize regulatory risks.[74] The uncertainty surrounding Kenya's cross-border data transfer laws may deter foreign investors, who might view the country's legal framework as inadequate for safeguarding sensitive data. This is particularly critical given the increasing reliance on data-driven technologies and industries, where the movement of data across borders is integral to

[69] Kipkoech D, 'Navigating the Crossroads: The Challenges of Cross-Border Data Flows under Domestic Laws in Africa' Strathmore University, 23 November 2023 https://cipit.strathmore.edu/navigating-the-crossroads-the-challenges-of-cross-border-data-flows-under-domestic-laws-in-africa/ on 2 December 2024.
[70] Gadhia A, 'Worldcoin case a 'watershed moment' for data protection in Kenya' iapp, 15 September 2023 https://iapp.org/news/a/worldcoin-case-a-watershed-moment-for-data-protection-in-kenya on 2 December 2024.
[71] Kipkoech D, 'Navigating the Crossroads: The Challenges of Cross-Border Data Flows under Domestic Laws in Africa' Strathmore University, 23 November 2023 https://cipit.strathmore.edu/navigating-the-crossroads-the-challenges-of-cross-border-data-flows-under-domestic-laws-in-africa/ on 2 December 2024.
[72] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en on 2 December 2024.
[73] Kipkoech D, 'Navigating the Crossroads: The Challenges of Cross-Border Data Flows under Domestic Laws in Africa' Strathmore University, 23 November 2023 https://cipit.strathmore.edu/navigating-the-crossroads-the-challenges-of-cross-border-data-flows-under-domestic-laws-in-africa/ on 2 December 2024.
[74] United States International Trade Commission, Data protection laws in Africa: A Pan-African survey and noted trends, 2021, 3.

operations.[75] Without addressing these gaps, Kenya risks being sidelined in the global data economy, missing out on significant economic benefits such as increased foreign direct investment, job creation, and technological advancement.

International cooperation and trust are also jeopardized by these challenges.[76] Countries with stringent data protection laws may restrict the flow of data to Kenya, perceiving its regulatory framework as insufficient to guarantee the protection of their citizens' personal data. This creates a fragmented data environment where Kenyan businesses and government agencies face restrictions on accessing global digital resources or forming international partnerships. For example, bilateral or multilateral agreements requiring data reciprocity may falter if Kenya's data protection framework does not meet the expectations of its counterparts. This lack of trust undermines not only trade and diplomatic relations but also Kenya's ability to participate meaningfully in global initiatives aimed at fostering a harmonized digital ecosystem.[77]

Lastly, the gaps and challenges in our cross-border data governance framework also have implications for its citizens' digital rights and freedoms.[78] The absence of explicit provisions for data sovereignty and local storage requirements raises questions about the protection of data held by foreign entities. Without a clear legal recourse in case of breaches occurring in other jurisdictions, individuals are left in a vulnerable position, unable to effectively enforce their rights or seek redress. Moreover, this legal ambiguity maintains a culture of non-accountability among data controllers and processors, further eroding public trust in Kenya's data protection mechanisms.

3.5. Conclusion

In conclusion, despite Kenya's commendable progress in establishing a legal framework for cross-border data transfers, several challenges persist. Key gaps include enforcement ambiguities, weak compliance mechanisms, and insufficient operational resources like robust DPIAs. These shortcomings expose Kenya to increased cybersecurity threats, hinder international trust, and limit its participation in the global digital economy. Addressing these issues is crucial to strengthening the framework's effectiveness, ensuring secure data exchanges, and positioning Kenya as a leader in digital governance.

---

[75] United States International Trade Commission, Data protection laws in Africa: A Pan-African survey and noted trends, 2021, 5.
[76] Kipkoech D, 'Navigating the Crossroads: The Challenges of Cross-Border Data Flows under Domestic Laws in Africa' Strathmore University, 23 November 2023 https://cipit.strathmore.edu/navigating-the-crossroads-the-challenges-of-cross-border-data-flows-under-domestic-laws-in-africa/ on 2 December 2024.
[77] Kipkoech D, 'Navigating the Crossroads: The Challenges of Cross-Border Data Flows under Domestic Laws in Africa' Strathmore University, 23 November 2023 https://cipit.strathmore.edu/navigating-the-crossroads-the-challenges-of-cross-border-data-flows-under-domestic-laws-in-africa/ on 2 December 2024.
[78] Kijirah M, *Data protection and data localisation in Kenya: Potential economic impact and effect on Kenya's commitments in various regional treaty frameworks*, Mandela Institute, School of Law, Johannesburg, 2021.

CHAPTER FOUR: CROSS-BORDER DATA TRANSFERS IN THE NETHERLANDS: LESSONS FOR KENYA

4.1. Introduction

The Netherlands is a strong advocate for data protection within the EU, adhering closely to the GDPR while implementing additional national measures to enhance its framework. The Dutch Data Protection Authority (Autoriteit Persoonsgegevens,) plays a key role in ensuring compliance with GDPR provisions, particularly in cross-border data transfers.[79] This chapter examines how the Netherlands enforces GDPR requirements, the authority's role in ensuring secure data flows, and the legal mechanisms governing data transfer. It lays the groundwork for comparing Kenya's framework with the Dutch model to identify areas where Kenya can improve its approach to cross-border data regulation.

4.2. The Netherlands' Legal Framework for Cross-Border Data Transfers

The Netherlands demonstrates a robust approach to cross-border data transfers, deeply embedded within the EU's GDPR. A key aspect of the Dutch framework is its active enforcement of GDPR principles, which ensures data privacy and security remain uncompromised, even when data flows beyond EU borders. The Dutch Data Protection Authority, Autoriteit Persoonsgegevens (AP), plays a central role in this regard.[80] Through its oversight, organizations are compelled to adhere to stringent data transfer requirements, including obtaining informed consent, employing data protection mechanisms such as SCCs, and conducting thorough Transfer Impact Assessments (TIAs).[81] For instance, following the Schrems II ruling in 2020, which invalidated the EU-U.S. Privacy Shield,[82] the AP issued guidance on mitigating risks in cross-border transfers by emphasizing alternative safeguards like SCCs and Binding Corporate Rules (BCRs).[83] This case exemplifies the Netherlands' proactive measures to align domestic practices with international rulings.

---

[79] https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa on 7 January 2025.
[80] Van der Laan, 'Data protection laws and regulations Netherlands 2024-2025' ICLG news, 31 July 2024 https://iclg.com/practice-areas/data-protection-laws-and-regulations/netherlands#:~:text=Therefore%2C%20the%20Dutch%20Government%20passed,could%20add%20to%20or%20vary. On 7 January 2025.
[81] https://gdprhub.eu/AP_(The_Netherlands)#:~:text=The%20Dutch%20Data%20Protection%20Authority,of%20enforcing%20GDPR%20in%20Netherlands. On 7 January 2025.
[82] *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (2020), Court of Justice of the European Union.
[83] https://www.autoriteitpersoonsgegevens.nl/en/themes/international/transfer-within-and-outside-the-eea/binding-corporate-rules-bcr on 7 January 2025.

The Netherlands also showcases its commitment to digital sovereignty, particularly within the EU, through initiatives such as the GAIA-X project. This European initiative, supported by the Dutch government, aims to establish a secure cloud infrastructure, reducing reliance on non-EU service providers and safeguarding data generated within the EU.[84] By advocating for such frameworks, the Netherlands ensures data originating within its jurisdiction remains protected from unauthorized external access, thus reinforcing GDPR standards at an infrastructural level.

Practical enforcement of these principles is evident in several high-profile cases. For example, Dutch authorities fined Booking.com 475,000 euros for failing to promptly report a data breach that exposed sensitive customer data.[85] This case underscores the Netherlands' rigorous approach to ensuring compliance with GDPR, even in cross-border contexts. Similarly, concerns raised by Dutch authorities over the use of Microsoft products in schools and government institutions highlight potential risks associated with the U.S. Cloud Act, which could expose EU data to foreign surveillance.[86] By scrutinizing such practices, the Netherlands reinforces its stance on protecting the integrity and security of cross-border data transfers.

Furthermore, the Netherlands aligns with broader EU legislation, such as the Data Governance Act and the Digital Markets Act, to enhance transparency and accountability in data flows across borders.[87] For example, these laws strengthen protections for sensitive data categories, such as health data, that may be shared with foreign entities.[88] This alignment ensures that Dutch practices are not only compliant with GDPR but also serve as a model for other jurisdictions striving for secure cross-border data governance.

In essence, the Netherlands' approach is characterized by a blend of strict regulatory enforcement, technological innovation, and alignment with broader EU strategies. These measures ensure that cross-border data transfers adhere to the highest standards of data protection while balancing the need for international cooperation in the digital economy. Kenya can draw valuable lessons from these practices, to strengthen its own cross-border data transfer framework.

4.3. The Netherlands' Practical Approaches and Enforcement Mechanisms

The Netherlands, through its Data Protection Authority, has established robust and practical approaches to ensure compliance with GDPR requirements, particularly in cross-border data transfers. A key pillar of this strategy is the AP's proactive guidance. The authority frequently

[84] https://gaia-x.nl/en/ on 8 January 2025.
[85] 'Dutch SA fines Booking.com for delay in reporting data breach' Official website of the European Union, 10 December 2020 https://www.edpb.europa.eu/news/national-news/2020/dutch-sa-fines-bookingcom-delay-reporting-data-breach_en#:~:text=Booking.com%20was%20informed%20of,decision%20in%20national%20language%20(NL) on 8 January 2025.
[86] https://www.privacycompany.eu/blog/new-dpia-for-the-dutch-government-and-universities-on-microsoft-teams-onedrive-and-sharepoint-online on 8 January 2025.
[87] 'Netherlands – digital economy' Official website of the international trade administration, 20 September 2024 https://www.trade.gov/country-commercial-guides/netherlands-digital-economy on 8 January 2025.
[88] https://business.gov.nl/regulation/protection-personal-data/ on 8 January 2025.

issues detailed guidance documents and recommendations which help organizations interpret GDPR provisions, including those on cross-border data transfers.[89] For instance, its emphasis on the principle of accountability requires companies to demonstrate compliance through thorough documentation and policies.[90] This approach ensures that organizations internalize data protection principles, reducing reliance on post-incident enforcement.

Moreover, the AP actively conducts audits to assess organizations' adherence to GDPR requirements, including secure data transfer mechanisms. These audits often focus on high-risk sectors such as financial services and technology companies, where cross-border data transfers are prevalent.[91] A notable example was the AP's scrutiny of TikTok's handling of EU users' data, which raised concerns about data access by entities outside the EU.[92] By imposing a fine and demanding operational adjustments, the AP demonstrated its commitment to safeguarding European data against unauthorized external access.

Secure transfer mechanisms are central to the Netherlands' approach, with an emphasis on implementing technical and organizational measures. The Netherlands encourages data encryption and other security practices to ensure the integrity and confidentiality of personal data during transfer.[93] Additionally, DPIAs are a cornerstone of compliance, particularly for transfers to jurisdictions lacking adequacy decisions.[94] The AP insists on rigorous DPIAs that evaluate risks and recommend mitigation strategies, ensuring that potential vulnerabilities are identified and addressed before data leaves the EU.

International cooperation also plays a vital role in the Netherlands' data protection enforcement. The AP works closely with EU institutions like the European Data Protection Board to coordinate cross-border investigations and enforce uniform GDPR standards.[95] For example, the One-Stop-Shop mechanism enables the AP to collaborate with other EU data protection

[89] 'Tasks and powers of the Dutch DPA' Autoriteit persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/tasks-and-powers-of-the-dutch-dpa#:~:text=The%20Dutch%20Data%20Protection%20Authority,the%20use%20of%20personal%20data on 8 January 2025.
[90] 'Duty of accountability' Autoriteit persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/duty-of-accountability on 8 January 2025.
[91] 'Netherlands – digital economy' Official website of the international trade administration, 20 September 2024 https://www.trade.gov/country-commercial-guides/netherlands-digital-economy on 8 January 2025.
[91] https://business.gov.nl/regulation/protection-personal-data/ on 8 January 2025.
[92] European Data Protection Board, 'Dutch DPA: Tiktok fined for violating children's privacy' Official website of the European Union, 22 July 2021 https://www.edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en on 9 January 2025.
[93] 'Tasks and powers of the Dutch DPA' Autoriteit persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/tasks-and-powers-of-the-dutch-dpa#:~:text=The%20Dutch%20Data%20Protection%20Authority,the%20use%20of%20personal%20data on 9 January 2025.
[94] https://www.gdpradvisor.co.uk/gdpr-compliance-audit#:~:text=Understand%20the%20requirements%20of%20GDPR,activities%20as%20required%20by%20GDPR. On 9 January 2025.
[95] 'Tasks and powers of the Dutch DPA' Autoriteit persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/tasks-and-powers-of-the-dutch-

authorities when handling cases involving multinational companies, streamlining enforcement across jurisdictions.[96]

As a leading data centre hub in Europe, the Netherlands has had to balance its economic role with stringent data protection standards. The country hosts numerous multinational tech companies and cloud service providers, making it a pivotal player in global data flows. Despite this, the AP maintains a strict oversight regime to ensure compliance.[97] For instance, Amsterdam's data centres, which handle significant volumes of international data traffic, are subject to routine assessments to confirm that data transfers align with GDPR directives.[98]

Through these practical approaches and enforcement mechanisms, the Netherlands showcases how a proactive regulatory framework can enable robust data protection while facilitating economic participation in the digital age.

4.4. Comparative Analysis: Netherlands vs. Kenya

One significant area of comparison lies in the roles and effectiveness of their respective data protection authorities. The Dutch Data Protection Authority (AP) operates with extensive resources and authority, enabling it to issue significant fines and release detailed guidance to ensure compliance.[99] For example, the AP has issued fines exceeding 1 million euros in high-profile cases, demonstrating its commitment to strict enforcement. Kenya's ODPC, has made notable strides but remains constrained by limited resources and institutional capacity.[100] The ODPC's recent guidelines on cross-border data transfers are a step in the right direction, but the authority's enforcement mechanisms and public engagement strategies remain underdeveloped compared to the Dutch model.

---

dpa#:~:text=The%20Dutch%20Data%20Protection%20Authority,the%20use%20of%20personal%20data on 9 January 2025.

[96] 13 February 2024 https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2024/netherlands/trends-and-developments#:~:text=In%20principle%2C%20no%20personal%20data%20may%20be,organisational%20measures%20in%20place%20for%20the%20transfer on 9 January 2025.

[97] 'Netherlands – digital economy' Official website of the international trade administration, 20 September 2024 https://www.trade.gov/country-commercial-guides/netherlands-digital-economy on 9 January 2025.

[97] https://business.gov.nl/regulation/protection-personal-data/ on 9 January 2025.

[98] Kokke D, 'RoyalHaskoningDHV: Predictive monitoring in data centres' Dutch data center association, 5 November 2024 https://www.dutchdatacenters.nl/en/nieuws/royalhaskoningdhv-predictive-monitoring-in-data-centres/ on 9 January 2025.

[99] 'Tasks and powers of the Dutch DPA' Autoriteit persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/tasks-and-powers-of-the-dutch-dpa#:~:text=The%20Dutch%20Data%20Protection%20Authority,the%20use%20of%20personal%20data on 10 January 2025.

[100] Indeje D, 'New report identifies achievements, challenges and recommendations to enhance data protection in Kenya' KICTANet, 8 May 2024 https://www.kictanet.or.ke/new-report-identifies-achievements-challenges-and-recommendations-to-enhance-data-protection-in-kenya/#:~:text=He%20also%20highlighted%20some%20challenges,other%20sectors%20regulators.%E2%80%9D%20He%20added on 10 January 2025.

In terms of adequacy decisions, the Netherlands, through the GDPR, benefits from the EU's stringent adequacy framework, which evaluates third countries' data protection systems before permitting data transfers. This framework ensures that personal data transferred out of the EU remains protected to a standard equivalent to that provided within the EU.[101] Kenya, however, lacks a comparable mechanism, relying instead on contractual safeguards and data subject consent.[102] This difference highlights an area where Kenya could benefit from adopting a more structured adequacy assessment process, perhaps modelled on the EU system.

Consent requirements and public awareness also differ between the two countries. The Netherlands places significant emphasis on informed consent,[103] backed by user-friendly guidelines and active public campaigns to educate individuals about their rights under the GDPR.[104] For instance, Dutch authorities regularly collaborate with civil society organizations to enhance digital literacy and awareness of data protection rights.[105] Kenya, while also mandating consent for data processing, faces challenges in ensuring that consent mechanisms are genuinely informed and accessible, particularly for marginalized communities with limited digital literacy.[106]

Secure transfer protocols and enforcement mechanisms further illustrate the contrast. The Netherlands mandates the use of advanced encryption methods, secure cloud practices, and comprehensive DPIAs for cross-border transfers.[107] DPIAs, required under the GDPR, have been effectively implemented by Dutch organizations, ensuring that potential risks to data privacy are identified and mitigated before transfers occur. Kenya's regulatory framework acknowledges these principles but falls short in providing specific operational guidelines or the technical capacity to enforce compliance.[108]

The Netherlands' status as a global data centre hub offers additional insights for Kenya. Despite hosting large-scale data operations, the Netherlands maintains a balance between data-driven innovation and robust privacy safeguards. This balance is achieved through stringent oversight, clear legal obligations, and a culture of corporate accountability. Kenya, aspiring to be a

---

[101] https://www.dpocentre.com/navigating-international-data-transfers-tias-vs-tras/ on 10 January 2025.
[102] Section 46, *The Data Protection (General) Regulations* (2021).
[103] Article 7, *General Data Protection Regulation (GDPR) ((EU) 2016/679).*
[104] Ulco van de Pol, 'Aiming for effective co-regulation of data protection: policies and practices of the Dutch DPA' Autoriteit persoonsgegevens https://autoriteitpersoonsgegevens.nl/uploads/imported/art_upo_2003_rve.pdf on 10 January 2025.
[105] 'Netherlands – digital economy' Official website of the international trade administration, 20 September 2024 https://www.trade.gov/country-commercial-guides/netherlands-digital-economy on 10 January 2025.
[105] https://business.gov.nl/regulation/protection-personal-data/ on 10 January 2025.
[106] Gadhia A, 'Worldcoin case a 'watershed moment' for data protection in Kenya' iapp, 15 September 2023 https://iapp.org/news/a/worldcoin-case-a-watershed-moment-for-data-protection-in-kenya on 11 January 2025.
[107] Jongen H, 'Privacy, data protection and cybersecurity: Netherlands' Lexology, 30 September 2024 https://www.lexology.com/indepth/privacy-data-protection-and-cybersecurity/netherlands on 11 January 2025.
[108] Indeje D, 'New report identifies achievements, challenges and recommendations to enhance data protection in Kenya' KICTANet, 8 May 2024 https://www.kictanet.or.ke/new-report-identifies-achievements-challenges-and-recommendations-to-enhance-data-protection-in-kenya/#:~:text=He%20also%20highlighted%20some%20challenges,other%20sectors%20regulators.%E2%80%9D%20He%20added on 11 January 2025.

regional ICT hub, can draw valuable lessons from this approach, particularly in managing data centres and fostering a culture of compliance among organizations.

4.5. Lessons and Best Practices for Kenya

One key lesson is the importance of regulatory clarity. The Netherlands benefits from a well-defined regulatory framework that integrates GDPR requirements into national legislation with clear guidance from the AP.[109] This clarity ensures that both organizations and individuals fully understand their rights and responsibilities. For instance, the AP regularly publishes accessible guidance documents to explain complex regulatory requirements, fostering both compliance and public trust.[110] Kenya could emulate this proactive engagement by the ODPC, developing simplified materials, hosting forums, and increasing transparency about enforcement actions. Greater clarity would not only enhance compliance but also improve the confidence of international stakeholders in Kenya's regulatory framework.

The Netherlands' emphasis on proactive compliance strategies is another best practice that Kenya can adopt. Dutch organizations are required to conduct mandatory DPIAs for high-risk data transfers, ensuring that potential privacy risks are addressed before they occur.[111] The AP has also partnered with companies to develop sector-specific guidelines tailored to industries such as finance and healthcare, allowing businesses to implement GDPR principles more effectively.[112] Kenya's ODPC could introduce mandatory DPIAs for certain categories of cross-border transfers, along with targeted guidance for sectors critical to Kenya's economy, such as agriculture and ICT. For example, by offering templates for DPIAs and sector-specific compliance checklists, the ODPC could make compliance more achievable for small and medium enterprises.

Fostering international partnerships is another area where Kenya can learn from the Netherlands. The Netherlands actively collaborates with EU member states and global organizations to align its practices with international standards and address emerging challenges.[113] For instance, the Dutch government has been instrumental in shaping the EU's stance on data sovereignty and cross-border data flows. Similarly, Kenya could strengthen its

---

[109] 'About the Dutch DPA' Autoriteit persoonsgegevens https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/organization-dutch-dpa#:~:text=The%20Dutch%20DPA%20(Autoriteit%20Persoonsgegevens,is%20divided%20into%206%20directorates on 16 January 2025.

[110] 'Documents' Autoriteit persoonsgegevens https://www.autoriteitpersoonsgegevens.nl/en/documents on 16 January 2025.

[111] 'Data protection impact assessment' Autoriteit persoonsgegevens https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia#:~:text=Does%20an%20organisation%20intend%20to,Criminal%20Records%20Act%20(Wjsg) on 16 January 2025.

[112] Ulco van de Pol, 'Aiming for effective co-regulation of data protection: policies and practices of the Dutch DPA' Autoriteit persoonsgegevens https://autoriteitpersoonsgegevens.nl/uploads/imported/art_upo_2003_rve.pdf on 16 January 2025.

[113] https://www.government.nl/topics/european-union/the-netherlands-and-developments-within-the-eu#:~:text=As%20a%20Member%20State%2C%20the,and%20rules%20will%20be%20amended on 17 January 2025.

ties with regional and international bodies, such as the African Union and the International Telecommunication Union, to harmonize data protection practices and build a coalition for advocating Africa-centric data governance standards. Participation in cross-border regulatory dialogues would also allow Kenya to stay informed about global trends and adapt its policies accordingly.

Lastly, the Dutch experience underscores the importance of embedding a culture of accountability. The Netherlands emphasizes not only regulatory compliance but also the ethical responsibility of organizations handling personal data. Public campaigns and educational programs raise awareness among citizens about their data rights,[114] empowering them to demand accountability from data controllers. Kenya could implement nationwide campaigns to promote digital literacy, particularly targeting marginalized groups, to ensure equitable access to information and a stronger understanding of data protection rights.

4.6. Conclusion

In conclusion, this chapter has provided a comprehensive analysis of the Netherlands' robust framework for cross-border data transfers under the GDPR, highlighting its proactive enforcement mechanisms, clear regulatory structures, and strong emphasis on data sovereignty. By comparing these practices with Kenya's evolving framework, it becomes evident that Kenya can benefit significantly from adopting lessons from the Dutch model, including fostering international collaboration, ensuring compliance through guidance and audits, and prioritizing transparency and public engagement. These insights lay the foundation for strengthening Kenya's data governance to align with global standards while addressing local challenges.

[114] Ulco van de Pol, 'Aiming for effective co-regulation of data protection: policies and practices of the Dutch DPA' Autoriteit persoonsgegevens https://autoriteitpersoonsgegevens.nl/uploads/imported/art_upo_2003_rve.pdf on 17 January 2025.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

5.1. Introduction

The regulation of cross-border data transfers has become an essential aspect of digital governance, particularly in an era where economic activity, communication, and public services increasingly depend on global data flows.[115] Kenya's Data Protection Act and its accompanying regulations mark a significant step toward safeguarding personal data in international contexts. However, as demonstrated in this study, gaps remain in enforcement mechanisms, adequacy determinations, and compliance requirements, raising concerns about the effectiveness of Kenya's regulatory framework in ensuring robust data protection.

This final chapter synthesizes the key findings of the research, providing a comprehensive overview of Kenya's current legal framework and its limitations. It also presents recommendations aimed at enhancing the country's approach to cross-border data transfers by incorporating best practices from jurisdictions such as the Netherlands. By addressing these issues, Kenya can strengthen its position as a secure and competitive digital economy while ensuring the protection of personal data in line with international standards.

5.2. Conclusion

The research has provided an in-depth analysis of Kenya's legal framework on cross-border data transfers, highlighting its strengths and weaknesses in comparison to international standards and best practices. Kenya's cross-border data transfer framework, anchored in the Data Protection Act, establishes a legal basis for regulating data flows.[116] However, its provisions on consent, adequacy decisions, and transfer safeguards lack detailed implementation guidelines, leading to inconsistencies in enforcement. The absence of clear exemptions further complicates compliance for individuals and businesses handling international data transfers.

The ODPC plays a crucial role in overseeing data protection compliance in Kenya, including cross-border data transfers. However, its enforcement capacity is constrained by limited resources, technical expertise, and institutional authority.[117] The ODPC lacks the extensive regulatory experience and infrastructure seen in more mature data protection authorities, such

[115] https://globaldataalliance.org/wp-content/uploads/2021/07/02112020GDAcrossborderdata.pdf on 19 January 2025.
[116] Part VI, *Data Protection Act* (Act No. 24 of 2019).
[117] Immaculate Kassait, 'Data Commissioner Urges Humanitarian Organizations to Prioritize Dignity of Data Subjects at Privacy Symposium Conference 2024' Office of the Data Protection Commissioner, 15 June 2024 https://www.odpc.go.ke/data-commissioner-urges-humanitarian-organizations-to-prioritize-dignity-of-data-subjects-at-privacy-symposium-conference-2024/#:~:text=The%20Data%20Commissioner%20also%20acknowledged,copy%20of%20citizens'%20data%20locally. On 19 January 2024.

as the Dutch Data Protection Authority which operates within the well-established framework of the GDPR.[118]

Unlike the Netherlands, where the regulator actively issues fines, conducts audits, and provides detailed compliance guidelines,[119] the ODPC has only recently begun enforcing penalties and remains largely dependent on voluntary compliance. Additionally, Kenya's framework does not yet have a well-defined mechanism for handling adequacy decisions or for ensuring that businesses implement effective safeguards for international data transfers. Without strengthened regulatory capacity and clearer enforcement mechanisms, Kenya risks falling behind in ensuring robust cross-border data protection.

The Netherlands, under the GDPR, enforces strict data protection measures, including well-defined transfer protocols and proactive regulatory oversight. Its adequacy assessment framework ensures that data transfers outside the EU comply with rigorous privacy standards, reducing risks associated with cross-border data flows.[120] The Dutch Data Protection Authority actively monitors compliance, imposes penalties for violations, and provides detailed guidance to organizations on lawful data transfers.

Additionally, the Netherlands emphasizes digital sovereignty, ensuring that data originating within the EU is protected from unauthorized foreign access.[121] This commitment to safeguarding personal data while enabling international data flows offers Kenya a strong model for enhancing its own regulatory framework. By adopting similar enforcement mechanisms, clear adequacy criteria, and proactive compliance strategies, Kenya can strengthen its cross-border data protection regime and align more closely with global best practices.

5.3. Recommendations

To enhance Kenya's cross-border data transfer regulations and address the identified gaps, several recommendations are proposed. These recommendations draw from international best practices, particularly from the Netherlands and the broader European framework, while considering Kenya's unique regulatory landscape and economic environment.

Firstly, Kenya should adopt a clear and structured adequacy framework for determining whether a recipient country provides sufficient data protection. The Netherlands operates under the GDPR, which has a defined process for assessing the adequacy of third countries before

[118] https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa on 19 January 2025.
[119] 'Tasks and powers of the Dutch DPA' Autoriteit persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/tasks-and-powers-of-the-dutch-dpa#:~:text=The%20Dutch%20Data%20Protection%20Authority,the%20use%20of%20personal%20data on 21 January 2025.
[120] Van der Laan, 'Data protection laws and regulations Netherlands 2024-2025' ICLG news, 31 July 2024 https://iclg.com/practice-areas/data-protection-laws-and-regulations/netherlands#:~:text=Therefore%2C%20the%20Dutch%20Government%20passed,could%20add%20to%20or%20vary. On 21 January 2025.
[121] https://www.dpocentre.com/navigating-international-data-transfers-tias-vs-tras/ on 21 January 2025.

permitting data transfers.[122] Kenya's DPA should similarly establish well-defined criteria for evaluating the adequacy of foreign jurisdictions. This can be achieved through structured guidelines issued by the ODPC, which should outline specific legal, security, and institutional factors that determine whether a receiving country offers comparable protection, and by publishing a whitelist of countries deemed "safe" to transfer data to like Nigeria did.[123]

Secondly, Kenya should strengthen the enforcement capacity of the ODPC by increasing financial and technical resources, as well as expanding its authority to conduct compliance audits and impose penalties effectively. The Dutch Data Protection Authority has significant enforcement powers, including the ability to impose substantial fines for non-compliance.[124] While Kenya's ODPC has enforcement authority, it faces limitations due to resource constraints and a developing compliance culture among organizations.[125] Increasing funding, staffing, and technological capacity for the ODPC would enhance its ability to monitor compliance, conduct audits, and respond to breaches faster.

Kenya should develop more precise and comprehensive guidelines for obtaining valid consent in cross-border data transfers. Under the GDPR, the Netherlands enforces stringent requirements on user consent, ensuring that data subjects are fully informed about how their data will be transferred and processed abroad.[126] In contrast, Kenya's DPA lacks detailed mechanisms for ensuring informed and explicit consent in cross-border scenarios.[127] Strengthening regulations on how organizations obtain, document, and manage consent will improve compliance and enhance data subject rights.

Additionally, Kenya should promote transparency and accountability through mandatory DPIAs for high-risk cross-border data transfers. The Netherlands requires organizations to conduct DPIAs in cases where data transfers pose significant privacy risks, particularly when sending data to jurisdictions with weaker protection frameworks.[128] Introducing a similar

---

[122] Jongen H, 'Privacy, data protection and cybersecurity: Netherlands' Lexology, 30 September 2024 https://www.lexology.com/indepth/privacy-data-protection-and-cybersecurity/netherlands on 23 January 2025.
[123] Annexure C, *Nigeria Data Protection Regulation*, November 2020.
[124] 'Tasks and powers of the Dutch DPA' Autoriteit persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/tasks-and-powers-of-the-dutch-dpa#:~:text=The%20Dutch%20Data%20Protection%20Authority,the%20use%20of%20personal%20data on 23 January 2025.
[125] Immaculate Kassait, 'Data Commissioner Urges Humanitarian Organizations to Prioritize Dignity of Data Subjects at Privacy Symposium Conference 2024' Office of the Data Protection Commissioner, 15 June 2024 https://www.odpc.go.ke/data-commissioner-urges-humanitarian-organizations-to-prioritize-dignity-of-data-subjects-at-privacy-symposium-conference-2024/#:~:text=The%20Data%20Commissioner%20also%20acknowledged,copy%20of%20citizens'%20data%20locally. On 23 January 2024.
[126] Article 7, *General Data Protection Regulation (GDPR) ((EU) 2016/679).*
[127] Gadhia A, 'Worldcoin case a 'watershed moment' for data protection in Kenya' iapp, 15 September 2023 https://iapp.org/news/a/worldcoin-case-a-watershed-moment-for-data-protection-in-kenya on 24 January 2025.
[128] https://www.gdpradvisor.co.uk/gdpr-compliance-audit#:~:text=Understand%20the%20requirements%20of%20GDPR,activities%20as%20required%20by%20GDPR. On 24 January 2025.

requirement in Kenya would ensure that businesses and government entities proactively identify and address risks before engaging in international data transfers.

Kenya should also foster greater international cooperation and participation in global and regional data protection initiatives. The Netherlands actively collaborates with the European Data Protection Board and other international bodies to harmonize data protection approaches and enhance enforcement efforts.[129] Kenya should engage with regional blocs such as the African Union and East African Community to develop harmonized data protection standards. This would not only facilitate smoother data flows within Africa but also position Kenya as a reliable hub for digital commerce and investment.

Finally, Kenya should invest in public awareness and capacity-building programs to ensure businesses, government institutions, and individuals understand their rights and obligations under the Data Protection Act. Many organizations struggle with compliance due to a lack of awareness or technical expertise. By implementing training programs, publishing guidance materials, and conducting outreach initiatives, Kenya can strengthen its data protection culture and ensure sustainable compliance with international best practices.

By implementing these recommendations, Kenya can build a robust and globally competitive data protection regime that supports digital innovation while ensuring the highest standards of privacy and security in cross-border data transfers.

[129] 'Tasks and powers of the Dutch DPA' Autoriteit persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/tasks-and-powers-of-the-dutch-dpa#:~:text=The%20Dutch%20Data%20Protection%20Authority,the%20use%20of%20personal%20data on 24 January 2025.

BIBLIOGRAPHY

Books

1. Abu, S. *Cross-Border Data Transfer and Privacy Protection*. Oxford University Press, 2019.
2. Braithwaite, J. *Responsive Regulation: Transcending the Deregulation Debate*. Oxford University Press, 2002.
3. Green, T. *Data Governance and Accountability: A Comparative Study*. Cambridge University Press, 2018.
4. Kijirah, M., & Thuo, J. *Data Sovereignty in the Digital Age: Implications for Trade and Privacy*. Routledge, 2020.
5. Lipsky, M. *Street-Level Bureaucracy: Dilemmas of the Individual in Public Services*. Russell Sage Foundation, 1980.
6. Veblen, T. *The Theory of the Leisure Class*. Macmillan, 1899.

Journals

1. Mwangi, S. N., 'Challenges in Enforcing Data Protection Laws in Developing Economies: A Case Study of Kenya' (2021) 14(2) *African Journal of Law and Technology* 87.
2. Owuor, J., & Brian, K., 'Legal Implications of Cross-Border Data Transfers in Africa: A Comparative Analysis' (2020) 22(4) *International Journal of Digital Law* 45.
3. Taylor, M., 'Institutional Capacity and the Effectiveness of Data Protection Laws' (2019) 10(3) *Global Privacy Review* 133.

Reports

1. Centre for International Governance Innovation (CIGI), *The State of Data Governance in Africa*, 2021.
2. Office of the Data Protection Commissioner (ODPC), *Guidelines on Data Protection Impact Assessments*, 2022.
3. Office of the Data Protection Commissioner (ODPC), *Secure Transfer Protocols for Cross-Border Data Transfers*, 2023.

Online sources

1. Office of the data protection commissioner, 'Guidelines' Kenya data protection regulator's website, https://www.odpc.go.ke/guidelines-2/ on 12 September 2024.
2. What is regulatory compliance?' metricstream, https://www.metricstream.com/learn/comprehensive-guide-to-regulatory-compliance.htm#:~:text=Regulatory%20compliance%20focuses%20on%20aligning,at%20streamlining%20internal%20business%20requirements. on 13 September 2024.

3. European Commission, ‘Standard Contractual Clauses’ Official website of the European union, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en on 12 September 2024.
4. Office of the data protection commissioner, ‘Guidance notes on consent’ Kenya data protection regulator’s website, https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Notes-on-Consent.pdf on 4 November 2024.
5. Van der Laan, ‘Data protection laws and regulations Netherlands 2024-2025’ ICLG news, 31 July 2024 https://iclg.com/practice-areas/data-protection-laws-and-regulations/netherlands#:~:text=Therefore%2C%20the%20Dutch%20Government%20passed,could%20add%20to%20or%20vary. On 7 January 2025.
6. ‘Documents’ Autoriteit persoonsgegevens https://www.autoriteitpersoonsgegevens.nl/en/documents on 16 January 2025.
7. ‘Tasks and powers of the Dutch DPA’ Autoriteit persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/about-the-dutch-dpa/tasks-and-powers-of-the-dutch-dpa#:~:text=The%20Dutch%20Data%20Protection%20Authority,the%20use%20of%20personal%20data on 24 January 2025.