ANALYSING THE CHALLENGES IN ENFORCEMENT OF DATA PROTECTION LAWS IN UGANDA

DAPHINE KAYEKI

CKS21B11/039

A DISSERTATION SUBMITTED TO THE SCHOOL OF LAW IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS OF UGANDA CHRISTIAN UNIVERSITY

May,2025

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLARATION OF AUTHORSHIP

I Kayeki Daphine, do hereby declare that this dissertation titled "Analyzing the challenges in the enforcement of Data Protection Laws in Uganda" is my original work and has not been submitted for any other degree or qualification. All sources of information used have been acknowledged appropriately.

Dated this.....22.....day of.....MAY.....2025

.....

sign

ii

APPROVAL

The undersigned hereunder certifies that the supervisor has read and recommends for acceptance by the university a dissertation titled:

Analyzing the challenges in enforcement of data protection laws in Uganda for the partial fulfillment of requirements for the award of the degree of Bachelor of Laws(LLB).

Supervisor: Miss. ANN NAMUKASA

Signature..... **Date**.22/05/2025...

iii

ABSTRACT

ANALYSING THE CHALLENGES IN ENFORCEMENT OF DATA PROTECTION LAWS IN UGANDA.

The Data protection and Privacy 2019 was enacted to regulate the collection, Processing and storing of personal data and to also provide rights to data subjects. This study defines different key terms that will be used within the dissertation such as data, personal data, data protection among others. Despite of the enforcement of data protection laws in Uganda there has been significant challenges like lack of sufficient funding to effectively monitor and enforce compliance, limited access to advanced digital tools for investigating data break, noncompliance with the laws among others. This study explores the key obstacles hindering effective enforcement including legal and regulatory gaps, institutional weakness, limited public awareness, and technological challenges. It examines the role of regulatory bodies such as the National Information Technology Authority -Uganda (NITA-U) and assesses their capacity to enforcement compliance and the role of the Data Protection officer (DPO) in enforcement of the DPPA. This study also assesses other supportive laws and regulations like the computer misuse Act 2011, Access to information Act 2005 and Electronic Transactions Act 2011 among others. Additionally, the study analyses case studies and draws comparisons with other jurisdictions such as the EU General Data Protection Regulations (GDPR) to highlight best practices that Uganda can adopt to strengthen data protection enforcement like adoption of regulations and possibly amending some areas of the law, Data protector or processor reporting compliance with the law. The findings reveal that inadequate resources, lack of technical expertise and weak enforcement mechanisms contribute to poor data protection. The study recommends

strengthening legal framework, enhancing institutional capacity, increasing public awareness and investing in digital infrastructure to improve enforcement. Therefore, by addressing these challenges, Uganda can ensure better compliance with data protection regulations, thereby safeguarding personal data in an increasingly digital economy

DEDICATION

I solely dedicate this dissertation to my dear Dad Mr. Khawanga Tom Robert and lovely mother Mrs. Esther Khawanga, and my lovely brothers Pius and Edwin whose commitment, support and love have been my greatest source of strength throughout this academic journey. This work is a reflection of your faith in me and I hereby share this achievement with you.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank the Almighty God for granting me the strength, wisdom, good health and perseverance to complete this dissertation effectively.

Thanks with most generosity goes to my parents my father and mother, and my brothers who have been supporting me financially and all the encouragement through my studies may God grant you countless blessings. I also want to take a moment to sincerely thank myself for the resilience, discipline, and determination I have shown through this journey. For every late night, every difficult decision, and every step forward, I am proud of the commitment and growth I have achieved.

A word of appreciation is to be noted to the Faculty and staff of the School of Law whose academic support, conducive academic environment and necessary resources have made this journey enriching.

I also thank all my course mates and friends for the encouragement, support and the care they offered to me through this course may God bless you abundantly.

Last but not least, I wish to acknowledge my supervisor Ms. Ann Namukasa for her invaluable guidance, constructive feedback and unwavering support which have been so instrumental throughout this research journey. I appreciate you Counsel.

TABLE OF CONTENTS

LIST OF ACCRONYMS

NITA-U-National Information Technology Authority-Uganda

EU- European Union

AUCCSPDP- African Union Convention on Cyber Security and Personal Data Protection

DPPA- Data protection and privacy Act

DPA- Data Protection Act

DPO- Data protection office

GDPR- General Data Protection Regulation

DPA- Data Protection Authority

UNCITRAL- United Nations Commission on International Trade Law

NDPR- Nigerian Data Protection Regulation

UCC- Uganda Communications Communication

URA- Uganda Revenue Authority

NSSF- National Social Security Fund

NIRA- National Identification and Registration Authority

OECD- Organization for Economic Cooperation and Development

APEC- Asian-Pacific Economic Cooperation

EDPB- European Data Protection Board

CBPR- Cross Boarder Privacy Rules

UNESCO-United Nations Educational, Scientific and Cultural Organization

UNHCHR- United Nations Higher Commission of Human Rights

ODPC- Office of Data Protection Commissioner

RECs- Regional Economic Communities

PDPO- Personal Data Protection Office

POPIA- Protection of Personal Information Act

DPIAs- Data Protection Impact Assessments

CHAPTER ONE

1.0 Introduction

Due to increasing digital transformation, personal data was frequently shared and utilized every day often without consent of the data subject hence leading to increasing risks associated with data breaches, cybercrime, and unauthorized access to personal information. Personal data protection became a critical issue worldwide as many countries have enacted laws to regulate data protection, processing and storage to safe guard individual privacy.

Globally, data protection frameworks evolved to address these challenges. The General Data Protection Regulation (GDPR) in the European Union became widely recognized as one of the most comprehensive data privacy frameworks globally.[1] It set a global standard, influencing many countries to establish similar laws.

The 2014 adoption of the African Union Convention on Cyber Security and Personal Information accelerated efforts to secure personal information in Africa by urging member nations to enact national data protection legislation.

Uganda in response to this development it enacted the Data Protection Act 2019 to regulate the management and handling of personal information and ensuring privacy rights.[2] The act aimed to establishment of a legal framework for responsible handling of personal data while balancing the interests of individuals, businesses, and the government. Despite its introduction, the law faced significant challenges in

[1] https://gdpr.eu/tag/gdpr

[2] Pdpo uganda,2022

enforcement, raising concerns about its effectiveness in ensuring privacy rights and securing sensitive information.

Therefore, this research critically analyzed the challenges in enforcement of data protection laws in Uganda, exploring the gaps, weaknesses, and limitations that hinder the full realization of privacy rights and some of the challenges include identity theft, surveillance abuses, law public awareness, inadequate technological infrastructure, unauthorized data access among others hence hindering compliance and how these challenges can be solved. By analyzing existing legal frameworks, regulatory mechanisms, and enforcement practices, the study aimed to highlight areas that required improvement to enhance data security and compliance with privacy laws in Uganda.

1.1 BACKGROUND OF THE STUDY

The concept of data protection dated way back in 1890 when U.S lawyers Samuel Warren and Louis Brande authored The Right to privacy Article. The Article introduced the idea that individuals should have the right to be left alone meaning that individuals should have legal protection against unwarranted intrusion into their private lives.

A significant advancement in data protection occurred with the introduction of Data Protection Convention Treaty in Europe, which legally recognized the right to privacy for European nations. More recently, the implementation of General Data Protection Regulations (GDPR) in Europe has marked one of the most prominent developments in data protection laws.

In Africa, the African Union took a major step towards safeguarding personal data and privacy in 2014 by introducing the African Convention on Cyber Security and

Personal Data protection. Many Nations have since enacted their national data protection laws.

Uganda was among the African countries that passed the data protection legislation for example the Data protection and Privacy Act 2019. It was introduced to uphold the right to Privacy as provided for under Article 273 which states that no person shall be subjected to interference with the Privacy of that person's home ,correspondence ,communication or other property. However, the law has faced certain challenges leading to hindrance of compliance.

Prior to this Act, Uganda's legal framework for data protection relied on various sources including the constitution of the Republic of Uganda, common law principles and statutes such as Access to information Act 2005, Uganda Communications Act 2003, Electronic Signatures Act 2011 and Computer Misuse Act 2011 among others. Despite of the introduction of the Data Protection and Privacy Act, its effectiveness on enforcement remains questionable particularly in developing countries like Uganda with issues such as weak regulatory framework, lack of awareness hindering effective implementation. In Uganda we have seen different cases that rise more concerns about data protection laws for example in the case of Mukasa peter versus MTN (2021) where the plaintiff sued MTN for unlawfully sharing of his personal data with the third parties without consent, highlighting the difficulties in holding corporation accountable for data breaches hence there's need for a strong enforcement mechanisms and judicial clarity in data protection laws.

Therefore, as the digital economy expounds, strengthening data protection mechanisms is essential to ensure Privacy, security and trust in the digital space.

[3] Constitution of the Republic of Uganda

1.2 STATEMENT OF THE PROBLEM.

While the Data Protection and Privacy Act 2019(DPPA) was enacted to protect personal information, enforcement remained weak revealing substantial legal gaps The central legal problem lied in the inadequate enforcement mechanisms within the Act for example the limited scope of regulatory powers, absence of specific provisions addressing modern data protection challenges, enforcement penalties for non-compliance. Therefore, this study critically examined the challenges hindering data protection laws in Uganda and explored viable solutions to strengthen data governance and safeguard personal information

1.3 SIGNIFICANCE OF THE STUDY.

This study provided insight into the weaknesses of Uganda's Data Protection enforcement landscape.

The study findings benefited regulatory institutions such as the Regulatory National Data protection officer and data collectors in enforcement of the laws.

This study provided practical recommendations to policy makers, regulatory bodies and legal practitioners.

This research contributed to academic literature in the field of law and served as a reference for legal practitioners and researchers interested in data protection issues.

1.4 JUSTIFICATION OF THE STUDY.

The study showed that although Uganda enacted the act, the law has weak enforcement and implementation mechanisms and that there is need to adopt more comprehensive measures to enforce the Act. The study helped to bridge the gap between law and practice, particularly in addressing technological, institutional and legal constraints.

1.5. OBJECTIVES OF THE STUDY.

1.5.1 General Objective

To examine the key challenges in enforcement of data protection laws of Uganda.

1.5.2 Specific Objectives.

To examine the legal and institutional framework governing data protection in Uganda.

To explore best practices from other jurisdictions that could enhance the enforcement of data protection laws in Uganda.

What are the key challenges in enforcement of data protection laws in Uganda?

To recommend policy, legal and institutional reform that could strengthen data protection enforcement in Uganda.

1.6RESEARCH QUESTIONS.

1.What is the legal and institutional frame work governing data protection in Uganda?

2.What are the key challenges in enforcement of data protection laws in Uganda?

3.What lessons can Uganda learn from other jurisdictions to improve data protection enforcement?

4.What policy, legal and institutional reforms can enhance data protection enforcement in Uganda?

1.7SCOPE OF THE STUDY.

1.7.1Content scope.

The study focused on the current data protection laws of Uganda it's provisions and contents and other laws on data protection both international and regional.

1.7.2Time scope.

This study focused on exploring the challenges in enforcement of data protection law from the time of its promulgation (2019) to the present and future legal aspects of enforcement.

7.3Geographical scope.

This study focused on Uganda, specifically analyzing the enforcement of data protection laws within the country. It analyzed the challenges faced in enforcement of data protection laws within Uganda. It examined the role of key institutions such as National Information Technology Authority-Uganda (NITA- U) Personal Data Protection Office (PDPO) and other relevant regulatory bodies in enforcing data protection laws.

1.8 LITERATURE REVIEW.

There existed a limited scholarly literature on the enforcement of data protection laws in Uganda. However, various studies have examined data protection Challenges in Africa and globally. Scholars such as Alex Boniface43 have conducted surveys on data protection laws in Africa, emphasizing the need for increased research training and modern legal frameworks dedicated to privacy and data security. Despite the gaps in literature specific to Uganda, existing research provided insights into enforcement challenges legal frame works and institutional capacities related to data protection.

Researchers like Colette Cuijpers, De Heart 5 distinguish between data Privacy and data protection. According to Cuijpers, the right to Privacy ensures an individual's undisturbed private life and protection laws focus on regulating how personal data is collected stored and used. De Heart further argue that the primary goal of data protection is to safeguard individuals against un authorized access, misuse and exploitation on their personal data.

[4] Alex Boniface, Privacy and Data Protection in Africa: a State of the art International Privacy Law2012, volume

[5] Colette Cuijpers, A Private Law Approach to Privacy: mandatory Law Obliged?

The European Union's General Data Protection Regulation (GDPR) is one of the most influential legal instruments in data protection.it establishes strict guidelines on consent, Data subject rights and enforcement mechanisms including penalties for non-compliance. Many African countries including Uganda, have drawn inspiration from the GDPR when drafting their data protection laws.

The African Union on 2014 it adopted the convention on cyber security and personal Data protection, encouraging African states to recognize the importance of safeguarding personal data while balancing free data flow from economic and technological development. At least 20 African countries have used the framework as a guideline for enacting national legislation.

Uganda enacted the Data protection and privacy Act 2019 which regulates the collection processing and storage of personal data granting individuals over control of their personal information, mandating enforcement by regulatory bodies despite these provisions enforcement remains weak due to institutional challenge, lack of awareness, limited compliance. Research by Dorothy Mukasa of Unwanted witness emphasizes the lack of awareness about data protection rights in Uganda. Many individuals and organizations do not fully understand their legal responsibilities leading to law compliance levels and that without the data protection laws it becomes so tricky on how organizations are going to be protected6.

In Africa, Kenya also enacted the Data Protection Act 2019 which established the office of the Data Protection Commissioner (OPDC) to oversee compliance. The ODPC

[6] Scarcity of data protection laws in Africa leaves NGOs exposed by Andrew Green/ 27th June 2018 [7] Schermer BW,Custers B, Van der Hof S(2014) The crisis of content: how stronger legal protection may lead to weaker consent in data protection

has actively enforced regulations by investigating breaches and imposing penalties, providing a model for Uganda to consider (Mwendwa 2021).

Schemer Custers and Van der Hof7 argue that while stronger legal protections are essential for data protection, they may inadvertently weaken the process of obtaining meaningful consent. Securing consent for data processing presents ethical legal and practical challenges. Other scholars like Bryant, Kaliisa and more others also addressed the data protection laws and their enforcement emphasizing the importance of supervisory authorities and accountability mechanisms within Africa.

Therefore, Uganda can adopt the best practices from other countries like Kenya, European countries to build a more robust data and protection framework through strengthening of regulatory institutions and enhancing compliance mechanisms among others.

1.9. METHODOLOGY

This research focused on doctrinal research methodology to analyze the challenges of enforcement. Doctrinal research involved analysis of statutes, case law, regulations and legal texts.

1.9.1 Research design

The study was qualitative and descriptive in nature as it sought to examine legal framework surrounding data protection laws in Uganda and to evaluate the effectiveness of their enforcement.

1.9.2 Sources of data

The study relied on primary and secondary legal sources to identify legal gaps and challenges for example statutes and legislation, case law, academic articles, books, reports and comparative jurisprudence.

1.9.3 Data analysis

The data analysis involved textual interpretation, doctrinal comparison and critical evaluation of the study.

1.10 LIMITATION OF THE STUDY

This research adopted a doctrinal legal research methodology, focusing on the analysis of statutes, case law to evaluate the challenges. Since doctrinal research relied on legal texts rather than practical observations, the study did not fully reflect how institutions implement the law in practice.

Given that Uganda's data protection law is relatively new, there may be limited judicial precedent or case law in interpreting key provisions.

While comparative analysis with jurisdictions for example GDPR, the distinct legal and institutional contexts may limit the applicability of these models in Uganda's setting.

Data protection is a rapidly evolving field, ongoing legislative amendments, policy changes or judicial decisions occurring after the study period may affect the continued relevance of the findings.

CONCLUSION

The preceding chapter provided a comprehensive analysis of findings derived from secondary data sources and comparative insights from other jurisdictions. From this review it became evident that Uganda's data protection landscape is still evolving with several notable challenges undermining effective enforcement. These findings set the stage for a deeper exploration into the doctrinal and practical aspects of enforcement in Uganda's context, which will be addressed in the subsequent chapters.

CHAPTER SYNOPSIS

Chapter two; summary of the provisions of Data Protection Act

The chapter consists of a summary of the provisions of data protection and privacy Act of Uganda 2019 and the non-legal aspects.

Chapter three; critical analysis of the Act

It consists of critical analysis of the data protection laws of Uganda so as to identify the loopholes and challenges within the law.

Chapter four; comparative analysis

The chapter consists of a comparative analysis between the data protection laws within Uganda with other national laws on data protection.

Chapter five; findings, recommendations and conclusions

This study focuses on providing a summary for findings and conclusions deducted from the research. It also consists of the necessary recommendations for solving of issues in the in the law.

CHAPTER TWO

SUMMARY OF THE PROVISIONS OF THE DATA PROTECTION AND PRIVACY ACT 2019 AND NON-LEGAL ASPECTS.

Introduction

This chapter provides a summary of the key provisions of the Data Protection and Privacy Act, 2019, outlining its main objectives, rights, and obligations. It also discusses the non-legal aspects that affect the enforcement and implementation of the Act in Uganda. By summarizing both legal and non-legal aspects, the chapter provides a comprehensive understanding of the challenges and opportunities surrounding data protection in Uganda.

2.2 summary of provisions of the Data Protection and Privacy Act, 2019.

The Data Protection and Privacy Act, 2019 aims to regulate the collection, processing, storage, and dissemination of personal data in Uganda and abroad if it relates to Ugandan citizens. It establishes the rights of data subjects whose data is being collected including the right to access their data, and obligations of data processors and controllers, collectors including to regulate the use and disclosure of personal information and it also establishes enforcement mechanisms and penalties. The Act aims to ensure that the individuals whose information has been collected, processed and requested to have powers to exercise the control over their personal data including consent to collect and process data.

The Data Protection and Privacy Act covers public and private organizations handling personal data both inside Uganda and outside Uganda for those managing data pertaining to Ugandan individuals.

The act also defines key divisions for example personal data to mean any information about a person from which a person can be identified for example age, nationality, identification numbers among others[7] so therefore data processors and collectors have the obligation to protect such data. The Act also defines a data collector to mean a person who collects personal data[8]. Data controller to mean a person who, alone, jointly with other persons who determine the purpose for and the manner in which data is processed or to be processed.[9] A data subject means an individual from who or in respect of whom personal data has been requested, collected, collated and processed.[10] A data processor to mean a person who processes data on behalf of the data controller and is not an employee of the data controller.[11] The law obliges these entities to ensure transparency, security and accountability in handling data. Data must be collected for specific, lawful purposes and stored securely to prevent unauthorized access or breaches as addressed in the case of Lloyd v Google where they addressed the claim on data breaches.

The Act also provides for the principles in which the data controller and data collector should collect personal data including the requirement that personal data must be collected fairly and lawfully, collected for specific legitimate purposes, accurate and kept up to date and that they should be accountable to the data subjects for the data collected, processed and stored.

[7] Section 2 of DPPA
[8] ibid
[9] ibid
[10] ibid
[11] ibid

2.2.1 Other related laws on data protection in Uganda.

In addition to the Data Protection and Privacy Act, 2019, Uganda has enacted other several laws, policies, statutes, and regulations that touch on aspects of data protection although they do not specifically focus on it. These laws complement and interact with the main Act. The more relevant ones are briefly discussed below.

The Constitution of the Republic of Uganda, 1995 (as amended). It guarantees the right to privacy of a person, home, and correspondence. 12 This constitutional provision forms the foundation for data protection rights in Uganda.

The Computer Misuse Act, 2011. it criminalizes unauthorized access and modification of computer system and computer material.1314 These provisions are essential in protecting the integrity, confidentiality, and availability of data in Uganda's digital environment.

The Electronic Signatures Act, 2011. It regulates the use electronic signatures. It includes the provisions for securing electronic records, books, registers and correspondence.15

The Anti-Pornography Act, 2014. It provides for prevention of misuse of persona; data for the publication or dissemination of pornographic content especially online.

[12] Article 27

[13] Section 4 and 7 of computer misuse Act, 2011

[14] Section 80

[15] Section 4

The Uganda communications Act, 2013. It outlines the various functions of Uganda communications commission to monitor, inspect , license, supervise and enforce compliance relating to communication services.15

National Information Technology Authority-Uganda(NITA-U). it is designated as the national data protection authority and it also maintains the register that lists every institution, person or public body collecting or processing personal data.

Conclusion;

The findings of this study on the legal basis for is that Uganda has established a foundational legal framework for data protection, anchored by the Data Protection and Privacy Act, 2019, which reflects key international principles such as lawfulness, consent, transparency, and accountability. Complementary legislation-including the Constitution, Computer Misuse Act, 2011, Electronic Signatures Act, 2011 and NITAU further reinforces the protection of personal data, particularly in digital environments. These laws collectively provide a baseline for safeguarding individuals' privacy rights in an increasingly digitized society. However, despite this legal architecture, effective enforcement, institutional capacity, and public awareness remain significant challenges, as will be critically examined in the subsequent chapters.

However, it has also got the non-legal aspects as discussed in the next section.

2.3 NON- LEGAL ASPECTS UNDER THE DATA PROTECTION AND PRIVACY ACT, 2019 OF UGANDA.

2.3 Introduction

Beyond the statutory framework, achieving effective data protection also involves non-legal aspects including creating acceptability, raising awareness and fostering a culture of data privacy through Education and organizational policy among customers about whether and how their data is being used and collected. These organizations are expected to establish clear corporate privacy, avoid practices that could compromise individual's privacy rights. The other non-legal aspects on data protection come from technological innovations and advancement. Implementing secure IT infrastructure, using encryption, and adopting data minimization strategies are essential. Additionally, simplifying the legal language and translating data protection concepts into local contexts enhances public understanding and compliance. While the DPPA provides a foundational legal structure, it also addresses the non-legal aspects basing on ethical considerations and practical implementations as explained.

2.4 ETHICAL CONSIDERATIONS.

The Act emphasizes the ethical implications like fairness, consent, accuracy, transparency, accountability, participation and legitimacy in collecting and handling of data.16 It is important for the organizations , businesses and institutions dealing with data in Uganda to learn to communicate a culture of trust with the data subjects. So instead of seeking compliance with laws and regulations, institutions and organizations should ethically consider doing the right thing during the handling and collection of data.

[16] Section 3 of Data Protection and Privacy Act, 2019

2.4.1. Transparency and accountability;

Organizations are required to be transparent about how they collect, process, and use personal their rights and obligations. The Act also emphasizes the duty of data collectors, controllers and processors to be accountable to the data subjects for the data they collect.17

Transparency includes providing information about the purpose of data collection. The period of retention, and the rights of the data subject before or shortly after data collection.

2.4.2 Fairness and non-discrimination. When collecting data, data processors and collectors must refrain from prejudice or discriminatory actions18. while section 3 of the DPPA provides for fair use of personal data, actual enforcement depends on whether the organizations uphold fairness as an ethical value. This is particularly important in areas of automated decision making, where algorithms may inadvertently reflect social biases.

2.4.3 Respect for individual privacy. The DPPA is founded on the recognition of privacy as a fundamental right. Beyond legal obligations, organizations have an ethical duty to respect the personal boundaries and data autonomy of individuals. This includes refraining from intrusive surveillance and ensuring consent is obtained in a genuine and informed manner. In contexts where digital literacy is low, such

[17] Section 3 of Data protection and Privacy Act, 2019

[18] https://www.promptcloud.com/blog/importance-of-ethical-data-collection/ [19] https://chapterfouruganda.org

respect demands extra diligence in simplifying consent processes and ensuring data subjects understand what they are consenting to.

2.4.4 Data subject rights.

People are entitled to know what information is kept about them, to access that information, to have inaccurate information corrected, and to have their data processed no further. These rights empower individuals to have control over their personal data and ensure that it is used responsibly.

2.5 PRACTICAL IMPLEMENTATION

2.5.1 Data Security;

The Act emphasizes the importance of securing personal data to prevent breaches and unauthorized access, including the use of strong passwords for digital data and secure storage for hard copy information.19 Data breaches should be immediately reported to the National Information Technology Authority and the authority determines whether the data subject should be notified.19 The Act also requires data controllers to destroy or delete personal data at the end of the retention period in a way that prevents reconstruction.[20]

Organizations data collectors and institutions are also encouraged to adapt these security measures for example physical security like Implementing measures to protect physical devices and data storage from unauthorized access, damage or loss.

[19] https://cipesa.org accessed 30th April 2025
[20] Data Protection and Privacy Act

Technical security like using encryption, access controls, firewalls and other security measures to protect data from cyber threats.

Maintaining regular data backups and having a strategy in place to restore data in the event of loss or damage.

And educating employees and other stakeholders about data security threats and best practices.

2.5.2 Public awareness and education;

Many people are not aware of the dangers of data misuse or their rights under the DPPA. Non legal efforts such as public education campaigns, workshops, and media outreach are vital for; informing the public about their rights as data subjects, encouraging consent- based data practices and lowering cases of voluntary data exposure without considering implications.

2.5.3 Corporate privacy policies and self – Regulation.

Beyond statutory obligations, companies should develop internal policies tailored to their data handling processes. These include; privacy notices and consent forms, data retention and deletion protocols and guidelines for third party data sharing.

2.5.4 Impact on specific sectors;

The Act has a significant impact on NGOs, requiring them to adhere to data protection principles, ensure data quality, and maintain transparency and security.21

[21] https://chapterfouruganda.org

The Act also affects the health sector, emphasizing the need for secure and protection of sensitive medical information.22

The Act's provisions related to data retention and deletion apply to all sectors, including government agencies and private entities.23

2.5.5 Appointment of Data Protection Officer (DPOs)

While the Act does not mandate every organization to appoint a DPO, having a dedicated professional for overseeing data protection is a best practice. DPOs play a central role in advising on data processing activities, monitoring compliance, and liaising with the Personal Data Protection Office (PDPO). The appointment of the DPOs is thus voluntary but effective non legal strategy for internal accountability.

2.5.6 capacity building and staff training

The DPPA acknowledges the role of institutional capacity in data protection but does not impose legal requirements for staff training. Nonetheless, regular training and awareness sessions are critical for embedding data protection principles in organization culture. They ensure that all staff members understand their roles in protecting personal data.

2.5.7 Conclusion

The non-legal aspects of the Data Protection and Privacy Act 2019 focus on the practical implementation of the Act, emphasizing the need for data security,

[22] https//www.pdpo.go.ug

[23] Data Protection and Privacy Act

transparency, accountability, and ethical data practices across various sectors in Uganda.

The findings of this study on the legal basis for Data protection law in Uganda has the proof that Uganda has a legal framework for Data protection and thus the other related laws such as the Computer Misuse Act among others and also the non-legal aspects.

CHAPTER THREE

CRITICAL ANALYSIS OF DATA PROTECTION AND PRIVACY ACT, 2019 IDENTIFYING THE LOOPHOLES OR CHALLEGES WITHIN THE LAW.

Introduction

The Data Protection and Privacy Act, 2019 was enacted to protect the privacy of individuals and regulate the collection and processing of personal data in Uganda. While the DPPA provides in proposition the main data protection principles, it has major gaps in terms of clearly articulating the obligation of data collectors, controllers and processors as well as robust responsibility mechanisms that make enforcement of the law and thus the protection of the right to privacy difficult.[24] Below are some of the loopholes or gaps within the law.

Ambiguity in definitions

The DPPA contains vague definitions for fundamental terms such as consent, personal data and sensitive personal data. For instance, the Act defines consent as any freely given, specific, informed and unambiguous indication of the data subjects' wishes, but it provides no practical criteria for determining what constitutes freely given or informed consent.

Therefore, lack of precision allows data controllers to interpret terms loosely, potentially compromising individuals' privacy.

[24] https://www.unwantedwitness.org

consent

There is lack of specific provision to withdraw consent by the data subject meaning when consent is granted it will be limited for them to withdraw and it will be on the discretion of the data controller and processor to withdraw. Therefore, this should be looked at in the Act. In providing for consent act should also provide for the right to withdraw consent.

The provision on consent should also include the requirement to inform the data subjects to be informed about how their data will be used under the Act. However, Uganda's Data protection and Privacy Act falls short by not comprehensively detailing the scope of safeguards required when handling sensitive personal data. In contrast to other countries, EU's GDPR sets a clear benchmark by mandating robust security safeguards to protect against unauthorized access, loss, and destruction. This gap in Uganda's law raises concerns about whether data collectors are sufficiently obligated to implement appropriate technical and organizational measures.

One obvious area of concern is the cross-border transfer of personal information. Section 1925only requires a data processor to ensure that the country where this data is being held has adequate data protection measures in place. This provision should also require stringent protection or binding corporate rules. There's a pressing need for Uganda's parliament to revise the Act to ensure that cross-border transfers do not compromise personal data while maintaining a balance with the interests of international trade. Additionally, section 10 of the Act is unclear on what exactly

[25] DPPA

constitutes as a violation on the rights of the data subjects. For effective enforcement, the law must explicitly define the actions that amount to rights violation. Without such specificity, enforcement agencies and courts may struggle to apply the law consistently, thereby weakening data protection mechanisms.

Analysis of data security provisions

The Act addresses data security for example it talks about security of person data where it obliges a collector or processor to secure the integrity and confidentiality of personal data in their possession or under their control specifically it requires them to take appropriate measures to prevent loss, damage and unauthorized destruction of personal data and unlawful access.[26] Furthermore it also addresses the issues of notification of data security breach. This section requires that where there's a data security breach, data collector, controller, processor shall immediately notify the authority that's the Personal Data Protection Office.[27] However despite of these provisions critical gaps remain in the law. The section 20 of the Act does not provide for the notification of the data subjects in case of breach of their personal data. A person has a right to be notified in case of any breach because it amounts to violation of the person's privacy. Therefore, a more robust legal requirement, including a mandatory notification timeframe for notifying the data subjects in case of breach.

Assessment of Data subjects' rights

[26] Section 20 of the DPPA

[27] Section 23 of the DPPA

Sections 24 to 2828 provides for the rights of data subjects to include, access to personal data, the right to erasure data, a right to prevent processing of data among others. However, these rights are not supported by sufficient procedural clarity or enforcement mechanisms. The law must go further to specify how these rights are not supported by sufficient procedural clarity or enforcement mechanisms. The law must go further to specify how these rights can be exercised, especially in cases involving automated decision-making, where individuals are most vulnerable to opaque data practices.

However, a critical review reveals that while the law recognizes these rights, it lacks the procedural clarity and robustness seen in global Data Protection Regulation (GDPR). One key concern lies in the automated decision making, which involves decisions made without human involvement. This is particularly sensitive when such decisions use social categories of data, such as health or religious beliefs, or when they affect individual's legal status or entitlements.

Uganda's approach lacks enforceable limitations on profiling a form of automated processing that analyses personal characteristics to predict behavior or preferences. Without clear safe guards, this creates a high risk for abuse, such as invasive targeting in advertising or discrimination in service delivery.

Section 24(1)(b) 29 which grants access to a description of personal data, also requires strengthening. It should be expanded to require access to detailed information about the purpose of data collection and how it is being used by the data controller.

[28] Data Protection and Privacy Act 2019

[29] ibid

This would enhance transparency and empower data subjects to make informed opinions about their data.

Section 2530 which provides for the right to prevent processing, should be improved to include minimum requirements, such as the absolute right to withdraw consent any time, without the burden of proving harm. Currently, the law appears to favor data controllers by making it the responsibility of the data subject to initiate objections in writing—an undue procedural burden

The right to be forgotten.

This right, partially addressed under section 1631 mandates that data controllers, processors erase personal data when it becomes irrelevant, outdated, or unlawfully obtained. However, the provisions vaguely drafted and lacks a clearly defined process. Importantly, it does not establish a direct, enforceable obligation for data controllers to assess whether stored data remains relevant. The burden again appears to rest on the data subject to initiate the process.

Furthermore, there is no direct linkage to automated systems or profiling outcomes that may store persistence data on individuals. A more progressive interpretation would require controllers to only delete data upon request but also implement internal mechanisms for routinely assessing the necessity of retaining personal data.

Uncertainty over the law's retroactive application.

[30] DPPA

[31] DPPA

Transitional provisions that would address data currently kept by individuals' government agencies and others are absent from the DPPA. Since the data was held prior to the law's implementation and the regulation does not apply retroactively, it is unclear how that data will be handled or processed.[32]

In relation to the above, the DPPA does not have provisions for consolidating data especially data held by government agencies to ensure it is safe and secure. At present every government agency and private actor collects data according to their wishes. Such data should be held in a central place to ensure easy management. Entities like UCC, URA, NIRA, NSSF, all hold important private data and this puts such data at risk of abuse.

The law does not provide for areas where data is collected without consent mainly by individual actors such as CCTV on private properties, camera drones among others. This ca be used to violate the right to privacy of individuals.[33]

Failure to provide power for the Authority to impose penalties

The law lacks a general provision for offences which would cater for provisions that do not have penalties. This is the case despite the fact that majority of the provisions do not create offences. It will be difficult for the Authority and individuals to enforce some provisions of the law since violating them does not rise to any administrative, civil or criminal sanction.

Limited scope of application.

[32] https://www.unwantedwitness.org

[33] https://www.unwantedwitness.org

The DPPA primarily applies to data processors and controllers within Uganda. It does not sufficiently address the issue of extraterritorial application for example foreign companies processing personal data of Ugandans remotely also it does not explicitly regulate goods and services or monitor from abroad. The inadequate provisions for cross-border data protection reduce the law's relevance in an increasingly digital and global data ecosystem.

Lack of capacity, public awareness and education.

There's low public awareness and education about the data protection rights and responsibilities. Many organizations also lack the capacity to implement data protection principle effectively. Therefore there should be public campaigns to educate individuals and organizations about the rights and responsibilities to ensure that they are aware of them to promote the practical effectiveness of the law.34

Weak enforcement mechanism;

The Act's enforcement mechanism may be insufficient to deter violations and ensure compliance, especially for large organizations or those operating across borders. Stronger enforcement measures and greater collaboration between regulatory bodies and data protection authorities are needed to address this issue. 35 For example, the enforcement body like NITA-U lacks the independence, technical capacity and financial autonomy typically seen in effective data protection authorities globally. This hinders accountability.

[34] Privacy international, uganda's Data Protection Privacy Act, 2019: Analysis and recommendations httsp://privacyinternational.org accessed 30th April 2025

[35] Privacy international, uganda;s DPPA, 2019; analysis and recommendations httsp://privacyinternational.org accessed on 30th April 2025

Absence of comprehensive sector regulations;

The law is general in nature and lacks sector-specific guidelines for areas like health, education, finance, and telecommunications, where personal data is frequently processed. The absence of detailed regulations results in inconsistent data protection practices across sectors.

Weak penalties and remedies;

The sanctions under the Act are relatively mild and may not deter serious violations. Additionally, the complaints and redress mechanisms are underdeveloped, discouraging individuals from seeking justice. Weak penalties and lack of effective remedies limit compliance incentives.

Data breaches are also a significant concern.

The act needs to address the risks of unauthorized access and misuse of personal data. IBM's data breach report shows the global average cost of a data breach in 2024 is around $4.88 million.

This is 10% higher than in 2023. On average, it amounts $5 million for the technical sector and more than $6 million for the healthcare sector per breach.36

Data breaches are among the most pressing data privacy challenges, primarily driven by phishing and credential theft. This threats often manifest as emails containing malicious links, the use of social engineering tactics, or vulnerabilities within the system. Security awareness training and use of security breach controls like firewalls and anti-software should be implemented to solve this. In the case of Lloyd v Google

[36] https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry.

is the UK case the addressed the claim on data breaches. In this case, the respondent issued a claim alleging the appellant google has breached its duties as a data controller under section 13 of DPA to over 4m Apple users during the period of 201112 when google was able to collect and use their browser information. Google opposed the application on grounds that the basis of claiming compensation under the DPA. Damages were not awarded because the claimant did not show he suffered distress as a result of the respondent's wrongful use of data.37

Conclusion;

The Data Protection and Privacy Act, 2019 is a significant legislative development in Uganda's digital governance framework. However, critical legal and practical challenges including vague definitions, weak enforcement mechanisms, and inadequate protection of data subject rights limit its effectiveness. Addressing these challenges through legal reform, institutional strengthening, public education, and the development of sector-specific regulations is vital to enhancing the law's impact.

[37] Lloyd v Google UKSC/2019/0213

CHAPTER FOUR

COMPARATIVE ANALYSI OF THE DATA PROTECTION LAWS WITH OTHER JUSRIDICTIONS.

4.0Introduction.

This chapter examines the legal framework of the Data Protection and Privacy Act against selected international and region data protection laws. The aim is to evaluate and asses Uganda's legal position in light of best practices and identify areas where enforcement can be strengthened.

This chapter will also asses the provisions of similar laws in other jurisdictions for example, Kenya with the view of picking best practices and legal provisions that might defer from our national legal framework with a view of improving enforcement and regulation in the region.

4.1 International legal frameworks.

The foundation of international data protection lies within broader Human Rights Instruments. The Universal Declaration of Human Rights (1948) under Article 12 and the international Covenant on Civil and Political Rights under Article 17, both affirm the right to privacy and the protection of personal life against arbitrary interference. These provisions though not specific to data protection, have been interpreted by the United Nations Human Rights Committee to include digital privacy and data protection, thereby laying the ground works for subsequent legal development in this area.38

[38] General comment 16

The OECD Guidelines on the protection of privacy and trans border flows of personal data (1980, Revised 2013). The organization for Economic Co-operation and Development played a pioneering role in shaping international data protection standards through its privacy guidelines. The OECD guidelines established eight core principles that's collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.39 It also goes ahead under PART ONE and defines data controller, personal data and trans border flows of personal data. Though not legally binding, they have significantly influenced national legislations and regional frameworks. The 2013 revision emphasized risk management, accountability, and cross-border enforcement cooperation, reflecting the complexities of modern data ecosystems.40

The council of Europe-convention 108 was adopted in 1981, also referred to as the council of Europe's Convention for the Protection of individuals with regard to Automatic Processing of Personal Data (convention 108) remains the only legally binding international treaty dedicated to data protection. It requires signatory states to ensure that personal data is collected and processed fairly, stored securely, and not transferred to countries without adequate protection. In 2018, the convention was modernized as convention 108, incorporating stronger safeguards, such as increased data subject rights, and obligations for data controllers and processors.

[39] The OECD guidelines on protection of privacy and Trans border Flows of personal Data (1980)
[40] The OECD guidelines on protection of privacy and Trans border Flows of personal Data (1980) [42] European Convention on Human Rights

It opens nature allows non- European states to become parties, promoting global harmonization. Over other countries have now enacted data protection laws, many of which have been influenced by EU Directive 95/46 EU law also includes the right to data protection at the constitutional level and the European Court of Human Rights has construed Article 8 of the European Convention on Human Rights to include data protection.42

4.2.1 Challenges undermining the effectiveness of international Data protection law

However, the status of the data protection laws at the international level remains uncertain and fragmented despite the existence of several international legal instruments. This uncertainty is driven by a combination of a legal, political, technical and economic factors which include the following.

The most fundamental challenge is the absence of a single, comprehensive, and binding international treaty on data protection. While instruments such as the OECD Guidelines and the APEC Privacy Framework provide normative guidance, they are non-binding and lack enforcement mechanism. Even the Convention 108, the only binding international treaty specially addressing data protection, is primarily European in scope, and its global uptake remains limited (council of Europe, 2018).

Another source of uncertainty lies in the diversity of legal systems and regulatory approaches.

The European Union's GDPR represents a right-based, comprehensive model, emphasizing strong individual rights and extraterritorial application. In contrast, the

United states follows a sectoral and market driven model, with different laws governing specific types of data (like health, finance, children).in Asia and Africa, hybrid approaches are emerging, often influenced by competing models. These discrepancies hinder international harmonization and result in legal conflicts, especially regarding cross-border data transfer.

The rise of digital nationalism and geographical rivalry has further complicated international consensus. Governments increasingly assert control over data within their jurisdictions under the banner of digital sovereignty, sometimes restricting data flows or requiring data localization. Disputes such as the invalidation of the EUUS privacy shield by the court of justice of the European union (schrems II case) illustrate how conflicting legal standards and privacy philosophies can destabilize international arrangements.

Inadequate enforcement and regulatory capacity. In many jurisdictions, particularly in global south, data protection laws have been enacted but remain under-enforced due to limited resources, institutional weaknesses, or lack of political will. This results in inconsistence implementation of international norms and undermines the credibility of cross-border data governance frameworks. Without robust regulatory authorities and technical expertise, international cooperation is difficult to operationalize.

The rapid evolution of digital technologies, including artificial intelligence, machine learning, and the internet of Things, continually challenges existing legal standards. International law struggles to keep peace with the novel ways personal data is

collected, processed and transferred. As a result, many data protection instruments become outdated quickly, leading to uncertainty in their interpretation and application.

Weak international enforcement mechanisms. Unlike other areas of international law, data protection lacks supranational enforcement bodies with universal jurisdiction. Although regional mechanisms like the European Data Protection Board (EDPB) or international cooperation frameworks for example the Global Privacy Assembly promote information sharing, they do not provide binding dispute resolution or enforcement authority. Consequently, compliance relies heavily on the strength of domestic enforcement, limiting the global reach of international norms.

Economic and commercial interests. Multinational cooperation often expert influence on the shaping and enforcement of data protection laws. In some cases, countries may deliberately adopt weaker privacy standards to attract digital investment or support free trade agreements. The prioritization of economic competiveness over individual privacy rights creates regulatory gaps and undermines the universality of data protection principles.

Incomplete Ratification and implementation of international conventions. Several important international instruments, such as the Malabo Convention, suffer from low rates of ratification and implementation. As of 2025, fewer than half of African Union member states have ratified the convention, thereby weakening its potential as a continental standard. Similarly, while convention 108 is open to non-European

states, its global uptake remains limited. This reflects the varying levels of political commitment and institutional readiness among states.

4.2.3 Future developments in International Data Protection Laws.

As digital technologies continue to evolve and data becomes an increasingly valuable asset, the landscape of international data protection law is poised for significant transformation, while the current regime is characterized by fragmentation and legal uncertainty, future deployments indicate a trend toward greater harmonization, institution strengthening among others. Therefore, this section explores the anticipated directions and potential reforms that may shape the future of international data protection law as explained below;

One of the most notable trends is the growing demand for harmonized international standards. As multinational corporations and cross-border data flows become ubiquitous, the need for interoperable privacy regulations is more pressing than ever. Several jurisdictions have begun aligning their national laws with global models such as the GDPR, which has become a de facto international benchmark. Countries in Africa, Latin America, and Asia, are increasingly incorporating GDPR-inspired principles, including lawful processing, data subject rights, and extraterritorial application, into their domestic frameworks.41

Efforts by international organizations, such as the UN, OECD to foster dialogue and consensus on cross-border data protection are likely to intensify. This may result in

[41] Global Data Privacy Laws 2021

codification of global data protection standards--a foundational step toward a binding international agreement in the long term.

Strengthening Regional Frameworks and cooperation. Regional initiatives are also expected to play a pivotal role in the future of data protection. In Africa, the Malabo Convention is likely to gain traction as more countries ratify and implement its provisions. The African Union's Digital Transformation Strategy (2020-2030) emphasizes the need for a continental data governance framework, which could support harmonized enforcement across member states.

Similarly, Asia may see the consolidation of APEC's Cross-Border Privacy Rules system, particularly with the formation of the Global CBPR Forum in 2022 by Australia, Canada, Japan Chinese among others.[42] This platform aims to expand the CBPR model beyond the APEC region, thereby promoting interoperable privacy standards across continents.[43]

Another future development is the anticipated strengthening of international enforcement and oversight mechanisms. The current system relies heavily on national data protection authorities, which often lack the capacity for cross-border collaboration. However, regional bodies such as the European Data Protection Board demonstrate how coordinated enforcement can be achieved. Moving forward, we are likely to witness the establishment of multilateral cooperation networks for enforcement, complaint handling, and dispute resolution.

[42] https://www.globalcbpr.org/about/

[43] African union convention on cyber security and personal data protection

There's also a growing call for an independent international data protection tribunal especially in light of disputes arising from surveillance practices and extraterritorial data access. While such development may face political resistance, it reflects the emerging need for impartial adjudication at the global level.

Integration with Emerging Technologies. The future of international data protection law will also be shaped by technological innovation, particularly in areas such as artificial intelligence, biometrics, quantum computing, and block chain. These technologies challenge traditional notions of consent, data minimization, and transparency. Consequently, new regulatory frameworks will need to address algorithmic accountability, automated decision-making, and privacy-by-design mechanisms.

International bodies such as the OECD, UNESCO, and Global Privacy Assembly are already drafting ethical and legal principles to guide the responsible use of AI and big data. These frameworks may eventually form the basis for technology-specific international data protection instruments, complementing general privacy laws.

Global digital trade negotiations will also influence the evolution of international data protection. Trade agreements increasingly include data governance clauses that seek to balance privacy rights with the free flow of information. The World Trade Organization and various regional trade blocs are likely to push for regulatory interoperability to reduce digital trade barriers while ensuring privacy protection. Simultaneously, debates over data localization— especially in authoritarian and datarich states—may lead to new international norms on the territoriality of data and the limits of state control.

Finally, there's a growing movement to root data protection in fundamental human rights principles. Initiatives by the United Nations High Commissioner for Human Rights (UNHCHR) and civil society organizations advocate for the recognition of privacy and data protection as standalone rights under international law. This trend is likely to intensify, especially as digital surveillance, data exploitation, and misinformation raise urgent ethical concerns. Future international instruments may thus incorporate binding obligations grounded in human dignity, equality, and democratic accountability.

4.3 Regional framework

Europe.

The European Parliament adopted the General Data Protection Regulation (GDPR) on April, 2016 and it became effective on May 25, 2018 replacing an outdated data protection directive from1995. It regulates the processing of personal data of individuals within the EU, regardless of where the data processor is located. The GDPR embodies principles such as lawfulness, fairness, transparency, purpose limitation, and data minimization. The GDPR aims to protect personal data by providing extensive rights to data subjects, including the right to access, rectify, erase, and port their data. 44 Moreover, it imposes strict obligations on data controllers, collectors and processors, backed by significant penalties for noncompliance.45 Its influence has promoted several countries, including Brazil, South Korea and Kenya, to align their domestic laws with its standards.

[44] https://securiti,ai/blog/gdpr-data-mapping

[45] General Data Protection Regulation (EU) 2016

Africa.

The African continent has experienced a significant digital transformation over the past two decades, accompanied by increasing awareness of importance of data protection and privacy. In response, numerous African countries have developed national data protection laws, and continental efforts have been made to establish a coherent regional legal framework. Despite these advances, the legal land scape remains fragmented, within uneven implementation and enforcement across jurisdictions. This section examines the legal framework in Africa plus the role of sub-regional organizations, and the status of national legislation in some African countries for example Kenya

The African Union Convention on Cyber Security and personal Data Protection (Malabo Convention).46 It was adopted in 2014 in Malabo, Equatorial Guinea. It represents the first comprehensive African treaty to address both cybercrime and personal data protection. The convention lays out the framework for the protection of personal data, requiring states to establish legal mechanisms to ensure data processing respects fundamental rights and freedoms. For example the key provisions are; the establishment of a national data protection authority under Article 11, the requirement for lawful and transparent processing of personal data under Article 13, the obligation to obtain informed consent from data subjects under Article 13, the protection of data subject rights, such as access, rectification, and opposition to processing under Article 15.47

[46] https://africanlii.org/akn/aa-au/act/convention/2014/cyber-security-and-personal-data-protection/eng@20140627/

[47] Malabo convention

While the Malabo convention marks a significant milestone, its effectiveness is limited by the low level of ratification. As of 2025, only 15 out of 55 African Union member states have ratified the convention.48 This limited update reflects political hesitation, capacity constraints, and the prioritization of other national concerns. In comparison with Uganda, Uganda's DPPA aligns with the Malabo Convention in terms of establishing a regulatory framework and safeguarding data subject rights. However, Uganda has not ratified the convention, which limits regional harmonization and cooperation on enforcement.

In addition to the Malabo convention, several Regional Economic Communities (RECs) Africa have developed their own frameworks or guidelines on data protection for example the Economic Community of West African States (ECOWAS) which adopted in 2010 a supplementary Act on personal Data protection, which requires member states to enact national data protection legislation constituent with the Acts principle's which mandates the creation of independent data protection authorities, adherence to international standards such as consent, purpose limitation and data security. The Southern African Development Community (SADC) does not have a binding data protection protocol, but it encourages member states to adopt privacy laws aligned with international best practices. Countries like south Africa have taken the lead in implementing such standards.

The East African Community (EAC) has taken a step towards enhancing digital integration and safeguarding data privacy with the development of regional Data

[48] Malabo convention

governance policy framework.[49] The EAC Data Governance Policy Framework, which aims at harmonizing data governance across partner states to foster secure, efficient, and inclusive digital systems for sustainable economic growth and regional integration, was validated by a diverse group of stakeholders in Kigali, Rwanda.[50]

Here are some of the EAC which have adopted the binding data protection legislation, through levels of implementation and enforcement

a) Kenya

Kenya enacted the Data Protection Act 2019. It provides for the rights of data subjects, controllers obligations, and the establishment of the Office of the Data Protection Commissioner (ODPC) is independent and actively enforces compliance. The Act also provides clear data processing principles like purpose limitation, accuracy, and accountability and penalties. In comparison to that of Uganda, Kenya provides a more enforceable model, particularly in regulator independence and enforcement powers.

Uganda's PDPO still operates under the NITA-U which could compromise independence.

Kenya's law also includes data protection impact assessments, which Uganda's law lacks.[51]

b) South Africa.

[49] https://www.eac.int/press-releases/3195-eac-set-to-advance-data-governance-and-protectionwithdevelopment-of-a-regional-policy-framework

[50] https://www.eac.int/press-releases/3195-eac-set-to-advance-data-governance-and-protectionwithdevelopment-of-a-regional-policy-framework

[51] Data Protection Act,2019

South Africa is a regional leader with its Protection of Personal Information Act (POPIA), enacted in 2013 and was enforced from 2021. The law establishes a comprehensive framework for lawful data processing, the Information Regulator as the enforcement body and data subject rights similar to those under the GDPR. It also provides for penalties including administrative fines and criminal penalties. In comparison with Uganda, South

Africa's enforcement framework is more mature and effective. Uganda can learn from

POPIA's emphasis on regulator independence, public awareness campaigns, and proactive enforcement strategies.[52]

c) Nigeria.

Nigeria's data protection regime has been largely shaped by the Nigerian Data Protection Regulation (NDPR) issued in 2019. Though not a law passed by the parliament, it provides substantial obligations for data processors and establishes sanctions for non-compliance. A new data protection bill is under parliamentary review to strengthen the legal framework.[53]

Comparison of key elements of international data protection standards—particularly the GDPR with the regional frameworks in Africa specifically the DPPA.

Foundational principles and scope. Both the GDPR and African regional frameworks emphasize foundational principles such as lawfulness, fairness, transparency,

[52] Protection of Personal Information Act.

[53] Nigerian Data Protection Regulation,2019

purpose limitation, and data minimization. However, while the GDPR is known for its comprehensive and enforceable obligations across all EU member states, African regional laws vary in enforceability and uniformity. For instance, the AU Convention on Cyber Security and Personal Data Protection sets a continental standard but has low ratification and implementation levels among member states.

In comparison, ECOWAS and SADC have developed detailed supplementary Acts and Model Laws, respectively which provide guidance but lack direct enforceability unless domesticated into national law. The EAC is still developing a harmonized data protection framework, and the member states exhibit varied levels of legal maturity, with Kenya and Rwanda being more advanced than others like South Sudan.

Supervisory Authority. Both the DPPA and the GDPR give data protection authorities essentially the same duties, broad authority, and scope. However, the Act leaves room for interpretation, and there is a notable disparity in the amount of detail supplied to describe and restrict these authorities. In order to safeguard the fundamental rights and freedoms of natural persons with regard to processing and enabling the free flow of personal data within the union, each member state is required by the GDPR to designate one or more independent public authorities to oversee the implementation of this regulation.54 While the DPPA establishes a PDPO who is responsible for personal data protection under NITA-U which shall report directly to the Board.55 And the office in performing its functions shall not be under the direction or control of any person or authority.56

[54] ARTICLE 5 of GDPR

[55] Section 4 of DPPA

[56] Section 5 of DPPA

Under the rights of data subject, internationally the GDPR grants robust rights to individuals including the rights to erasure, access, rectify among others. These rights have influenced African frameworks which also recognize most of these rights. However, implementation in many African countries remains inconsistent due to limited awareness, weaker institutions among others. For example, Kenya's Data Protection Act mirrors many GDPR provisions including the right to be forgotten and to object processing while Uganda's Data Protection Act is more limited in its recognition of data subjects' rights, particularly regarding automated decision making and portability.

Regulatory oversight and enforcement. The GDPR establishes strong supervisory authorities with wide powers to impose an administrative fine pursuant to Article 83 which provides for the fines. African regional frameworks similarly call for independent data protection authorities (DPAs), but only a handful of countries have established effective regulatory bodies. Kenya and Nigeria have relatively functional DPAs, and Uganda under the DPPA also provides a Personal Data Office who oversees the implementation of and be responsible for the enforcement of the Act.[57] while many EAC countries lack these institutions or have weak enforcement capacity.

Cross-Border Data Transfers. A key area of divergence lies in cross-border data transfers regulations. The GDPR imposes strict controls, allowing transfers only to jurisdictions with adequate protection or under approved safeguards and shall not

[57] Section 5 of the DPPA

require specific authorization.58African frameworks recognize concern, particularly the AU convention which require data controllers to ensure similar levels of protection before transferring data abroad. Under the DPPA it provides similar protection but the Act only recognizes consent as an alternative mechanism for data transfer. 59 However, enforcement mechanisms are underdeveloped, and many national laws lack clarity or practical procedures for compliance.

Consent and legal basis for processing. Consent is a central legal basis for data processing across frameworks. The GDPR requires that consent be freely given, specific, informed, and unambiguous.60 It provides that the withdraw of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Withdrawing will be as simple as consenting. 61 African laws also emphasize consent but often lack detailed guidance on obtaining or withdrawing it, leading to weaker safeguards in practice. For example, under the DPPA section 7 it provides for consent but it does not specifically refer to consent withdraw. It provides that consent is required unless expectations apply under section 7(3).62

Accountability. Both the GDPR and the Act provide for the principle of accountability, however they do so in different forms with the Act emphasizing the capacity for data subjects to hold persons to account. Furthermore, the Act does not establish the distinction like the GDPR between processor and controller liabilities. Article 5(2)

[58] Article 45 of GDPR
[59] Section 9 of DPPA
[60] Article 4 of the GDPR
[61] Article 7(3) of GDPR
[62] Section 7 of DPPA

and section 3 provides for this principle. Under liability of data controllers and data processors Article 82(2) provides that controller involved in processing shall be liable for the damage caused by processing which infringes this regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. 63 whereas the DPPA does not differentiate liabilities between data controllers, collectors, or processors.

Collection of data related to children. Both the GDPR and the DPPA provide for the requirement and consent of children's data under article 8 and section 8 respectively. However, the act does not include regulations for providing children with privacy notices, in contrast to the GDPR. While the act does not specifically address privacy notices for children, Article 5864 stipulates that any information and communication addressed to children should be in a clear and simple language that the children can understand, given that children deserve special protection.

Conclusion.

This chapter has critically examined and compared international and regional data protection frameworks, with a focus on the GDPR and the regional instruments within Africa, particularly those affecting EAC member states. The analysis reveals that while African frameworks increasingly adopt global best practices—such as consent based data processing, data subjects, and the establishment of regulatory authorities—implementation remains uneven and largely aspirational in many states. Therefore, although legislative frameworks are gradually aligning with international

[63] Article 82 of GDPR

[64] GDPR

standards, the effectiveness of these laws in protecting personal data depends on political will, institutional capacity, public awareness, and regional cooperation. There's an urgent need for EAC member states to harmonize their laws, strengthen their regulatory bodies, and foster cross-border cooperation to address the growing challenges of data privacy in an increasingly

CHAPTER 5

SUMMARY OF FINDINGS, RECOMMENDATIONS AND CONCLUSIONS.

5.0 INTRODUCTION

This chapter wraps up the major findings from the doctrinal and comparative analysis undertaken in the preceding chapters and makes recommendations on how the challenges observed in the research can be addressed. It also highlights critical issues related to the enforcement of data protection laws in Uganda, drawing from legislative gaps, institutional weaknesses and the broader socio-legal context. These findings form empirical and analytical basis upon which the recommendations in the next section are grounded.

5.1 Key findings

The study revealed that the Data Protection and Privacy Act,2019 has several substantive and procedural gaps that hinder effective enforcement. Notably, the Act lacks clear definitions for essential terms such as consent, sensitive personal data, profiling, and automated decision-making. The absence of these definitions limits the Act's interpretability and opens avenues for arbitrary application. Additionally, the Act does not provide for Data Protection Impact Assessments (DPIAs), which are critical for assessing the risks associated with new technologies and data processing operations. The failure to mandate DPIAs makes it difficult to embed privacy- by design principles into data governance.

Weaknesses in institutional enforcement mechanisms. The Personal Data Protection Office (PDPO), housed under the National Information Technology-Uganda (NITA-U),

is tasked with overseeing compliance with the DPPA. However, the study found out that the office lacks financial autonomy, independence, and technical expertise needed to effectively carry out its mandate. Its institution placement with NITA-U compromises its impartiality, particularly when investigating data breaches involving government institutions. Furthermore, there is minimal coordination between key regulatory bodies such as the UCC and URA all of which play roles in data management and cybersecurity.

Another key finding relates to the low levels of public awareness regarding data protection rights in Uganda. The majority of data subjects are unaware of their rights under the DPPA, including the right to access, rectify, or erase their personal data. This lack of awareness is compounded by low digital literacy, especially in rural areas and among marginalized communities. As a result, violations often go unreported, and data controllers operate with minimal accountability.

The study also found that Uganda's legal framework lacks robust provisions on cross border data transfers. The DPPA does not specify the criteria for assessing the adequacy of foreign jurisdictions, nor does it mandate safeguards for international data flows. In the age of cloud computing and multinational data processing, this omission creates significant risks to data sovereignty and accountability. Foreign companies processing Uganda citizens' data may not be held to comparable standards of protection.

There is uneven implementation of data protection practices between government agencies and private entities. Some ministries and public agencies continue to collect

and process personal data without obtaining informed consent or providing adequate transparency. On the private sector side, while some large institutions especially in banking and telecoms have adopted compliance frameworks, small and medium-sized enterprises (SMEs) often operate without any data protection policies or protocols.

Lessons from international and regional comparisons. A comparative analysis of jurisdictions such as the European Union (GDPR), South Africa (POPIA), and Kenya (DPA 2019) demonstrated that effective enforcement is strongly linked to the presence of independent data protection authorities, clear procedural rules, and active judicial oversight. These countries have integrated principles such as data minimization, transparency, and accountability more comprehensively into their legal frameworks. Uganda could benefit from adapting these best practices to strengthen domestic enforcement.

In summary, the findings point to structural and systemic challenge in enforcing data protection laws in Uganda. While the legislative foundation exists, the law suffers from definitional and procedural weaknesses, underdeveloped enforcement institutions, and a public that is largely uniformed of rights. Without addressing these issues, Uganda risks undermining the very purpose of its data protection regime—namely, to safeguard the dignity, autonomy, and digital security of its citizens.

5.2 Recommendations

One of the most urgent step is to amend the DPPA to address its substantive deficiencies. As identified in the findings, the Act lacks precision in key areas,

including definitions of consent, sensitive personal data. These ambiguities create uncertainty in interpretation and enforcement. It is recommended that the parliament initiate amendments to the Act to introduce clear and specific definitions aligned with international standards, specify sanctions for different categories of offences and also mandate DPAIs for high-risk data processing activities.

Strengthening institutional capacity and independence. The PDPO must be made operationally independent and well resourced. Its attachment to NITA-U limits its autonomy, practically in enforcing violations involving state actors. It is recommended the PDPO be transformed into an independent statutory authority, with a dedicated budget and powers to investigate, prosecute and impose penalties. A multi-sectoral oversight board be established to ensure accountability and continuous training of staff and collaboration with international agencies be institutionalized to enhance expertise.

Enhancing public awareness and digital literacy. Ugandans are uniformed about their rights under the DPPA, to address this gap the government in partnership with the civil society, should initiate national awareness campaigns using radio, television and social media. Digital literacy should be integrated into the national education curriculum, beginning at the secondary school level and also establishing community based training programs to target vulnerable groups for example the youth and persons with disabilities.

Cybersecurity measures. The government should implement adequate security measures to protect database from unauthorized access or breach. Train staff on

Data protection and compliance requirements. Appoint a DPO to handle large amounts of Data and conduct regular impact assessments to discover any security gaps and create risk mitigation plans.58 Developing robust Cross-Border Data Transfer Rules. By amending the DPPA to include adequacy determinations for third countries and provide for binding corporate rules. To develop cross-border transfer guidelines in line with Article 4 of the Malabo Convention and Chapter v of the GDPR

Encouraging compliance among public and private actors. The government should develop sector-specific codes of practice, particularly for finance, health, education and telecommunications. Require mandatory registration of data controllers, processors and also impose administrative fines and civil penalties for noncompliance.

Fostering Regional and international cooperation. It is recommended that Uganda should ratify the Malabo Convention and implement its provisions domestically and also actively participate in the Network of African Data Protection Authorities to build regional frameworks.

Need to provide for transitional provisions that would cater for data held by the state and nonstarter actors before coming into force of the law. All data should be consolidated in one place and data in private actor's hands should be destroyed to ensure it is not abused.65

[65] (https://www.unwantedwitness.org) accessed 30th April 2025

5.3 Conclusions

The key findings demonstrated that while Uganda has made a commendable step in enacting the DPPA, the law is marred by several legislative ambiguities, enforcement weaknesses and systemic limitations like lack of precise definitions, limited institution capacity, insufficient public awareness among others. Moreover, the comparative analysis highlighted that successful enforcement of data protection laws in other jurisdictions such as European Union is significantly aided by the presence of independent data protection authorities, comprehensive legal definitions and strong public engagement.

Ultimately, for Uganda's Data Protection regime to be effective, there is need for a stronger political will, increased public awareness, institutional reforms, and alignment with global data protection standards. The findings of this study underscore the urgency of addressing these challenges to ensure that the right to privacy is not only recognized in law but also meaningfully

BIBLIOGRAPHY

Books, Articles, papers and magazines

Alex Boniface, Privacy and Data Protection in Africa: A State of the Art International Privacy Law 2012, volume 1

Lee A Bygrave, Data Privacy Law: An international perspective (Oxford University press 2014)

Colette Cuijpers, A Private Law Approach to Privacy: mandatory Law Obliged?

Graham Greenleaf, Global Data Privacy Laws 2021

Christopher. Kuner, Trans border Data Flows and Data Privacy Law (2nd edn, Oxford University Press 2020)

Privacy international, Uganda's Data Protection Privacy Act, 2019: Analysis and recommendations httsp://privacyinternational.org accessed 30th April 2025

B Schemer, B Custers and S Van der Hof 'The crisis of content: How stronger legal protection may lead to weaker consent in data protection' (2014)

Andrew Green, 'scarcity of Data Protection Laws in Africa Leaves NGOs Exposed' (/ 27th June 2018)

The OECD, Guidelines on protection of privacy and Trans border Flows of personal Data (1980)

Government and institutional Reports

Collaboration on international ICT policy in East and Southern Africa(CIPESA),

Uganda's Data Protection Landscape (CIPESA Report, 2022) National Information Technology-Uganda (NITA-U 2024).

Personal Data Protection Office, strategic plan 2022-2026(2022)

Uganda Human Rights Commission, Annual Report on Human Rights and Freedoms in Uganda, 2023(2024)

websites

Chapter four Uganda, Homepage (https://chapterfouruganda.org) accessed 30th April 2025

CIPESA, collaboration on International ICT Policy in East and Southern Africa https://cipesa.org accessed 30th April 2025

National Information Technology Authority Uganda(NITA-U), Personal Data Protection Office (https://privacyinternational.org) accessed 30th April 2025

Privacy international, Uganda's Data Protection Privacy Act, 2019: Analysis and Recommendations(httsp://privacyinternational.org) accessed 30th April 2025

Unwanted witness, Homepage(https://www.unwantedwitness.org) accessed 30th April 2025

National legislation and Treaties

Constitution of the Republic of Uganda,1995

Data Protection and Privacy, Act 2019 (Uganda)

General Data Protection Regulation (EU Regulation2016/679)

Kenya Data Protection Act,2019

Malabo Convention (African Union Convention On Cyber Security and Personal Data Protection, 2014)

Nigerian Data Protection Regulation,2019

Protection of Personal Information Act 4 of 2013(south Africa)

List of cases

Google v Lloyd [2021] UKSC/2019/0213

Mukasa Peter v MTN (Uganda, 2021)