AN ANALYSIS OF THE EFICACY OF THE DATA PROTECTION AND PRIVACY ACT, 2019 IN UGANDA

LINDA CAROLINE ARINDA

CS20B11/021

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

May, 2024

UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa

DECLARATION

I, **ARINDA .LINDA .CAROLINE**, a student at Uganda Christian University in Mukono, officially declare that the dissertation I have submitted, titled is an original work that I accomplished with the assistance of Dr. Kamusiime. Oscar, a university lecturer.

SIGNED BY:

ARINDA .LINDA .CAROLINE ……

DATE……

APPROVAL.

I vouch for **ARINDA .LINDA .CAROLINE** conducted the study and authored this report with my guidance.

The report was submitted for assessment with my approval as a university supervisor.

……..... .....

Dr. KAMUSIIME.OSCAR. Signature

SUPERVISOR

ABSTRACT.

The President signed the long-awaited and desperately needed Data Protection and Privacy Bill of 2018 into law on February 25, 2019.The acquisition, storage, processing, and use of personal data by a variety of entities (including government agencies, businesses, and private institutions operating both within and outside Uganda) is regulated by the Data Protection and Privacy Act of 2019 ("the Act").

Uganda has made efforts to emulate the General Data Protection Regulation (GDPR) of the European Union, which mandates member states to safeguard the privacy and data usage rights of their citizens both inside and outside the economic bloc. As a result, the 1995 Constitution of the Republic of Uganda, in addition to the Data Protection and Privacy Act, 2019, and other legislation, fail to meet the standards of international data privacy best practices.

This Act contains numerous opportunities to safeguard the Right to Privacy, but it also contains loopholes that ensure enforcement will fail.

DEDICATION.

This dissertation is dedicated to my parents, for their moral, spiritual, and financial support from childhood to this point in my education, as well as for the rest of my family.

And to my supervisor despite his busy schedule, he took off time to provide me with the necessary assistance required.

To my Lord and Savior, Jesus Christ, who has been true to me since the beginning and will continue to do so. I am appreciative for all of the above and the attention that has been provided to me.

ACKNOWLEDGEMENT.

I would like to thank everyone who helped finish this research report. In humble thankfulness, I raise my voice,

First and foremost, I praise the Almighty God for His love, grace, and limitless choices. Every dawn, your light shines, guiding me with divine hands. For both visible and invisible blessings, for strength, courage, and cleansed hearts. I hold you dear in every breath, your presence near, with a grateful heart, for you have been my cornerstone in the trying times of my educational journey.

I want to express my heartfelt gratitude to my supervisor, DR.KAMUSIIME.OSCAR for their tremendous direction, unshakable support, and constructive comments during the period of this research project. Their advice and support helped shape the direction and quality of this effort.

I am also appreciative to Uganda Christian University for providing the required resources, facilities, and academic environment for research. I would like to express my heartfelt gratitude to all of the participants who kindly donated their time and insights for this study. Their inputs have enriched the findings and increased the importance of our study. Furthermore, I'd want to thank my colleagues and friends for their encouragement, understanding, and insightful discussions that have sparked my thinking and provided moral support during difficult moments. Finally, I am grateful to my family for their unfailing love, encouragement, and patience during this journey. Their unwavering support has been my anchor, allowing me to negotiate the complexity of academic pursuit.

Finally, I'd like to express my heartfelt gratitude to everyone who helped complete this research report, whether directly or indirectly. Your assistance has been critical in making this project feasible.

Thank you. MAY THE ALMIGHTY GOD BLESS YOU ALL ABUNDANTLY?

LIST OF ABBREVIATIONS

DPPA - Data Protection ant Privacy Act.

NITA - National Information Technology Authority.

PDPO - Personal Data Protection Offices

UPDF - Uganda People's Defense Force.

GOU - Government of Uganda.

CSV - Comma Separated Values.

MoJCA – Ministry of Justice and Constitutional Affairs.

UCC - Uganda Communications Commission.

GDPR – General Data Protection Regulation.

EU – European Union.

TABLE OF CONTENT

CHAPTER ONE.

1.0. INTRODUCTION.

This chapter was based on the study's background, problem statement, objectives, research questions, scope, significance, literature examined by various authors, and the technique utilized to perform the research.

1.1. BACKGROUND OF THE STUDY

The concept of data protection can be traced way back to 1800 when United States lawyers Samuel Warren and Louis. Brande wrote the "**right to privacy Article**" that first envisaged the right to be left alone, Warren and Brande propounded that the right to privacy therefore means the right to be left alone.

Another significant milestone in the concept's development occurred with the establishment of the Data Protection Convention Treaty in Europe, which established the right to privacy in European law for the first time. The World recently witnessed the introduction of the General Data Protection Regulation for Europe, which was probably one of the most high-profile data protection legal events in history.

In Africa, the African Union took the first regional move to protect personal data and the right to privacy in 2014, when it adopted the African Convention on Cyber Security and Personal Data Protection. Other countries have established national data protection legislation.

Uganda is one of several African countries that has passed a national data Protection law. The Data Protection and Privacy Act of 2019.The Act is a legal step toward advancing and realizing the right to privacy enshrined in the Constitution of the Republic of Uganda 1995, which states that no person shall be subjected to interference with the privacy of his or her home, correspondence, communication, or other property. The current Act however depicts some loopholes and lacks proper implementation and enforcement mechanisms.

Prior to the enactment of the current Data Protection and Privacy Act, Uganda's legal framework governing data and privacy rights was based on the Constitution, common law principles, and statutes such as the Access to Information Act of 2005, Uganda Communication Act of 2003, Electronic Signatures Act of 2011, and Computer Misuse Act of 2011.The new Act, however, does not portray adequate implementation and enforcement procedures when considering the rate

at which data is used in the world today, with the exception of poorer countries. As a result, lawmakers should have included comprehensive measures in the act that provide a broad and long-lasting regulatory legal framework for data protection issues whilst finding a way to balance the individual rights of Ugandans with the government's intention to promote national security and the need to make profit by businesses.

1.2. STATEMENT OF THE PROBLEM

Despite the fact that the Act was promulgated and is now in operation, it contains gaps and fails to include important and vital regulations regarding the act's implementation and enforcement. Unregulated data processing activities in Uganda by public and private entities continue despite the existence of the regulations. This study examines the DPPA Uganda to determine whether it is beneficial in reducing insecurity while also protecting and improving the right to privacy. With big data becoming an asset for any company, corporation, or organization, there is greater access to information, which, if not properly managed, might compromise people's right to privacy. This study contrasts Uganda's current data protection law with international standards and thresholds for the concept of data protection in privacy, and it also demonstrates that data usage trends in Uganda indicate a need for strong enforcement of data protection and privacy laws.

Furthermore, given the importance of data and information usage in this day and age, with many companies and organizations adopting a data and information-based approach to operation that jeopardizes people's right to privacy, an all-protective data protection law is one of the most important things that should be given top priority, as well as well-established mechanisms for implementation and enforcement.

1.3. PURPOSE OF THE STUDY.

The purpose of the study is to critically analyze the Data Protection Act 2019 and its impact on the right to Privacy in Uganda.

1.4. OBJECTIVES

1.4.1. General objective of the study;

To analyze the efficacy of the Data Protection and Privacy Act, 2019.

1.4.2. Specific objectives of the study;

To identify salient features of the right to privacy.

To give an in-depth analysis of the Data Protection and Privacy law 2019 in Uganda.

To analyze the effectiveness of the Data Protection and Privacy Act in enforcing the right to Privacy.

1.5. RESEACH QUESTIONS

- What are salient features of the DPPA, 2019 and its efficiency in the promotion of the right to Privacy as enshrined under the 1995 Constitution of Uganda as amended?

1.6. SCOPE OF THE STUDY

- **Content Scope;**

  The subject of this scope involves current data protection laws both national and international legislations it also focuses on the present and future trends on data management and protection.

- **Geographical Scope;**

  This research focuses on Uganda as a geographical context and research foundation. It examines the applicability of data privacy and data protection legislation to data crimes and breaches in the Republic of Uganda. Jurisdictional issues of data protection were one of the topics presented during the Brussels International Conference on Computer Privacy and Protection on January 23, 2015. At the meeting, it was emphasized that while the internet covers the globe and knows no borders, legal systems are territorial. There are fundamental and practical issues given the significant differences in data protection regimes both in general and law enforcement. This paper therefore focuses on analyzing the data protection act of Uganda which is located in East Africa and is the first country to adopt a national data protection law.

- **Time Scope;**

The study focuses on exploring the DPPA from its time of commencement to the present time and future legal aspects of data management and security.

1.7. SIGNIFICANCE OF THE STUDY

- **GOVERMENT**

It will guide the government to understand the right to privacy and the different mechanisms that the government has put in place to protect the same.

- **MINISTRY OF INFORMATION, COMMUNICATIONS AND TECHNOLOGY.**

To understand its role in relation to data Protection.

- **ACADEMICIANS.**

The study will provide more knowledge to researchers or academicians desiring to conduct a relevant study.

- **Researcher.**

The study will enable the researcher to attain the relevant knowledge in the study and also accomplish required for an award for Bachelor of law at Uganda Christian University.

1.8. METHODOLOGY

This research is going to be focused on the doctrinal method of research. This method has been used to examine the current law on data protection.

Data was collected from different literature authorities and journals on the internet and finally picked different views of authors and their analysis on the topic.

1.9. LITERATURE REVIEW.

Article 27, 1995 Constitution of Republic of Uganda as amended, provides of the right to privacy and different literature has been advanced on this topic especially on data protection as shown below.

There is little literature on the concept of data protection and privacy in Uganda and Africa; however, Alex. Boniface. Makulilo assessed his views in Privacy and data protection in Africa: a state of the art international privacy law, 2012, vol.2, and conducted a survey of the major literature on data protection in Africa. He proposed that efforts be directed on training, research, networking, and the establishment of modern libraries dedicated to data protection law.

Nevertheless, I have examined the available literature on the subject as propounded below;

Cuijpers, De Hert, and Gurtwirth have attempted to define and distinguish between the two concepts of data protection and data privacy as used in this research. Cuijpers notes that because an individual right to privacy protects an undisturbed private life and offers the individual control over intrusion into their private sphere, it is different from protection of the individual with regard to the processing of personal data, which is not restricted to the private sphere. It goes

without saying that data protection regulations are not intended to address privacy in its broadest meaning; rather, they are fundamentally related to the concept of individuals.

De Hert and Gutwirth, in their authority c.cuijpers, "a private law approach to privacy: mandatory law obliged," claim that the real object of data protection is to safeguard individual people from unjustified data collection, storage, use, and broadcast of their personal information. This appears to be related to the basic goal of the right to privacy: to protect against unjustified intrusion into one's personal life.

Schermer.Custers and Van der Hof have suggested that higher legal protection may result in weaker consent in data protection. Obtaining consent for processing personal data raises ethical, legal, and practical concerns. Well-intentioned regulation may give a contradictory incentive for data controllers to pursue solutions that erode rather than strengthen confidence. The European Union, for example, passed a cookie legislation that prohibits websites from monitoring users without their knowledge or consent by using small quantities of data (cookies) saved in the user's browser.

Some websites replied by giving a take it or leave it consent option, which did not provide users with a meaningful choice. This may have followed the text of the law but failed to apply it in spirit. Overall, users did not see improved privacy outcomes. Solving the challenging problem of consent is likely to necessitate a combination of legal and technical solutions, and in some circumstances, service providers may be motivated to circumvent the law due to strong economic incentives. Personal data protection regulations should be created in a way that balances what is legally necessary with what is technically achievable, as well as what best reflects the individual's interests when asked to give consent.

1.10. CHAPTER SYNOPSIS.

The study will deal with four chapters where chapter one dealt with the introduction involving background of the concept of data protection with Uganda as a case study, the problem statement and then the subsequent parts that is the literature review, Chapter two deals with the data Protection Act in Uganda, Chapter three provides an in-depth analysis of its regulation of the right to Privacy, and lastly chapter four discussed the recommendations and conclusions.

CHAPTER TWO (2).

AN ANALYSIS OF THE RIGHT TO PRIVACY AS ENSHRINED UNDER THE 1995 CONSTITUTION OF THE REPUBLIC OF UGANDA.

2.0. INTRODUCTION.

This chapter elaborates on an in-depth analysis of the right to privacy as enshrined under the 1995 Constitution of the Republic of Uganda. The chapter provides for the challenges to DATA PROTECTION AND PRIVACY ACT regarding privacy as enshrined in the 1995 Constitution of the Republic of Uganda as amended.

2.1. THE RIGHT TO PRIVACY;

It is only prudent to say that the right to privacy is a fundamental human right, enshrined in various International Human Rights Instruments. It is pivotal to the protection of human dignity and forms the basis of any democratic society and it also supports and reinforces other rights such as freedom of expression, information, and association. Activities that restrict the right to privacy such as surveillance and censorship can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued as elaborated by Hon.Justice Manyindo in the case of **Charles. Onyango Obbo and Andrew.Muwenda vs. AG (Constitutional Petition No.15 of 1997) [1997] UGCC 7.** The right to privacy has evolved to encompass State obligations concerning the protection of personal data, thanks to the innovations in information technology that allow unimagined forms of collecting, storing, and sharing personal data.

2.1.1. THE 1995 CONSTITUTION OF THE REPUBLIC OF UGANDA REGARDING THE RIGHT TO PRIVACY;

The 1995 Constitution of the Republic of Uganda as amended expressly recognizes the right to privacy and alarms for its protection for instance **Article 27, 1995 Constitution of the Republic of Uganda as amended** clearly explains that no person shall be subjected to unlawful search of their person, home or other property of that person or unlawful entry by others of the premises of that person. Thus, **Article 27(supra)** is to the effect that among the rights that have been held to be pivotal to

the dignity and well-being of the individual is the right to privacy, which covers the privacy of the physical body as well as of the home, correspondence, and communication of the individual also known as image rights. In furtherance, **Article 27(2) (supra)** stipulates that no individual shall be subjected to the intrusion of the privacy of that individual's home, correspondence, communication, or other property. For instance, *in 2014, Uganda's government through the National Information Technology (MoICT) and the Ministry of Justice and Constitutional Affairs (MoJCA) issued a draft Data Protection and Privacy Bill for public comment and it was enacted into law in February 2019.*

Article 27(supra) protects an individual's right to privacy of person, home, and other property, and thus prohibits any form of an unlawful search of the home, property, and individual's person. This Article further bars unlawful entry into a person's premises and interference with the privacy of a person's home, communication, or other property, illegal. In the **Canadian case of King V. Therens [1985] S.C.J.NO.30,18 C.C.C.(3d) 481,** *the police entered and searched the accused's house without a search warrant, and the Canadian Supreme Court found that since the police did so without reasonable cause or a search warrant, they had violated the accused's constitutional right to privacy. The court also found that taking the accused's fingerprints amounted to an act of violation of this right to privacy unfortunately; the right has been the subject of numerous violations of a serious nature in Uganda, whether on grounds related to the enforcement of national security the fight against terrorism, or treason or in the prevention of illegal immigration.*

Article 28(1),1995 Constitution of the Republic of Uganda as amended provides for the concept of fair hearing which protects the person's rights to a fair and speedy trial, and also stipulates that such trial shall be heard publicly by an unbiased court or tribunal established by law. This elaborates that all trials must be heard in open court allowing everyone to witness the hearing, although the court reserves the right to have the proceedings on camera where the matter touches on sensitive matters of

National Security or issues of morals whose disclosure is not in the public interests and may compromise national security or that of the litigants. Court cases are meant to be public simply because the courts have to open to the people while doing their work since they carry out their duties in line with **Article 126(1), 1995 Constitution of the Republic of Uganda as amended** that provides for the concept of Judicial power which a cardinal role of the courts of Judicature. In the same vein, **Article 41(1) of the 1995 Constitution of the Republic of Uganda as amended** stipulates that every citizen has a right of access to information in the possession of the state or any other organ or agency of the state except where the release of the information is likely to prejudice the security or sovereignty of the State or interfere with the right to the privacy of any other person. **Article 41(supra)** provides for a more elaborate assertion for an efficient, effective, accountable, and transparent government and gives effect to this which aims at protecting individuals from disclosing information as well as empowering the public to effectively scrutinize and participate in government's decisions that affect them. Thus, it is the power of the parliament to make laws providing for the classes of information referred to **in clause (1) of Article 41(supra)** and the mechanism for obtaining access to that information in fulfillment of this mandate; parliament enacted the Access to Information Act in 2005. In general, the Act reaffirms all citizens' constitutional rights to information but significantly increases access to updated information. **Article 41(2) (supra)** mandates Parliament to make laws that provide the classes of information referred to in **Article 41(1) (supra)** and the mechanism for obtaining access to such information. The main aim of Article 41 has been transcribed into law with the pronouncement of the Access to Information Act of 2005. Regrettably, the law appears to have swerved somewhat from the spirit of the constitutional provision placing obstacles in the way of ensuring that information ultimately belongs to the public. "*As highlighted in a newspaper article of Daily Monitor, a Magistrate declined to grant several journalists from the Daily Monitor access to the oil exploration agreements signed by the government.*"

Article 41(supra) represents a radical redevelopment of the notion of information and guarantees that the public has access to it. For instance, in the decided case of

Green Watch (U) Ltd v. A.G and Anor [2002] UGHCCD 28, the petitioner claimed that it had a right of access to the Power Purchase Agreement (PPA) about the proposed construction of a hydro-electric power dam at Bujagali Falls on the river Nile. The respondents raised several objections regarding the appropriateness of the application and argued that it had not infringed the right since it was not a party to the PPA. The Court was confronted with the issue of determining whether the PPA was a 'public document' within the meaning of section 72 of the Evidence Act. The Court elaborated on the elements of the right to information, holding that the right under Article 41 did not only envisage possession of the required information. Thus, the fact that the state was not a party to the PPA did not excuse it from having to avail the information sought. On this accord, Justice Egonda-Ntende pointed out that Article 41(1) of the Constitution of the Republic of Uganda provides for information in the possession of the state. The state does not have to be a party to the agreement.

In another court decision of **Major General Tinyefuza Vs Attorney General [1997] UGCC 3**, Mulenga JSC stated that where the state contended that the information sought fell within the ambit of the restriction in Article 41(1), it had the burden to prove that the disclosure of such information was likely to prejudice the security or sovereignty of the state.

In **Zachary Olum and Anor v. Attorney General (Constitutional Petition No. 6 of 1999),** the Court was confronted with the discretion given to the speaker of Parliament to grant or reject leave to a member of Parliament to use proceedings of the house in evidence before a court of law under section 15 of the National Assembly (Powers and Privileges) Act. Justice Mpagi Bahigeine referred to Section 15 of cap 249(supra) to prescribing a special procedure for accessing information in the possession of Parliament which was inconsistent with Article 41 of the 1995 Constitution of the Republic of Uganda.

This decision can applied pari materali with the decision of **Jim Muhwezi Katugugu v. Patrick Kiggundu and Anor (Constitutional petition NO.4 of 1998)** in which the Constitutional Court misapplied the provisions of Article 41. Instead relying on the

National Assembly (Powers and Privileges) Act (which restricted access) despite it being subordinate to the Constitution.

In a decided case of **Attorney General v. Chief Editor, Monitor Publications Ltd & Anor (Misc. Application No.615 of 2002)** the Constitutional court upheld the notion that the government could not prevent the publication of what it regarded as a sensitive matter on the grounds of privacy or sovereignty, even though the judge ultimately granted an injunction against the paper.

Their lordships in the case of **Paul K. Ssemwogerere & Anor. V. The Attorney General (Constitutional Appeal No.9 (2002),** elaborated on whether or not the provision is given full expression is often dependent on what particular information is at stake. They further stated that it is unclear whether the government can comply with an order of the court to disclose particular information that it originally declined to reveal, which raises questions about the implementation of the provision of the Bill of Rights as enshrined under Chapter 4(supra). Apart from the Act bailing out general information on access to framework, it jealously guards the sanctity of the right of access to information and sets out to facilitate increased access yet one of the impediments to full disclosure and maximum access to information in the public domain are the archaic and inconsistent laws. Most of them had been enacted essentially to protect colonial governments of the day but have persistently remained on the National Statute Books. Successor regimes have and continue to utilize them to keep themselves in power by limiting public participation.

These laws cannot stand Constitutional scrutiny in the wake of renewed calls for commitment to good governance, rule of law and Constitutionalism thus should be subject to **Article 274, 1995 Constitution of the Republic of Uganda as amended.** Even with frequency of violation, there are few cases in which individuals have challenged the authorities over their actions for instance the cases below note both involved Lesbian Gay Bisexual Transgender Intersex (LGBTI) activists coming out to challenge the law which was against their act.

For instance, in the case of **Victor Juliet Mukasa & Yvonne Oyo v. Attorney General, Misc. Cause No. 24/06,** the Police entered the petitioner's premises without a search warrant, searched them, pilfered their property, and even undressed them. This Act was found to be unlawful and a clear violation of **Article 27 of the 1995 Constitution of the Republic of Uganda as amended**, in addition to violating several provisions of International Law cited by the judge. The High Court awarded the applicant a ward of Uganda Shillings 3,000,000/= (Three million shillings) for the violation of Article 27(2) of the 1995 Constitution of the Republic of Uganda related to the confiscation and damage done to his property by over-zealous Local Council Officials.

Concerning the right of privacy of the home and person under **Article 27 of the Constitution (supra),** the court has no doubt, again using the objective test, that the exposure, of the identities of the persons and homes of the applicants to fight gayism and the activities of gays, as can easily be seen from the general outlook of the impugned publication, threaten the rights of the applications to privacy of the person and their homes and they are entitled to that right. Thus, the protections stated in **Article 27 of the 1995 Constitution of the Republic of Uganda as amended** extended to areas of communication such as the tapping of phone calls, intercepting mail, and the illegal accessing of bank statements. Therefore, the Anti-Terrorism Act especially sections 18 and 19, and the recent enactment of the Interception of Communications Act seriously challenge and undermine the provisions of Article 41 of the 1995 Constitution of the Republic of Uganda. Thus, in all cases of undue influence, the critical question is whether or not the persuasion or the advice, in other words, the influence, has invaded the free volition of the (victim) to accept or reject the persuasion or advice or withstand the influence. The data subject may be led but must not be driven and the subject's will; must be the offspring of his/her own volition, not a record of someone else's.

In **Bank of Credit and Commerce International S.A v Aboody [1992] 4 ALL ER 955,** the Court of Appeal classified this doctrine into two types; actual and presumed. Under actual undue influence, the claimant must prove that he or she was induced to

sign a contract or agree to a transaction under applied undue influence; whereas in presumed undue influence the claimant only has to prove that there was enough trust and reliance between the parties that the side committing the wrong abused that relationship by exerting undue influence and inducing them to enter an ambiguous transaction. Consequently, for consent to be informed and specific, the data subject must be notified about the controller's identity, what kind of data will be processed, how it will be used, and the purpose of the processing operations as a safeguard. The data subject must also be informed about his or her right to withdraw consent at any time.

2.2. **Challenges of the Data Protection and Privacy Act regarding protection of the right to privacy;**

Section 22(3) of the Data Protection and Privacy Act provides that a data controller shall observe generally accepted information security practices and procedures, and specific industry or professional rules and regulations. What the Act does not provide for, however, is what appropriate security safeguards are. Nevertheless, it is unequivocal that a data controller should be always vigilant, and ensure data is secure to the best of his ability. This places a lot of burden on the data controller.

Section 7(2) (g) of the Data Protection and Privacy Act states that "data can be collected from another person, source or public /body where it is not reasonably practicable to obtain the consent of the data subject," depending on the circumstances under which the information is required data could be provided by other sources without the owner's consent under the guise of it not being 'reasonably practical' to obtain the data subject's consent. The circumstances under which this could happen need to be specified to ensure the protection of data in the absence of consent.

The challenge of the definition of Personal Data is another one as stipulated below; the definition of "personal data" is narrower than the EU (European Union) General Data Protection Regulation (GDPR) definition. Under **section 2 of DPPA ACT**, personal data refers to any information about a person from which the person can be

identified, that is recorded in any form and that includes data relating to nationality, age or marital status; educational level or occupation of the person; identification number, symbol or other particulars assigned to a person; identify data or other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual.

Therefore, the Act sets limits that do not exist under **GDPR (General Data Protection Regulation)** which defines personal data as "any information relating to an identified or identifiable natural person". In practice and subject to secondary legislation or guidance, the definition of personal data does not seem to cover for example, the address or utility bills of an individual, unless such address or bills include an expression or opinion about the individual. Apart from the seemingly exhaustive definition, the Act bars the processing (subject to exceptions) of "special personal data", namely personal data relating to religious or philosophical beliefs, political opinions, sexual life, financial information, health status, or medical records. The definition of personal data may be broader than the enumeration under **section 2 of the Data Protection and Privacy Act.**

Legal Basis is another challenge being faced;

Section 11 of the Data Protection and Privacy Act, 2019 provides for the collection of data from the data subject and that the default legal basis for processing personal data is the consent of the data subject. The notable exceptions to the consent requirement are the performance of a contract, compliance with a legal obligation, permission or obligation by law to process personal data, the necessity for public bodies to perform their public duties, national security, and justice and law enforcement. However, this contradicts one of the main contrasts with the right to privacy as there is the absence of legitimate interest as a legal basis for processing. Under the European Union General Data Protection Regulation for instance personal data can be processed based on legitimate interest. The intention is that according to the European Commission to allow processing of personal data to carry out tasks related to business activities when processing is not necessarily justified by a legal

obligation or carried out to execute the terms of a contract with an individual. Under the Act, in such a context, prior consent will be required. It is prudent to note that the Act allows unlawful display of work, Section 35 of the Data Protection and Privacy Act obstructs unlawful display of personal data and if it is lawfully collected must be ready for processing on incidents of historical, statistical, or research purpose. It is not specified whether" statistical or research purposes" include marketing, big data, and profiling for business purposes or whether this exception is confined to a more orthodox concept (research and statistics in the public interest by government bodies, research institutes.

Rights of Data Subjects has been elaborated as another challenge;

Provisions of sections 24, 25, and 26 of the Data Protection and Privacy Act, data subjects can exercise several rights including the rights to withdraw consent, to access personal information, to prevent processing of personal data, including for direct marketing, to object to data processing for automated decision-making, to have the data rectified, blocked or erased, subject to the filing of a complaint before the Data Protection Authority. All those rights are also provided under GDPR (supra). However, under GDPR, the rights to be forgotten and to request data rectification can be exercised directly before the data controller, without claiming the regulator which by humanity and privacy violates one's right to protection of privacy. "An elaborate look at the law, one would arrive to the conclusion that Uganda has tried to mimic the European Union's General Data Protection Regulation (GDPR)." The regulation requires EU member states to protect the data use privacy rights of its citizens, both within and outside the economic bloc. Nevertheless, when a comparison between both legislations is made, there seems to be no option but to conclude that the Ugandan law falls short of international data privacy best practices and lacks accountability. To make matters worse, the Ugandan law doesn't compel data controllers to have appropriate technical and organizational procedures which include suitable privacy policies and keeping sufficient records of their process activities yet that is the case with GDPR.

Data Protection Authority, a regulatory body;

Under **part VI The DPPA Act** establishes a Personal Data Protection Office (PDPO) under the National Information Technology Authority (NITA), even though the Act further provides that PDPO "shall not be under the direction or control of" NITA in "performing its functions under this Act. Amongst its several responsibilities, PDPO is responsible for the implementation and enforcement of the Act, for creating and keeping a register of all data processing activities, and for investigating complaints sanction powers are within the NITA's remit, which seems to have, under the Act, overlapping responsibilities with PDPO, such as keeping and maintaining the register and conducting investigations further to a complaint. The law is unclear on how the state will strike a balance between data protection and surveillance, sometimes referred to as national security and how it will be held accountable in case there is any breach. In 2014, the UN General Assembly passed a resolution that was co-sponsored by 57 member states. Therein, it asked all member states to review their procedures, practices, and legislation related to communication surveillance, interception, and collection of personal data, emphasizing the need for states to ensure the full and effective implementation of their obligations under international human rights law.

Data protection officers;

Section 4(4), DPPA, 2019 provides that all institutions must appoint a data protection Officer. "Institution" is not defined. The term could refer to any legal entity, including public bodies and private organizations, but this is unclear. The requirement to appoint a Data Protection Officer can be compared to the GDPR requirement. However, restrictions seem to be put on the obligation to public authorities or bodies and to other organizations of which core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale and this can help data owners enjoy their rights. To make matters worse, although the Act talks about establishing an office described as Personal Data Protection Office and that the head of this office will be called the National Personal

Data Protection Director whose major role will be to oversee people's personal data and implementing this Act, much seems not be achieved because history has proven that believing in such would be bordering on naivety. How sure are we that when push comes to shove, this director, who most likely will be a political appointee, won't summarily surrender people's personal information to security agencies or other government bodies without following the now laid-out procedure.

Sanctions;

Penalties for companies are comparable to the GDPR sanction regime when it comes to the calculation method. Under the **DPPA Act**, the maximum penalty amounts to 2% of the company's gross annual turnover. As regards individuals, the fines are UGX 4.8 million (GBP 975) for unlawfully obtaining or disclosing personal data and for unlawful destruction, deletion, concealment or alteration of personal data and UGX 4.9 million (GBP 995) for sale of personal data while all three offences bring a potential imprisonment of up to 10 years. The **Data Protection and Privacy Act** is an illustration of many African countries desire to adopt and harmonize legislation to encourage digitalization and establish trust in electronic transactions.

However, this has not been real as expressed in the case of **Charles Onyango Obbo v Attorney General (supra)** when the Supreme Court explained the circumstances when a constitutional right will not be protected and in accordance to the judgment where the exercise of one's rights prejudices the human rights of another and where such exercise prejudices the public interests. The judge was in agreement with the counsel for the defendant that advertising on billboards is a form of freedom of expression its exercise was prejudicial to the plaintiff's right to privacy of his image.

"As suggested in Winfield et al, Tort law at page 424, it is irrelevant that the use of the image was innocent especially as the plaintiff was not the target of the photographer but was nevertheless very visible in the photographs."

A blanket provision allowing access to all information, which does not lay down a minimal level of data protection, could constitute an infringement of the rights of privacy because different government bodies require different information, for example that requested by the Ministry of Education from the Ministry of Health and Defense may not be provided by the Ministry of Defense. If the information is to be made accessible by these public authorities, departments or ministries.

The fact that key populations are not included and some of the realities of Uganda's population are not adequately taken into account by the requirement for registration information in **Article 30 and schedule 3(supra)** is a further significant loophole under this law. The Act requires an individual who is registering to provide information about their sex, the scope of which is limited to male and female categories and does not provide for people born with disorders of sex development (intersex people), and internationally recognized medical conditions.

Members of parliament rejected a clause that would have been inclusive of intersex individuals who do not fall neatly within the male/female categories over considerations that this would encourage homosexuality (an entirely unrelated aspect). In order to gather such data that would inform the planning process on how these populations should be addressed, Parliament should take advantage of the registration procedure and all available sources.

The **Data Protection and Privacy Act** does not adequately provide for the interests of persons living with disabilities (PWDs) since it does not expressly provide for collection of such data. If indeed the purpose of this law is to aid planning and to improve service provision, then the registration process should encompass as much relevant data as possible and information on populations of PWDs is highly relevant. Uganda has both international and domestic obligations to ensure that the registration process is favorable to all individuals and parliament must ensure that every individual is able to access registration centers. There is no indication as to the length of time that the collected personal data may be retained, which raises concerns as to the legality of the use of the citizen data. While section 14(1)(3), DPPA,2019 states

that data cannot be held for a period longer than is necessary, the actual period is not indicated. Therefore, we recommend that the law clearly indicate the retention period. The retention of data for national security purposes also raises concern for the security and use of personal data as, yet again, national security is not defined. Section 15, DPPA, 2019 it is not clear what happens when a data controller does not provide security measures for data stored, while section 17 does not state what happens when a data controller discloses data unlawfully. Penalties for defaulters need to be clearly stated.

Section 18, DPPA,2019 on 'notification of data security breaches', rather than simply stating that the data subject should be notified "immediately", the Act should specify a timeframe within which a data controller should notify a data subject after getting knowledge of the breach. We recommend a maximum notification time of two working days. This notification should, wherever applicable, be done through multiple communication channels as per the contact details provided by the data subject. Besides, publishing of a breach on the website or in mass media may further put the privacy and data of a data subject at risk and potentially lead to further breaches to the privacy of the data subject. The mass media measures proposed in the Act should not be employed if any details about the particulars of the affected individual or of the nature of breaches are to be communicated. Instead, telephonic notification may be added to email and to last known residential or post address.

Section 23, DPPA, 2019 tries to enforce protection of data, it fails to clearly state the penalties that data controllers should face for contravening the law. It also does not mention the actions which would constitute failure to protect data and privacy such as negligence and unauthorized access and dissemination. The DPPA (Act) does not address protection of data collected by data processors or controllers operating beyond Uganda's borders but utilizing data belonging to Ugandan individuals or organizations. We recommend that a principle on jurisdiction be added in the Act and penalties indicated for any defaulters. The proposed clause should read as follows. "Personal data shall not be transferred to a country or territory outside Uganda unless

that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data". Lack of autonomy and independent oversight of intelligence agencies for example the oversight of lawful security acts should be a combination of executive control; parliamentary oversight; judicial review and monitoring by expert bodies. This is attributed to the fact that it is the president who holds the role of overseeing the mandate and operations of all of the intelligence agencies. The power to gather intelligence and conduct surveillance are concentrated around various institutions like the Uganda People's Defense Force (UPDF) and the Uganda Police Force (UPF). Therefore, through the institutions mentioned above, the President exercises control over sensitive intelligence operations while day-to-day spying for intelligence gathering appears less centralized. This is evidenced by the establishment of the 1987 Security Organizations Act which established the Internal Security Organization (ISO) and External Security Organization (ESO). These two agencies are directed by Director Generals appointed by and accountable to the president and exist to collect intelligence and provide advice on Uganda's security directly to the President. This therefore, puts the President at the center of controlling all issues related to data protection, it feels like biasness can prevail in the court ruling after being controlled by the President. Poor implementation of data protection law; Although the Data protection and Privacy Act was recently amended in 2019, Uganda still face challenges in protection of their privacy as it has been on going where most female prominent persons have been unveiled by the so-called finances which violates their rights to privacy and on top of that affects their health. To make matters worse, the compulsory SIM card registration and the retention of information about mobile phone users in a centralized database threaten the right to privacy in Uganda. SIM registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalized groups. It can also have discriminatory effect by excluding users from accessing mobile networks. While the proposed law is relevant to provide for and harmonize the process of collecting identification information, there are a number of loopholes around data protection and requirements for registration that arguably render it unconstitutional in its

current state. The Parliament of Uganda passed the Registration of Persons Act and it was signed by the President in February 2019; the purpose of the Act is to harmonize and consolidate the law on registration of persons in Uganda and to provide for the registration of persons.

Generally, the Act makes registration compulsory and it provides for cooperation with other agencies, government departments and ministries in sharing the information that is gathered. Therefore, while the law is a much-needed piece of legislation to provide for and harmonize the process of collecting identification information, there are a number of loopholes around data protection and requirements for registration which arguably render the DPPA Act unconstitutional in its current state. Parliament is well within its constitutionally mandated powers in making laws for peace, order, development and good governance but what cannot be justified is making laws that contravene the Constitution.

CONCLUSION.

In a nutshell, Uganda has tried to mimic the European Union's General Data Protection Regulation (GDPR) which requires EU member states to protect data usage and privacy rights of its citizens both within and outside the economic bloc hence on addition to the Data Protection and Privacy Act, 2019 of Uganda, the 1995 Constitution of the Republic of Uganda together with other legislations fall short of international data privacy best practices.

CHAPTER THREE (3).

ANALYSIS OF THE DATA PROTECTION ACT, 2019.

3.0. INTRODUCTION.

This chapter examines Uganda's data protection law, examining the statute in detail and identifying deficiencies. Data protection refers to the policies, safeguards, and legally binding procedures put in place to preserve your personal information while maintaining your control over it. In summary, you should be able to choose whether or not to share certain information, who has access to it, for how long, and for what purpose, and the option to change some of this information, among other things.

3.1. DATA PROTECTION AND PRIVACY LAW, 2019.

The long-awaited and much-needed Data Protection and Privacy Bill of 2018 was eventually signed into law by the President on February 25, 2019.The new Data Protection and Privacy Act of 2019 ("the Act") governs the acquisition, storage, processing, and use of personal data by various entities, including government agencies, enterprises, and private institutions operating both within and outside Uganda.

The **Data Protection and Privacy Act, 2019** puts into effect **Article 27 (2) of Uganda's 1995 Constitution as amended,** which ensures citizens' right to privacy. The law states that "no person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."

The **Data Protection and Privacy Act, 2019** also creates, criminalizes, and punishes specific activities that, when committed, constitute offenses under the terms of the legislation.

Finally, the DPPA Act directs the National Information Technology Authority-Uganda ("the Authority") to guarantee that all responsible persons/individuals comply with all terms of the Act. This legal warning is meant to inform all Ugandans about the basic obligations emanating from the Act, as well as to provide guidance on how to strive for compliance with the Act's provisions.

Interpretation;

The **DPPA Act**'s Interpretation section specifies a range of essential terminology that are central to understanding the new law's contents. Although we cannot reproduce all defined words, we have chosen key definitions for this alert. For example, data is defined as information processed by automated equipment following instructions. Personal data refers to information about a person that can be used to identify that person and is recorded in any form, such as nationality, age, educational level, and identity data.

The DPPA Act is consonant with Article 4 of the GDPR clearly define Personal data as any information relating to an identified or identifiable person referred to as a data subject and the case of **DURANT V FINANCIAL SERVICES AUTHORITY [2003] EWCA CIV.1746**, Personal data has been to mean all data that relates to an individual if it is information that affects a person's privacy, whether in his personal or family life, business or professional capacity.

A **data subject** is an individual from or about whose personal information has been requested, gathered, compiled, processed, or kept.

A **data controller** is someone who chooses the purpose and way in which personal data is or will be processed, either alone, jointly with others, in common with others, or as part of a legislative duty.

A **data collector** is a person who collects.

It is vital to note that one of the Act's key elements is the requirement and duty it puts on individuals or organizations that collect, manage, and control personal data.

These include data collectors/processors, data controllers, and anyone else who stores or uses personal data in their business.

Second, the Act outlines numerous rights that data subjects have with relation to the personal data gathered or processed.

In doing so, the Act prioritizes data protection and privacy as the most important rights to uphold.

As a result, companies that deal with personal data in order to conduct business must be well-versed in the principles, rights, and obligations outlined in the new Act for each party. According to the definitions above, these are data collectors, controllers, and/or processors. As a result, compliance with the Act's requirements will serve to prevent entities/persons from paying large monetary fines or jail sentences imposed by the Act.

What is likely more crucial to notice is that the Act applies to all mechanisms for collecting, processing, and regulating personal data? To that purpose, it makes no difference whether the personal data is gathered, processed, and controlled manually or using Information Communications Technology instruments like computer systems. When personal data is involved, one is instantly brought within the scope of the Act.

3.2. PRINCIPLES OF DATA PROTECTION AND PRIVACY ACT.

The primary goal of the Act is to protect data subjects' privacy and personal information. In order to do this, the Act specifies specific standards to guide organizations/individuals dealing with personal data. This includes:

Section 10 of DPPA Act prohibits a data controller, data processor, or data collector from collecting, storing, or processing personal data in a way that violates a data subject's privacy rights.

Second, **Section 13 of the DPPA Act** requires all data collectors to provide the following information to a data subject prior to collecting personal data.

The nature, classification, and purpose of data to be collected;

The name and address of the person in charge of collection.

Whether or not the data supply is mandatory or discretionary, as well as the availability of the right to access and request rectification of the gathered data.

The recipients of personal information;

If the data is not provided, what are the consequences?

The time period during which collected data will be held in order to achieve the objective for which it was collected.

The information provided above ensures that only acceptable and relevant personal data is disclosed to data collectors, and most significantly, it allows data subjects to make an informed decision before consenting to the collection of their personal data. As a data collector, you must bring the following facts to the attention of any data subject before collecting any data from them. Failure to do so becomes an infraction. Furthermore, as a precaution, a data collector/controller should attempt to explain and/or translate the preceding information to a data subject in a manner and language with which they are familiar. This eliminates the possibility of misunderstandings while also ensuring compliance with the standards of the Illiterates Protection Act, Cap.78, while dealing with illiterates. It is prudent to provide all sorts of data subjects with the ability to expressly consent, either through a click wrap agreement (for digital platforms) or physical signatures/thump prints for paper-based platforms.

It is crucial to note that **Section 33 (2) of the DPPA Act** specifies that it will be a defense in court proceedings if one can demonstrate that they took reasonable care in all circumstances to comply with the Act's obligations.

Third, **Section 3 of the DPPA Act** establishes data protection standards that all data collectors, processors, and controllers must adhere to in order to secure personal data. The data controller, processor, or person handling personal data must be accountable to the data subject, collect and process data fairly and lawfully, ensure data quality, collect relevant and necessary personal data, and retain it for the required period. Ensure transparency and participation of data subjects in collecting, processing, use, and storage of personal data, and maintain data security safeguards.

As a result, as a data entity, you must constantly guarantee that you follow the standards listed above when working with data. This further assures data subjects that there are controlling procedures/guidelines in place to monitor their activities while dealing with personal data.

ACTION STEPS TO BE TAKEN BY DATA CONTROLLERS, PROCESSORS AND COLLECTORS.

To protect and preserve a data subject's autonomy and privacy, the Act establishes a series of action steps that data collectors, controllers, and processors must follow. This includes:

CONSENT FROM THE DATA SUBJECT;

As a general rule, **Section 7 of DPPA Act** requires data collectors and processors to seek the data subject's consent before collecting or processing their personal data. However, the Act allows some exceptions to this requirement. They are:

Where such collection or processing is permitted or required by law;

When necessary for national security, public duty performance, or law enforcement.

The data controller may use personal information for contract fulfillment, medical purposes, or legal compliance. Data collectors and processors must obtain consent from data subjects before collecting or processing personal data, unless there are exceptions. Consent can be obtained through various means, including physical and digital methods.

For instance in case of **NALUBEGA.SHADIA VS. STABEX INTERNATIONAL LIMITED, CIVIL SUIT NO.665 OF 2021.** The provisions of the DPPA Act were tested when the respondent used the photos of the claimant without authorization.

Court made some remarkable conclusions like the fact that it is mandatory to acquire clear and unambiguous consent from a data subject before collecting or processing his or her personal data like photos as it was in this case.

Personal data relating to children;

The Act bans collecting or processing personal data of children unless agreement is obtained from the parent or guardian, or if it is necessary to comply with the law.

For research or statistical purposes;

This protects children from data entities that are likely to exploit and extort data from them when left alone. Furthermore, adults may readily lure and control children. In the realm of business operations involving children, data entities are allowed to gather relevant information, albeit under strict adherence to safety measures mandated by the law. However, data firms that conduct commerce involving children are entitled to acquire such data. However, this does not bar them from complying with the Act's safety obligations.

Direct Collection of Personal Data;

In accordance with **section 11 of the DPPA Act**, the data collector must collect the personal data from the subject directly.

There are certain circumstances that can be justified under paragraph 2 for the collection of personal information from another person or source, such as a public body. They include:

Where such data are already included in a public document;

The data subject intentionally made the data public.

The data subject has given consent to having the data collected from another source, and it is unlikely to affect his or her privacy.

The collection of data is required;

To prevent, detect, prosecute, and punish an offense

To protect national security

To enforce legislation that imposes pecuniary penalties or concerns the collection of public revenues, and to conduct proceedings before any court or Tribunal.

The consent of the subject is not possible to obtain.

This section shows the importance that the Act places on the autonomy and privacy of a data subject in relation to their personal data.

It is therefore obvious that in order to collect data from a different source, the collector will have to meet the requirements outlined in **section 11(2) (e) of the DPPA Act.** The reading of **section 11(2) (e) of the DPPA Act** shows that private entities/individuals may not be able to collect personal data from other sources for their own personal or commercial purposes, since the conditions appear to be limited to public-interest objectives.

The data collector must also be aware that the collection of personal data from another source does not relieve him or her of his or their responsibility to provide the information specified in **section 13(1)**, **DPPA ACT**. Prior to collecting the data, except where;

Information that relates to National Safety;

Information about the enforcement of laws that impose a financial penalty.

Information about the preparation and conduct of proceedings in a court, tribunal or other legal institution;

Information on the enforcement of laws relating to public revenue collection.

When it is important to protect the enforcement powers of an agency responsible for the investigation, prosecution, or punishment of a crime.

When data is collected in an indirect manner, data controllers, data collectors and data processors must create and formulate links to automatically send privacy and confidentiality statements to the data subject.

This is to reassure data subjects that their data, however collected, will be kept safe.

Collecting for a specific reason;

Data collectors must only keep and retain personal data as long as necessary to accomplish the purpose for which they were collected or processed. Every data controller, processor, and collector must therefore implement institutional practices to ensure that any personal data that has served its purpose is destroyed, provided that it does not violate other statutory requirements, such as the Income Tax Act. These system practices must be of high quality and security. They should be applied both in the digital and physical space.

In order to do this, a data retention policy should be defined with defined retention periods that are known by the data subject in their personal information. After the specified retention period, digital data should be deleted or physical files with personal data destroyed using secure methods.

Specific Personal Data;

Section 9 of the Act prohibits the collection or processing of certain personal data. The Act prohibits the collection and processing of personal data, including;

- Anything that relates to religion or philosophy.

-Political opinion

- Financial and sexual information

- The health status of an individual or their medical records.

The exceptions include data collected under the **Uganda Bureau of Statistics Act** and data collected by an employer in order to perform a legal obligation. These data must be freely provided and consented to by the data subject.

Data processors and data collectors who collected such data before this law, and fall outside of the exceptions allowed by this law, should cease such practices. If this is not done, it would be an offense and a violation of the Act.

The **DPPA Act**, while mentioning the possibility of collecting such information for a legitimate purpose, does not define what "legitimate activity" is. This means that every organization should consider their core mandate or activities before collecting any of the prohibited personal data. A religious organization may collect data on a person's religion, while a political party can gather information about a person's political views and not their religious beliefs.

Keneth. Muhangi in his article **"OVERVIEW OF DATA PROTECTION REGIME IN UGANDA."** States, "*On the basis of this provision (Section 9, DPPA), it is prudent to note that some data analytics companies like Cambridge Analytica that profile data subjects for profit may not be able to operate legally in Uganda. For Ainstance, in Nigeria, a UK newspaper, The Guardian reported that Israeli hackers provided CambridgeAnaltytica with President Muhammed.Buhari's personal emails. The emails that included information about Buhari's ill health and medical records were leaked in order to dissuade voters and to weaken Buhari's campaign.*"

Minimalism and quality of the information;

The **sections 14 and 15, DPPA ACT** state that controllers and processors of personal data are only required by law to collect and process the data necessary for their specific purposes.

Both data entities and the data subject must make sure that the personal data they collect, process or render is accurate, complete, and not misleading.

Security Measures;

Part IV of the DPPA Act outlines the security measures to be implemented by data controllers/collectors or data processors in order to protect personal data.

As almost all data entities are both physically and online present, it is important to understand that the Act's security measures apply to both digital and physical security.

In implementing security, the data controllers, collectors or processors should implement measures to ensure the safety of the physical space in which any personal data may be held or stored (physical or digital) and any technical security for information communication systems in which personal data is held. They include:

Section 20 of the DPPA Act states that a controller/collector/processor must ensure the integrity of any personal data in their possession. Adopting reasonable and appropriate measures can help prevent loss, destruction, unauthorized access, and unlawful processing.

A data controller must take the following security measures:

Identifying reasonable external and internal risks to the personal data that you have in your possession.

Set up and maintain adequate safeguards to protect against identified risks

Verify regularly that the safeguards have been implemented effectively.

As new risks or weaknesses arise, ensure that safeguards are updated.

Section 21, DPPA ACT requires that data controllers ensure , before processing any personal data by the data processor, that the security measures highlighted above have been adhered to.

The **National Information Technology Authority of Uganda's (NITA-U) Guidelines** for Operation Usage and Managed of Information Technology Infrastructure by MDAs and Local Governments is a useful starting point for the implementation of some of the digital security measures. These guidelines include some examples of practical security measures.

Installation of access systems at the locations where IT equipment sites or rooms are located; alarm systems, security cameras, intrusion detection systems and other

measures. A data controller must also adhere to generally accepted security procedures, rules, and regulations.

Here are some generally accepted information security procedures and practices that data controllers and data processors can adopt and utilize in relation to both digital and physical data.

Keep hard copies of your personal information in rooms or containers that are only accessible to authorized personnel.

Configuration of systems and networks in a secure manner;

Use tools such as WinZip or PGP to encrypt your personal data sent via email.

Information Security Incident Management

Regularly perform risk assessments to identify and assess the likelihood and risk of information security threats that may affect confidentiality and integrity.

Install firewalls licensed in hardware or software on your network and desktops.

Configure your firewall to deny all connections by default;

Define the process of granting or revoking access to physical facilities that store or process personal data based on approval by appropriate management.

Install Active Directory with user-access controls and restrictions known;

Visitors must also be accompanied on site by staff from the data controllers, processors or collectors and be identifiable at all times (e.g. Visitors should always wear visitor badges.)

Breach in security;

In addition, in the event of a breach of data security due to an unauthorized acquisition or access, the Data Controller/Collector/Processor should immediately report the incident to the Authority. The Authority will determine whether or not the data controller/processor/collector should notify the subject of a data breach. If the

authority considers that such a notice is appropriate, it will be given by any of the methods specified under the Act depending upon the circumstances.

When notifying the Authority about the unauthorised access, the controller/processor/collector should provide enough information regarding the breach.

In addition to the above, some data subjects may have a specific timeframe in which they require that a controller/collector notify them about a breach of personal data. The data controller/collector must adhere to these time limits in order not to breach their contract/agreement with the data subject.

The Authority may also direct that the controller/processor/collector publicizes the breach in a certain way if it believes the publicity will protect the subject.

Data controllers, processors, and/or collectors of data should develop and implement a plan for managing incidents involving information security. The plan should also include the following:

Information security incidents: Definition

Roles and responsibilities for personnel in relation to incident management

Protocols and contacts to report and resolve information security incidents.

Data subjects' rights; Data subjects are the primary and main source of personal information. They enjoy a variety of rights under this Act. These rights are all designed to protect data subjects and ensure privacy of their data.

Accessing personal information;

After proving their identity according to the Act, they can request that a data controller grant them access to any personal data. The request can include confirmation of whether or not the data controller holds personal data on the particular data subject. It may also contain information about the type of data, and who accessed them.

In **section 24, DPPA ACT.** The data controller is required to refuse a request from a data subject if the information provided is not sufficient about the identity of the data subject and where they are located. It ensures the data subject is the one who receives the data. It also prevents fraudsters and impersonators from accessing the personal data of other people.

A data controller cannot comply with a request from a subject if they can't release the data requested without disclosing another person's information, unless:

The other person consents to disclosure.

If the request is reasonable, the answer will be yes.

A court order is required.

The data that is referred to in the above paragraph is data that identifies a third party as the source of data the controller believes will be obtained by the person making the request.

A data controller may not, however, use paragraph 4 to refuse certain information that can be released without revealing the identity of another person. He or she can use their expertise to release requested data while excluding information that discloses the identity of another person.

A data controller must comply with the request of a data subject for information within thirty (30) calendar days.

This section contains several qualifiers that show the importance of the Act in protecting the privacy and security of personal information, both for the data subjects themselves as well as any third parties who may release their data to an individual.

To comply with the Act, it is important that data controllers and collectors invest in systems and procedures to facilitate the retrieval and accessibility of any collected or requested personal data.

Right not to process personal data;

The data subject can notify the data controller or processor by writing at any time that they no longer wish to have their personal data processed if it causes them or is likely to cause them unwarranted damage or distress.

Second, the controller must inform the subject within fourteen (14) calendar days after receiving the notice that the data subject has complied with the law, intends to do so, or gives the reasons why they have not complied. The notification must be written. The Authority will receive a copy of any notices where the controller has given reasons for not complying. If the Authority is satisfied that the data subject's complaint is justified, then it will direct the controller to comply with it within seven (7) working days.

Even after the collection of personal data, this provision guarantees that a data subject has a right to or control over those data.

Right of correction/ deletion or destruction of personal data (The Right to Be "Forgotten");

"The right to be forgotten was first introduced by the European Court of Justice in a case involving Google Spain, where the ECJ affirmed that data subjects have a right to be forgotten and held that Google must delete inadequate, irrelevant or no longer relevant data from its results when a member of the public requests it."

Section 16 DPPA ACT permits data subjects to correct their personal data as needed. This provision allows for data subjects to request that their personal data be corrected, deleted, or destroyed by data controllers. The data may be outdated, excessive or whose original purpose is no longer valid. Or, the data controller does not have the right to keep it. For instance in the case of **FLOOD VS. TIMES NEWSPAPER LTD. [2010] EWCA CIV 804**, *a police officer was accused in a newspaper article, of taking bribes from Russian exiles with criminal connections. The article was printed in the paper edition of the Sunday Times and was also made available in its entirety online. Approximately a year after the article was first published, a report cleared the police officer of any wrongdoing and held that online archive of the story must be updated to take account of exculpatory developments.*

The right to "forget" has been named. If the controller cannot meet the request of the data subject, it will inform them and explain the reason for their decision. The DPPA Act grants the Authority the power to order that a data controller rectify or rectify data, block data, destroy data, or erase it if the complainant is satisfied. Data controllers and collectors must invest in systems and processes that enable the correction or deletion of personal data as needed.

After the data collection purpose is completed, data controllers must also develop standard retention policies. Data controllers/processors should make sure that their policies do not violate statutory laws on data retention.

Uganda currently does not have an integrated national policy for data and records retention that covers all sectors.

Data retention policies, also known as records retention policies, are the established protocols of an organization for retaining data for operational, or other purposes. The policy allows the users of the organization to organize their information in a systematic way, so that it can be accessed and searched later. It also allows them to dispose off old data once they no longer need it. These policies are implemented between the organization's different customers who will be collecting and using personal data.

In addition to physical backups, a good retention policy will include electronic data backups (such as cloud computing). It is better to have the latter in case of destruction.

A data retention policy should also consider the evolution of the value and retention laws that an organization might be subjected to. In 2006, The U.S. Supreme Court acknowledged that it was not possible to keep all data indefinitely.

Organizations must, however, demonstrate that only data not subject to regulatory requirements is deleted and that this process is repeatable and predictable. This means that different types of data are stored for varying lengths of times. The hospital may have a different retention period for its employee emails than it does for patient records.

The following laws in Uganda have specific retention provisions for certain data categories.

The Anti-Money Laundering Act of 2013 (AMLA);

According to Section 7 of AMLA, a person accountable must keep records of an individual's real identity for 11 years and at least 10 years after the conclusion of a business relation. AMLA criminalizes failure to comply with above provision.

The Insurance Act of 2017 (I.A.): According to section 106(2) of the I.A., licensees or former licensees must keep financial statements as well as other records pertaining to the year for which they were issued. In the same way, failing to comply with this provision is an offense under the I.A punishable with a heavy fine.

The Authority's mandate is to monitor and evaluate the activities of the data controllers with respect to the retention periods for personal data. However, its powers are not greater than the retention provisions of various laws.

Erasure, deletion, blocking and rectification of personal data. The Authority can also order that the data controller rectify, update or block certain data if it finds out from a complaint of the data subject that the data are inaccurate. This right applies whether the data are accurate records of information obtained or received by the controller from the subject or third parties.

If the Authority finds that the data is inaccurate, it will instruct the data controller to correct the record with the information deemed appropriate.

The data controller must notify third parties who had previously been disclosed the data of the upgrade once the complaint has been resolved.

As a result, the parties who have access to personal data can stay up to date with any changes or updates made to that data. This is because it is subject to frequent change. This also prevents data entities using or relying upon inaccurate or outdated information that could be harmful to the entity as well as the data subject.

Right not to process data for direct marketing;

Section 26 of the DPPA Act gives data subjects greater control and power over how their data is collected, and ultimately used. They also have the right to view their data. The Act prohibits data controllers using data subjects' data for marketing without their consent. This provision applies when companies collect personal data about an individual for a specific purpose, and then use that data for marketing without the consent of the individual. Direct marketing is any form of communication directed directly at an individual, including advertising and marketing materials.

This is common with companies sending unsolicited for promotional/marketing messages to the data subjects. Often, these messages are sent via email or phone numbers. A data subject may be charged a fee if they receive information above that wasn't requested.

A data subject can request that a controller stop processing their personal information in the above circumstances. The data subject as well as the authority must be informed if a controller refuses to comply with a request. If the Authority is satisfied with a request, then it will direct a controller to follow suit. It is important to remember that a person can enter into an agreement for the use of their personal data in order to receive monetary benefits. In order to comply with this law, companies must include an opt-in option in their documents, so that the data subject can decide whether they wish to receive promotional material.

Second, it is important to include a "unsubscribe option" so that the user can decide how long he or she wants to receive marketing information.

Data controllers must not assume that because a data subject has received a certain service, that they will be interested in their other services. SOtherwise, they may suffer the consequences.

Rights relating to automated decision making;

Section 27 of the DPPA Act prohibits a process whereby decisions are made primarily using automated methods without human involvement. The Act provides mechanisms to protect individuals from data controllers who make decisions solely on the basis of

automated means. A data subject can write to the data controller to ask him to make sure that the decisions affecting them are not made automatically.

However, if a decision which significantly affects the subject is solely based on an automated processing, the controller must inform the subject as soon as possible.

A data subject can request that the controller reconsider an automated decision by sending a written notification.

After receiving the above notification, the data controller has twenty-one (21) days to reconsider the automated decision. They must inform the data subject by writing of any steps they have taken or will take to comply with this notice.

If the data controller's efforts to comply with the data subject's notice do not meet his or her expectations, the person must file a complaint with the Authority within fourteen (14) calendar days.

The Authority is the final arbiter of whether a controller has taken the necessary steps to comply with the notice given by the data subject.

A decision can be taken automatically in relation to;

The process by which a data subject enters into or performs a contract;

To a lawful or authorized purpose.

As a data controller you should identify those decisions which are likely to be made using automatic processing methods.

Inform the data subject about automatic processing.

Introduce and inform data subjects about simple ways to involve humans in decision-making, such as granting access to automated decisions to allow data subjects to review any accuracy issues;

Add additional organizational and technical measures to enable human interaction with data

Inform the data subject about the data that is used to make decisions.

Introduce simple steps to challenge a decision made solely by an automated system that has a significant impact on a data subject.

Perform data protection impact analyses (DPIAs) before using automated decision-making methods and address any issues identified.

Data controllers must implement system checks to protect children and other special groups from being subjected to automated decisions.

Penalties and offences;

The Act's last chapter creates offences that are punishable by both incarceration and fines for any data processor or collector found guilty. They include:

Unlawful disclosure or obtaining of personal data

The destruction, deletion or concealment of personal data without authorization;

Sale of personal data;

All of the above offences are punishable by a prison sentence between 10 years and higher, or a fine of up to 240 currency points.

Compensation for Damage or Distress;

A data subject may be entitled to compensation under section 33 for damage or distress caused by the contravention of the Act's provisions by the data controller/processor/collector, responsible party, once and a complaint has been determined by a competent court.

3.3. Conclusion

The Data Protection and Privacy Act's provisions also apply to the processing of data outside Uganda. The responsible data controller/processor/collector should make sure that the country in question has implemented measures to protect such personal data. The Data Protection and Privacy Act is a step in the correct direction, but it will

take time to taste its fruits. A good law is needed to protect this resource. The Act, as can be seen, creates a variety of opportunities and challenges for a wide range of people. However, there is a need to change the culture of work, processes, and systems among data collectors. To begin with, they should invest in the technology and infrastructure that will allow them to comply with the Act's numerous provisions. Data collectors, controllers and processors must also adopt policies such as Security Incident Management Policy, Data Retention Policies, and others that will guide them in achieving compliance with the Act.

CHAPTER FOUR.

RECOMMENDATIONS AND CONCLUSIONS.

4.0. INTRODUCTION.

In an era marked by rapid advancements and evolving challenges, research serves as a cornerstone for informed decision-making and progress. With this ethos in mind, the following recommendation stems from a comprehensive research endeavor aimed at addressing **THE EFICACY OF THE DATA PROTECTION AND PRIVACY, 2019.**

4.1. Recommendations.

Recommendations for improvement in the Computer Misuse Act of Uganda; Establishment of Access to Open Data;

The open data platform shall be accessible through GoU (Government of Uganda) open data portal. This therefore means that not all data shall necessarily be held on the portal, but it shall be a mean of signposting people to the data they require. The portal shall be designed with both technical and non-technical users in mind and shall adhere to open standards. Data Presentation by dataset owners; All dataset owners shall publish their data in non-proprietary formats such as comma separated values (csv). Additionally, in consultation with the open-source policy and to the extent

permitted by law, public bodies shall prioritize the use of open formats that are non-proprietary, publicly available, and that place no restrictions upon their use.

Opening access to data also encourages public sector efficiencies and savings through reduced duplication, streamlined processes, and the development and delivery of tools/services more quickly and at lower costs.

Focus should be emphasized on open data policy; Implementation of open data initiatives is expected to bring about a number of benefits that includes, better management and use of data within government and enabling broader access and use for example by non-government organizations, businesses and industry, academia, innovators and civil society provides a range of benefits to both the public and private sector. Enabling participatory governance; increased access to government data which provides the public with greater insight in to government activities, service delivery and use of public resources.

Support for innovation should be re-enforced to help internet users access knowledge resources in the form of data support and innovation by reducing duplication and promoting reuse of existing resources. In the long run it can create new opportunities for economic growth, new business and jobs.

Recommendations to the government;

Copyright and Intellectual Property Rights should be enforced; To ensure clarity on who can use data and for what purposes, unless otherwise stated the users shall be free to copy, publish, distribute, adapt and exploit the information commercially or otherwise so long as they acknowledge the source of the information via an attribution statement. Feedback Mechanisms should be encouraged;

Public sector bodies shall publish their data in as raw a form as possible with any errors or limitations with the data noted in the metadata. Feedback lops on data quality shall be developed via the open data platform. This shall facilitate users to

submit comments and feed back to data publishers to drive improvement in the data over time.

Updating of published datasets should be encouraged;

Many open data initiatives which are initially successful in publishing data subsequently fail due to data not being refreshed. All datasets published on the open data platforms shall be mandated to be refreshed according to the schedule stated in the associated metadata record. Further restricted data that shall not be released for example personal data due to the fact that the public sector holds citizen data to conduct business with the citizen and deliver appropriate services.

Governments' effort shall be made to create a permanent and lasting access to time stamps of data by creating an archiving policy that is aligned to the provisions of the National Records Policy.

Government shall add an open data component to the development of essential data e-government systems. Promote the use of open government data in solving society challenges. For instance, partner with innovation hubs in Uganda to transform open government data into new economic opportunities.

Further it is recommended to implement data monitoring and feedback system to measure increased efficiencies from publication of open data and identify demand for additional data.

Recommendations to the Ministry of ICT and National Guidance;

The Ministry of ICT and National Guidance shall issue guidance for all media platforms to publish open data consistent with best practices and establish high-level commitment; ensure that the ICT staffs have adequate technical skills to implement open data like acknowledging of open data standards, metadata and database management.

Ministry of Justice and Constitutional Affairs;

The Ministry of Justice and Constitutional Affairs (MoJCA) shall provide legal advice and legal services to Government with regard to cybercrime; provide technical guidance and support to the development of a comprehensive legal framework for cybercrime.

Further it should conduct a full due diligence review of existing legislation regulations and policies relevant to open data to identify gaps and inconsistencies. Provide legal advice to their Agencies regarding confidentiality and privacy to accomplish gender equality in regard to privacy.

Uganda Communications Commission;

Uganda Communications Commission (UCC) shall among others regulate the release and circulation of data/information across telecommunications, radio, television and postal and courier services industry.

Create partnerships with telecommunications providers, intermediaries and businesses to help provide access to data in rural and low-bandwidth areas.

National Information Technology Authority (NITA-U);

The National Information Technology Authority Uganda (NITA-U) shall establish a centralized online portal to provide a single listing of all available open data. Provide Data Hosting Services for Agency Data sets.

Initiate partnerships with developers and innovation hubs to begin to unlock the economic value of open data in Uganda issue the Government Enterprise Architecture and interoperability Framework for utilization to maintain interoperability, data standards and processes related to data management.

General recommendations;

Government, citizen, academic, and the private sector shall ably work together and collaboratively find new answers to solve societal problems using available open data from previously conducted studies. Therefore, an open data steering Committee and Technical Committee shall help to improve the interoperability and openness of government information. The Committees shall focus on leveraging government-wide communities of practice to help with the development of tools that support information interoperability and openness. Part of this work shall be to share best practices related to interoperability and openness within. These collaborations shall be subjected to statutory limitations and conducted in a way that fully protects privacy, confidentially, confidential business information and intellectual property rights.

4.2 CONCLUSION.

From the findings of the study, although it is new, the law on Data Protection and Privacy, 2019 of Uganda provides for the much-needed protection for personal identifiable information which is a key in this digital age. It provides important safeguards that will protect Ugandan citizens as they use online services. This law also provides many avenues to facilitate growth in IT sector for example the law makes it possible for Ugandan players to comply with international standards, improving credibility and customer trust, which inevitably leads to more business. The new law goes a long way in making more secure Uganda's cyber space.

BIBLIOGRAPHY.

STATUTES.

1995 constitution of Republic of Uganda as amended.

Data Protection and Privacy Act, 2019.

Anti – Money Laundering Act of 2013.

Insurance Act of 2017

CASES.

Charles. Onyango. Obbo & Andrew. Mwenda Via. A.G (Constitutional Petition No.15 of 1997)

King Via. Therens [1955] S.C.J. NO. 30, IBC.C.C. (3rd) 48 1.

Green Watch (U) Ltd Vs. A.G & Anor [2002] UGHCCD 23.

Major General Tinyefunza Vs. A.G [1997] UGCC 3.

Zachary. Olum & Anur Vs A.G (Constitutional Petition No.6 of 1999)

Jim. Mchwezi. Katugugu Vs. Patrick. Kiggundu & Anor (Constitutional Petition No. 7 of 1993).

A.G Vs. Chief Editor Monitor Publications Ltd & Anor (Misc. Application No.6 s of 2002.

Paul.K. Ssemwogerere & Anor Vs. A.G (Constitutional Appeal No. 9 of 2002.

Victor Juliet Mukasa & Vvonne. Oyo Vs. A.G, Misc. Couse No. 21/06.

Bank of Credit and Commerce International S.A Vs. A boody [1992] 2 ALL ER 95.

Durant Vs. Financial services Authority [2023] EWCA C.x. 1746.

Nalubega. Shadia Vs. Stable International Limited Civil Sut No. 665 of 2021.

Flood Vs. Times Newspaper Ltd [2010] EWCA CN 804.

BOOKS AND JOURNALS.

Halsbury's Law of England, 'The Data protection principles and the seventh Data Protection Principles, Confidence and Data protection' volume 8(1) (2018).

Hoven, J, (eds) Information Technology and Moral Philosophy Cambridge University Press, Privacy and the Protection of Personal Data in Weckert, 2008, p.311.

Lallali S. et, "A secure Search Engine for the Personal Cloud". In: Proceedings of the 2015 International Conference on Management of Data, New York, USA: ACM, 2015, pp. 1445 – 1450.

Mandy , p. Webster, 'Data Security and Outsourcing', Company Secretary's Review, Issue 21, February 2019.

Mark, Turner and Nick Pantlin, Financial Services in the cloud', Journal of International Banking and Financial Law Volume 26/Issue 2, February 2011.

Richard, Holis. 'Data security part 1 five factors leading to Data Compromise Privacy and Data Protection', Volume 10, Issue 2, December 2018.

Richard, Holis. 'Data security Part 2 five factors leading to Data Compromise Privacy and Data Protection', Volume 10, Issue 3, February, 2010.

Solove, D.J, Understanding Privacy Harvard University Press, 2008,p.196.

Stewart, Room, 'The changing face of data security law' Journal of Privacy and Data Protection, Volume8, Issue 7, August, 2018.

The Economist 'Is Cloud computing secure computing?' April 23rd – 29th 2011.

The Sunday times, December 7 2007.

Thompson, C, "Brave New World of Digital Intimacy', New York Times, 5 September 2008.

Tim, Wright and Dominic, Hodgkinson, 'Government response to House of Lords Science and Technology Committee Report on Personal Internet Security', Computer and Telecommunications Law Review 2008.

Warren, S.D and Brandeis, L.D. the Right to Privacy Harvard Law Review Boston 5 Dec 15; 2010.

Wax, S.T. and Schalz, C., J. , A Multitude of Errors; The Brandon Mayfield Case National Association of Criminal Defense Lawyers, 2010.

Westin, A; Privacy and Freedom New York NY, Atheneum 2017.

Xiao H, et al. "Is feature Selection secure against Training Data Poisoning?" In: Proceedings of the 32nd International Conference on Machine Learning (ICML-15), 2015,pp. 1689 – 1698.

Zurich, Internet of Things, International Conference for Industry and Academia, March 26 – 28 2008.