The Highs and Lows of Uganda's Data Protection and Privacy Act 2019

Introduction

In December 2018, Uganda enacted the Data Protection and Privacy Act, 2019 (hereinafter the Act),[1] four years after a draft of the law was first made public. The Act among other things, provides for; the protection of the privacy of the individual and of personal data by regulating the collection and processing of personal information. It also provides for; the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers; and regulates the use or disclosure of personal information. The law came into force on February 25, 2019 following presidential assent.

With the passing of this law, Uganda became the 23rd African country and the first in East Africa to have enacted a comprehensive legislation on data protection and privacy. Other countries with such laws are Angola, Benin, Botswana, Burkina Faso, Chad, Cape Verde, Côte d'Ivoire, Equatorial Guinea, Gabon, Ghana, Lesotho, Madagascar, Mali, Mauritius, Mauritania, Morocco, Senegal, Seychelles, South Africa, Tunisia, Zambia and Zimbabwe.

The Act provides Ugandans with the strongest safeguards of their right to privacy as provided for in Article 27 of the Constitution, as well as data protection provisions contained in subsequent laws including the Electronic Transactions Act, 2011, Computer Misuse Act, 2011, Electronic Signatures Act, 2011, National Information Technology Authority, Uganda Act (NITA-U Act), and the Access to Information Act, 2005.

The law also provides certainty of the rights of the data subject, their duties and obligations and also highlights the duties and obligation of data collectors, controllers and processors. The law this far provides benchmarks and controls for each of the parties concerned with the collection, management and processing of personal data. This helps to ensure that all decisions and actions taken in relation to personal data are done so within the confines of the law.

Further, the Act reflects Uganda's commitment to obligations under international laws to which it is party, on the right to privacy, including the International Covenant on Civil & Political Rights (Article 11); Universal Declaration of Human Rights (Article 12); UN Convention on the Rights of the Child (article 16); United Nations Convention on Migrant Workers (article 14); African Charter on the Rights and Welfare of the Child (article 10;) and African Union Principles on Freedom of Expression (the right of access to information) (article 4).

This brief highlights the key provisions of the Data Protection Act and the gaps that need to be addressed.

1 *Data Protection and Privacy Act, 2019, https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf Ω*

Definitions and Scope

The Act represents a fundamental improvement in the data and privacy safeguards when compared with the initial draft bills presented to parliament, especially the Data Protection and Privacy Bill, 2015.[2] Specifically, the Act provides clear definitions of personal data; puts in place checks and balances for data collectors and controllers; clearly defines the principles of data collection and creates and imposes clear obligations on parties that may deal with individual data. However, the provisions of the Act especially the non-inclusion of freedom of expression, artistic and journalistic works as part of the justifications for data collection and processing without prior consent of the data subject under section 7 (2) and collection of data about a data subject from a third party under section 11 (2) have a chilling effect on the enjoyment of human rights and freedoms related to freedom of expression and artistic and journalistic works.

Giving Effect to the Constitution

The Data Protection Act gives effect to article 27 of the Constitution of the Republic of Uganda, 1995. Article 27 provides for the right to privacy of the person, including their home, correspondence and communication. This is reflected in section 10 of the Act, which reiterates the right to privacy. It should be noted, however, that from reading the Act, the right to privacy is subject to a number of exemptions including where data is collected or processed for reasons such as national security, medical data, public duty, court processes and lawful processes.

Application of the Law

The Act under section 1 extends its application of the law to foreign persons, bodies and institutions. It should be noted that the interpretation section has not incorporated the suggested definition of who "a person" [3] is. A person has, however, been interpreted to include natural and incorporated bodies. This has been validated in the case of Greenwatch (U) Limited v. Attorney General and Uganda Electricity Transmission Company Ltd, High Court Ruling No.139/2001 in which court decided that corporate bodies, though not natural persons, are taken as persons in law and can enforce rights provided for under the Bill of Rights of the Constitution. By the foregoing decision and the definition of a corporation under section 2 of the Act as meaning an entity which is created by law and is separate and distinct from its owners, the law applies to both natural and persons in law in regards to rights and obligations.

Principles of Data Protection

The law under Part II adheres to and emphasises data protection principles which are provided for in section 3 including accountability; fair and lawful processing; specification and purpose limitation; data retention for only specified periods; quality assurance; transparency and participation of the data subject; and observance of security safeguards. Adherence to data protection principles is in line with the international best practices of data protection such as those provided in the Organisation for Economic Co-operation and Development (OECD), the African Union Convention on Cyber Security and Personal Data Protection under article 13 and the General Data Protection Regulation (GDPR).

Establishment of the Personal Data Protection Office

The Act creates an independent data protection office under section 4 to oversee matters regarding controlling and processing of personal data. Although the office is under the supervision of the NITA-U Board, according to section 5(3), the office is not to be subjected to direction or control of any person or Authority while performing its functions. The office is to be headed by a national personal data protection director whose manner of appointment under section 4(2) shall be specified by an instrument of appointment made by the Minister responsible for information and communications technology in consultation with NITA-U.

2 *See, CIPESA reflections on the 2015 Data Protection and Privacy Bill, 2015, https://cipesa.org/?wpfb_dl=263*

3 *CIPESA had proposed to define a person as "Any person" –includes natural persons and persons in the eyes of the law such as incorporated bodies and companies. suggestion for the term "person" - https://cipesa.org/?wpfb_dl=263*

The establishment of this office guarantees some level of independence in matters of collection, control and processing of personal data. By this independence, data subjects are assured of some level of protection, enforcement and realisation of their data related rights in cases of breach and violation. However, since the data protection director will be appointed, it is in doubt as to whether they will execute their duties independently and without yielding to external pressure.

Though the Act does not provide for a data protection commission, it provides for the creation of a Data Protection Register under section 29. The Data Protection Register is by section 30 to be made available for inspection by any person.

Data Collection and Processing

Part III of the Act elaborates data protection and processing and makes reference to the principles of data protection contained in section 3. It lays down a number of conditions before data collection and processing are conducted. This includes consent of the data subject before collection or processing of data under section 7; prohibition of processing of data relating to children under section 8 unless with the consent of parents or guardians;[4] and compliance with the law and research for statistical purposes. The introduction of data relating to children is new in the Act and speaks to Uganda's compliance with the right to privacy of the child which is inter alia provided for in article 16 of the UN Convention on the Rights of the Child and article 10 of the African Charter on the Rights and Welfare of the Child. The two articles are inter alia to the effect that no child should be subjected to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation.

Section 9 further prohibits the collection and processing of special personal data such as that in relation to beliefs in religion or philosophy, political opinions, sexual life, financial information, health status or medical records of an individual save for data collected within the acceptable lawful limits. The 2015 bill did not provide for prohibition to process data related to finances, health status or medical records.

Further, the law, under section 10 bars any form of infringement on the privacy of a data subject except under section 11 where personal data may be collected from a third party such as in situations where collection is from a public record, there is deliberate exposure of data, consent of the data subject and for lawful purposes. Under section 12, Data is also supposed to be collected by a data collector or data controller only for specific purpose which should be explicitly defined and is related to the functions or activity of the data collector, or data controller.

Section 13 calls for data subjects to be informed and explained to that data is to be collected for a particular purpose. Where the data subject has unrestricted control over collection of their data, they are free to accept or reject. However, they must consent where it is mandatory to provide such data.

In processing data, section 14 requires the data processor to ensure that only necessary or relevant data is processed. Such data must be complete, accurate, up-to-date and not misleading. Further, the data subject should, in line with section 16, be given an opportunity to correct or delete or destroy their data.

These provisions on data collection and processing are not only important for data integrity but also form the basis for which data privacy and other rights of the data subject can be enforced. As per the above provisions, data subjects can pursue remedies in courts of law where their data has been dealt with in an unfair and dishonest manner by collectors, controllers and processors.

4 *A child according to article 257 (1) (c) of the Constitution of the Republic of Uganda, 1995 and section 2 of the Children Act Cap 59 is a person below the age of eighteen years.*

Retention of Records of Personal Data

In line with the data retention principle which is to the effect that data should be kept for no longer than is necessary for the purposes for which it is being processed, the Act under section 18 subsections (1), (3), (4) and (5) provides that personal data shall be retained only for a period necessary to achieve the purpose for which the data is collected and processed. After this period, such data should be deleted or destroyed beyond reconstruction in an intelligible form. The circumstances that warrant data retention beyond purpose include authorisation by law; lawful purposes; data required by a contract between the parties to the contract; and consent of the data subject. Despite the foregoing provision, under section 18 (1) and (2) personal data may be retained beyond purpose for collection and processing. The grounds for such retention include; where data is retained for lawful purposes such as court processes or investigations, national security and for historical, statistical, or research purposes.

Processing Personal Data outside Uganda

The Act is emphatic on cross-border data processing. Under section 19, data processors in Uganda are to ensure that the country in which data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by Uganda's law. Moreover, this processing is subject to the data subject's consent. The provision checks on illegal transfers and abuse of data. It also assures data subjects of data integrity and affords them international protection of their data and privacy.

Security of Data

Security of data is provided for under Part IV of the Act. The law under sections 20 and 21 makes strides in ensuring that appropriate data security measures are put in place by data collectors or processors by securing the integrity of personal data in their possession. Further, section 22 requires that where personal data is processed by authorised third parties, it shall be treated with utmost confidentiality and shall not be disclosed unless under requirement of the law.

Where there are cases of data breaches, the data collector, processor or controller under section 23, is required to immediately notify the NITA-U of the breach and the remedial action taken. The authority shall, where it has determined that the data subject should be informed of the breach, notify the data subject through registered mail, electronic mail, placement in a prominent position on the website of the responsible party or by publication in the mass media.

However, Section 23 of the Act, does not prioritise notification of the data subject in cases of security breach, an aspect that goes to the root of privacy. The section requires the data controller, data collector or data processor to notify the authority and the authority in turn determines whether the data subject should be informed. Further, where it is determined that the data subject should be notified, the prescribed modes of notification like placement in a prominent position on the website of the responsible party clearly breach individual privacy. Moreover, the law does not define who the responsible party is.

Rights of Data Subjects

The rights of data subjects are by law elaborate and are provided for by the Act under Part V, sections 24-28. The rights of the data subject are important for a variety of reasons including ensuring data integrity, personal autonomy and control over one's data, ensuring security and safety of data and the data subject, proper and fair use of data within the law requirements. Consequently, rights of data subjects contribute to control of data and enforcement against collectors, controllers and processors in case of breach of data related rights.

Amongst the rights highlighted in the Act are access to personal information under section 24, though with some limitations and the right to prevent processing of personal data by the data controller or processor under section 25. This exercise is, however, subject to the discretion of the data controller to within 14 days, respond to the notice by the data subject in respect to prevention of processing of personal data. Further, under section 25 (4), the NITA-U may, within seven days, direct the data controller to comply with the notice. Under section 26, the right to prevent processing of personal data extends to cases where processing is for direct marketing.

Under section 27, data subjects have rights related to automated decision-taking. Where a decision is to be taken by or on behalf of the data subject based solely on processing personal data by automatic means, the data subject may be notified by a notice in writing. Hence, as decisions based on automated data processing significantly affect the data subject, data controllers must bring such notice to the attention of the data subject within 21 days. Further, it is a requirement that a data controller within 21 days informs the data subject in writing of the steps that they have taken in compliance with the notice.

The data subject is also, under section 28, entitled to rectification, blocking, erasure and destruction of personal data where such data is inaccurate. The data controller is further required to update the statement of the true facts which NITA-U considers appropriate. Where such actions have been taken, the data controller is required to notify third parties to whom the data has been previously disclosed of the rectification, blocking, updating, erasure or destruction. This serves the purpose of ensuring that all wrong information pertaining to the data subject is replaced with correct data.

Complaint handling

Under section 31, complaints in case of breach and non-compliance by the data collector, processor or controller shall be made by the data subject to the Authority in a prescribed manner and where there are violations, the data collector, processor or controller may in writing make a complaint to the Authority. The authority according to section 32 has investigatory powers into breaches and violations and may make orders as to remedy of breach and restoration of data integrity. Pertinent questions arise as to why the complaints are directed to NITA-U as opposed to the Personal Data Protection Office which should ideally be directly responsible for all personal data related issues.

In terms of compensation for non-compliance with the Data Protection Act by a data controller, processor or collector under section 33, a data subject is entitled to apply to a court of competent jurisdiction for compensation from the data collector, processor or controller for the damage or distress. Further, an aggrieved person has a right to appeal against the decision of the Authority to the Minister within 30 days from the date of notice of the decision.

Offences and Penalties

Offences which may be committed under the Data Protection Act are laid down in Part VIII of the Act. These offences include unlawfully obtaining or disclosing personal data under section 35 which upon conviction attracts a fine not exceeding UGX 4.8 million (USD 1,288) or imprisonment for 10 years or both. The penal sanction under this section is too harsh. Arguably, the main purpose of the harsh fine could be to limit the use of data for artistic and journalistic works especially where such information is constituted by truth and necessary for the promotion of accountability and transparency. Similarly, the effect of the foregoing penalty is self-censorship against use of such data.

Further, section 36 on prohibits unlawful destruction, deletion, concealment or alteration of personal data. The penalty for unlawful destruction, deletion or concealment upon conviction is UGX4.8 million (USD 1,288) or imprisonment not exceeding 10 years or both. This sanction may be justified especially since it provides some checks against unscrupulous individuals who would otherwise evade justice by prescribing a harsh sanction.

Other offences include sale of personal data which is provided for by section 37 and attracts a fine UGX4.8 million (USD 1,288) or imprisonment not exceeding 10 years or both where one is convicted. The law also provides for offences by corporations under section 38 in reference to sections 31 and 32 of the Act. Where a corporation under section 31 fails to report to NITA-U of any belief that a data collector, processor or controller is infringing upon the rights of a data subject or any other person or is in violation of the Act.

Further, it is an offence under section 32 of the Act where a corporation acts contrary to the authority directives, specifically on restoration of the integrity of data collected, processed or held by the data collector, processor or controller or the rights of the data subject. The officers of the corporation and the corporation who knowingly and willfully authorise or permit the contravention are severally and jointly liable for the offence. Where the parties are convicted, the individual persons may be liable to penalties specified in section 35, 36 and 37 depending on the offence committed.

In addition to the foregoing offences, the corporation under section 38 (2) may on conviction be ordered to pay a fine not exceeding two percent of the corporation's annual gross turnover. By this provision, the Act makes strides in expounding on offences by corporations. This, however, does not cater for data dealings where such data is necessary for artistic, journalistic and research works. It also underlooks the fact that such stringent provisions could have a chilling effect on freedom of expression especially on media houses and practitioners and non-governmental organisations and civil society sector.

Regulations

By section 39 of the Act, the Minister is required, in consultation with the Authority by statutory Instrument, to make regulations to address matters prescribed by the Data Protection Act, provide for procedural aspects in relation to the law, provide for the retention period of personal data and for any other matters necessary for the enforcement of the Act.

In respect to the function of issuing regulations, we therefore call upon thee Minister to execute his/her mandate under section 39 of the Act and issue regulations to ensure certainty in the implementation and enforcement of the Data Protection and Privacy Act.

Conclusion

The Data Protection Act, 2013, is a welcome development as it guarantees creditable and important protection of personal data and privacy of Ugandans. Further, the law buttresses privacy as a fundamental human right for Ugandans. It is further instructive on data protection principles, spells out the various rights of the data subject and provides certainty on the enforcement of the data and privacy rights by providing for the duties and obligations of the respective parties. Nevertheless, it should be noted that the Act falls short in certain aspects such as individual autonomy over personal data as it is more concerned with regulation that the rights and their enforcement by the data subject. Moreover, it has harsh penalties that potentially limit freedom of speech, expression and the artistic, journalistic, research and other academic works. Indeed it is not to the standard of the leading European GDPR which offers significant guidance on personal data protection. Despite the shortcomings in the Act, the government should through the responsible Minister swiftly to make regulations, set up Personal Data Protection Office, popularise the law amongst the public and key stakeholders and work with civil society, the private sector and academia to ensure that the Act is not only implemented but that the Ugandan citizenry enjoy their right to privacy and data protection including all the related rights.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org