Data protection and Privacy Act, 2019

Table of Content

List of acronyms

CCTV	Close Circuit Television
DPPA	Data Protection and Privacy Act
NIRA	National Registration and Identification Authority
NITA	National Information Technology Authority
NSSF	National Social Security Fund
UCC	Uganda Communications Commission
URA	Uganda Revenue Authority
UW	Unwanted Witness

1.0 Introduction

This analysis examines Uganda's Data Protection and Privacy Act, 2019 (DPPA). It assessed the Act against international recognized data protection standards, and national human rights obligations, and makes recommendations on how the enforcement of law should be improved through the adoption of regulations and possibly amending some areas of the law. The assessment is aimed at helping state and non-state actors determine the adequacies of the Act and establish areas of improvement.

Data processing has been a major concern for the information age where a lot of data is being generated and processed by a growing number of actors, and the lack of effective and enforceable regulations means that there are risks that this data could be abused resulting into not only infringements of the right to privacy but also other rights such as property rights with varying consequences. Many countries around the world have take steps to regulate the processing of personal data by both public and private entities with the aim of protecting people and their data from various risks. Uganda's DPPA aimed at achieving the same objectives and this briefing assesses whether the DPPA meets human rights standards, and internationally recognized data protection standards and principles.

2.0 General background to the DPPA

The DPPA was assented to by the president of Uganda on the 25th of February 2019. The law comes against a background of several debates and arguments on what should or should not be included. Since the presentation of a Bill in 2014, Unwanted Witness (UW) has engaged with the government, the parliament and other stakeholders to provide research and analytical briefings on the Bill.[1] A number of recommendations put forward by UW and their local and international partners were included in the Bill; however major gaps remain.

The DPPA aims at protecting the privacy of individuals and of personal data by regulating the collection and processing of personal information. It also seeks to provide for the rights of persons whose data is collected. the Act applies to collection, holding and using personal data within Uganda and data collected outside Uganda relating to Ugandan citizens.

As it comes into force, the law will need to be tested against accepted international standards as well as matching the local situation in Uganda to consider its adequacy and gaps that may exist.

The DPPA is divided into 8 parts covering preliminary, principles of data collection and processing, security of data, rights of data subjects, data protection register, complaints and offences. The different parts provide for administrative and sanctions on the application of the law.

An on-going concern with the accountability and enforcement mechanisms provided for under the DPPA is that the Authority, responsible to oversee the enforcement of the law, is defined as the National Information Technology Authority (NITA). The DPPA creates a Data Protection Office (DPO) under the NITA, whose role to oversee the overall enforcement of the DPPA. The National Information Technology Authority – Uganda (NITA-U) does not

[1] https://www.unwantedwitness.org/wp-content/uploads/2018/02/Submission-of-Comments-on-the-Data-Protection-and-Privacy-Bill-2015.pdf

constitute an independent authority given it is under the general supervision of the Minister of Information and Communication Technology (MoICT). The NITA-U Board of Directors, which is the supreme governing body of NITA-U, is appointed by the Minister of Information and Communication Technology and constituted as the governing body of the Authority.

This means that the Act fails to establish of an independent data protection authority to supervise the way in which a body or an individual uses other individuals' personal data. This body is essential in order to ensure the enforcement of the data protection framework, and also to ensure trust in the system. This will be an area to monitor closely moving forward, and which will have to be addressed through other measures.

The DPO is charged with enforcing the DPPA and specifically to;

a. Oversee the implementation of the DPPA
b. Promote the protection and observance of the right to privacy and personal data
c. Monitor, investigate and report on observance of the right to privacy and personal data
d. Carry out sensitization on the DPPA
e. Investigate cases of violation of data protection and privacy
f. Maintain data protection register among other functions.

It should be noted that the DPPA generally lacks civil and penal sanctions for violations of the law and of the orders made by the DPO. This in effect will make it difficult for the DPO to carry out some of the functions above. For example, where the DPO investigates and finds a breach of the law or data protection principles, it is not clear how its orders will be enforced after such a finding. It is also not clear where the DPO will submit its reports and the purpose of reports once made.

Data is defined as information which processed by means of equipment operating automatically in response to instructions given for that purpose or is recorded with the intention that is should be used or processed[2]. A data collector is a person who collects data.

The law has several other definitions, however a few key provisions and words are not defined as we shall see in the sections that follow. Below is the assessment of different aspects of the Act.

3.0 Data protection principles

Data protection principles are provided for under part II of the DPPA. It provides for duties and responsibilities that a person or entity holding data shall comply with. Superficially the DPPA provides that a person holding data including a data collector, processor, controller or any person who collects, processes, holds or uses data shall follow the set principles. The principles of data protection under S. 3 include

1. Accountability to the data subject
2. Fairness and lawfulness
3. Adequacy and relevancy of data
4. Use of data as authorized by law
5. Ensuring quality of information collected, processed or held

[2] See S. 2 of Data Protection and Privacy Act, 2019

6. Transparency and participation of data subject
7. Ensuring safety and security of the data

When reviewing the above principles, it is clear that there are a number of good provisions though a number of gaps exist. Generally, the law legislates for the basics of data protection and to ensure the processing of personal data is regulated and data controllers and processors have clear obligations to protect people and their data. The actual implementation of the law may depend on willingness of public and private entities to follow the principles and obligations set out in the law. The DPPA does not have specific provisions to provide for civil or criminal sanctions in case of breach of the principles or other aspects of the law. This not only undermines the principles but also the provisions of the Act. Below is a review of the different principles set in the DPPA

3.1 Accountability to the data subject for the data collected.

Accountability requires that the data collector, controller or processor is able to put in place measures that will ensure that data is held, processed or otherwise used with respect to data protection principles.

Beyond S 3(1) (a) which provides for the accountability principle, a review of the DPPA shows that there are limited specific provisions outlining the requirement of the data collector, processor or controller to demonstrate compliance with the law. Important organisational measures for demonstrating compliance include data protection/ privacy impact assessments, appointment of data protection officers, data protection/ privacy by design and by default requirements and record-keeping obligations. The above may affect integrity of data processing system and undermine general accountability.

The DPPA does not have provisions that compels a data collector, controller or processor to inform the subject of any changes or risks that may happen to the data once it is held, including informing the data subject of the measures being taken to ensure data is safe. S. 23 provides for informing the authority of the breaches and remedies taken. Much as this is good, it only provides for a one-way accountability where the data controller or processer is only accountable to the Authority and not to the subject whose data may be at risk. There is no obligation to inform the data subject of any breaches that may happen.

The DPPA fails to provide clear requirements for data collector, processor or controller obligations to demonstrate how they are complying with the law and the lack of provisions mandating the data collector, processor or controller to inform the data subject in cases of breach undermines the key accountability provisions and standards in the law.

3.2 Lawfulness and fairness of data collection

The principle of lawfulness and fairness is at the core of data protection. It requires any data processing activities by a data collector, controller or processor must be undertaken in a way that respects of rule of law and that meets a legal ground for processing.

The DPPA, 2019 does not specifically point out areas that maybe lawful or unlawful in collection of data. It provides under S. 3 that data must be collected or processed lawfully and fairly. S. 7 requires that consent, as defined as ‘freely given, specific, informed and unambiguous’, must be obtained from a person before data is collected.

However, S. 7(2) provides for broad exceptions to collect personal data without consent. It is an exception to the general rule of consent. It provides that:

(a) Data will be collected without consent where it is required by law
(b) Where the collection of data is necessary for public use
(c) For national security
(d) For prevention, detection, investigation, prosecution or punishment of an offence or breach of the law
(e) For performance of a contract where the data subject is a party
(f) For medical purposes

Much as some of the exceptions such as national security, investigation and prosecution of offences are important and accepted exceptions in a free and democratic society, the provisions of S. 7(2) have excesses and could potentially be abused. For example, provisions allowing collection of data for medical reasons may be abused to collect all forms of private data without consent from the holder. This is the case despite the fact in normal medical practice medical workers seek consent to treat a person and where such a person is unable to consent such consent is sought from the next of kin. The law should have provided for such parameters to avoid abuse of such discretion.

On the other hand, fairness involves processing must be done in ways that people would reasonably expect and not in ways that have unjustified adverse effects on them[3]. To determine fairness, one has to look at the process of obtaining data and using the data[4]. Access and processing of data must not be misleading or detrimental to the data subject. There should also be informed consent on subsequent processing of data beyond what it was acquired for and such subsequent processing should be in line with the original purpose for which the data was acquired.

S. 8 of the Act prohibits collection of data of a child without consent of the child's guardian or parents. This is important in as far as promoting the principle of fairness is concerned. Related to the above

3.3 Purpose limitation

Purpose limitation is provided for under S. 3(1)(c) which provides that a person must collect data that is adequate, relevant and not excessive or unnecessary. What is necessary and relevant is determined on a case by case basis. It can depend on purpose of the data being collected. This principle is necessary in preventing unnecessary intrusion and potential violation of the right to privacy.

S. 14 provides that a data controller or processer shall only process data that is necessary or relevant and such data shall not be excessive or beyond what is authorized by law. The provision is important in as far as it promotes minimality principle of data protection. This will ensure data is not abused and the data collected is in line with purpose and use.

[3] Lydia F de la Torre (2019) What does "lawfulness, fairness and transparency" mean under EU Data Protection law? Available at https://medium.com/golden-data/what-does-lawfulness-fairness-and-transparency-mean-under-eu-dp-law-a385d249d754 accessed on 28th April 2019
[4] ibid

3.4 Retain personal data for a period authorized by law

Personal data should only be retained for the period of time that the data is required for the purpose for which it was originally collected and stored. This will strengthen and clarify the obligation to delete data at the end of processing, which should be included in another provision.

However, it is important to consider how this principle interacts with other data retention requirements provided for in other laws. There are a number of laws that require keeping of data for specific period of time. For example, the Anti Money Laundering Act, 2013 requires that data collected for purposes of Anti Money laundering shall be kept for a period of not less than 10 years, while taxation, company and other laws require keeping data for a period of not less than 3-5 years.

It should be noted that the DPPA does not provide for a specific period for which data should be kept. In order for individuals to be fairly informed about the processing of their data, they must be informed how long their data will be retained. It is encouraged that the Authority provide for further guidance on data retention for data controllers and processors, and data controllers should establish retention schedules specifying the retention periods for all the data that they hold.

The DPPA provides for the main internationally recognized principles which encompass principles adopted in many countries in ensuring protection of data. However, the fact that the law does not sanction the violation of these principles and lacks a general offence for situations that may arise in the process of handling, collecting and processing data means it may not be effective when it comes to implementing the principles and provisions meant to support the data protection principles.

4.0 Rights of data subjects

The DPPA provides for the rights of data subjects under Part V. These rights provide data subjects with mechanisms to control the processing of their data. They help data subjects determine how their data should be used while at the same time placing obligations on the data controller or processor to ensure their data processing activities are lawful. They also are important in avoiding abuse of data and ensuring protection of privacy.

Under S. 24 a data subject has a right of information and to access. A data subject has a right of access to information relating to their data. The DPPA provides that such a person has to identify themselves before the data is provided. It provides that the Minister responsible for information and communications technology shall make forms to provide for how such information shall be accessed.

This right is important in as far as it gives the data subject the right to access data about themselves which is being processed by a data controller, and get copies of this data including accessing results of processed data about the data subject by him/herself.

However, the DPPA provides for exceptions to the principle of access to information. It allows situations where a third party can access information held by a data controller or processer. This can happen where the data subject has provided consent to the access of such data. The other exception is where it is reasonable in the circumstances to give data to a third party

without consent of the data subject[5]. This provision can easily be abused where personal data is given to third parties without consent of the data subject.

This may violate the person's right to privacy. The provision can be considered unconstitutional since article 41 on the right to access to information prohibits accessing information that may result in violation of a right to privacy of a person.

A data subject has a right to prevent the processing of personal data where such processing of personal data is likely to cause unwarranted damage or distress to the subject[6]. In order to exercise this right, the data subject is expected to apply in writing the person holding the data mainly data controller or processor requesting the that he/she stops processing the data. This is an important in as far as protecting the data subject is concerned. Once a request is made, the data controller or processor has 14 days to inform the data subject of the action they have taken. The data controller may be asked to edit, erase, stop processing the data in question, however, the data controller, processor or person holding data has the discretion to reject the request.

The fact that the data controller or processor can refuse to comply with the request to stop processing means the right is not absolute. The data subject may have a situation which they consider to have negative effect on them but the data processor does not agree. This has a potential to be abused and where a situation like this results the data subject may have to resort to court to prevent the processing of data.

A data subject has right to prevent processing of personal data for direct marketing[7]. Direct marketing is defined as communication of advertising or marketing materials which is directed at a particular individual[8].

The data subject has to exercise this write by writing to the data controller or processer and the data controller or processor may accept or refuse the request. Where such a request is refused the data controller or processor will inform the authority of the decision and the authority will look into it and accept or reject it.

Other rights available to the data subject include

1. the right to demand for stop of automated decision marking
   under this right the data subject can demand that certain automated decision making or processing of data be stopped. This right will however be upheld if it does not affect the rest of the data.
2. the right to rectify data
   The data subject has a right to request for rectification of data where data is incomplete, inaccurate or where there are errors on the data.
3. right to erase or destroy personal data
   the data subject has a right to demand for erasure or destruction of personal data where there are errors of personal data.

The above rights are essential in ensuring the right to privacy is upheld. However, the current provisions are not comprehensive enough as they provide for broad exceptions for data

[5] See S. 24(4)(b)
[6] S. 25 of DPPA
[7] S. 26 of DPPA
[8] S. 26(6) of DPPA

collectors, processors or controllers. For example, the law does not clearly spell out the right for the data subject to withdraw his or her consent to have his or her data collected, processed or held in any form. Whereas this could be considered under the right to prevent processing of personal data, the law subjects such a discretion of the data controller or processor meaning it may be difficult to withdraw consent once given.

The above rights give the data subject an obligation to remain vigilant and know what kind of data is out there and how it can damage them. It is essential that the Authority to pro-actively inform and raise awareness amongst the public about their rights, and the safeguards they can expect to benefit from as provided by the law. This obligation also falls on data collectors, processors and controllers to clearly inform data subjects at the time of collection about the processing activities. This becomes difficult to enforce especially given the fact that a lot of data is held in private hands and some of it was acquired before the law came into force.

5.0 Key gaps in the law

Whilst the DPPA provides in theory the main data protection principles, it has major gaps in terms of clearly articulating the obligations of data collectors, controllers and processors as well as robust accountability mechanisms that make enforcement of the law and therefore the protection of the right to privacy difficult. Below are the key gaps in the law.

No provision for withdrawing consent: The lack of specific provision on withdraw of consent by the data subject means once consent is given the data subject's rights will be limited and can only be exercised subject to the discretion of the data controller, data processor or the authority. This undermines the very basis of consent and the right to privacy.

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

Lack of clarity on retrospective application of the law: The DPPA lacks transitional provisions which would cater for data already held by individual's government agencies and others. It is not clear how that data is going to be processed or handled since its holding was before the law came into force and the law does not have a retrospective application.

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

The law does not provide for areas where data is collected without consent mainly by individual actors such as CCTV on private properties, camera drones etc. these can be used to violate the right to privacy of individuals. This is especially a concern given the fact that at the time the law is being implemented there is debate that private CCTV should be linked to government

CCTV as a measure to fight crime. This will directly make private CCTV part of public mass data collection.

Recommendations

Need for regulations which would redefine key data protection principles. These would help patch up the gaps in the principles in the mother laws by providing specific obligations to the data collector including offences where the data collector or processor does not meet the legal obligations.

Regulations should provide for parameters in cases of medical use of data as an exception to consent. At present the law does not give parameters for this as an exception to consent and this is subject to abuse.

The Minister should make regulations that make it mandatory for data collector, processor or controller to report on compliance with the law. This should also include a requirement to report to data subjects in case of breach of data security put in place by the data collector, processor or control. These will enhance the existing accountability provisions in the DPPA.

Law should provide for withdraw of consent where the data subject can choose to exercise his or her write to withdraw consent he or she issued for data to be collected. Such consent should not be subjected to what the authority or the data controller or processor thinks are the reason for withdraw.

Law should provide for general offences which would enable sanctioning aspects of the law that give a duty and a duty may not be met.

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