HRAPF
HUMAN RIGHTS AWARENESS AND PROMOTION FORUM

www.hrapf.org

THE DATA PROTECTION AND PRIVACY BILL, 2015:

ITS IMPLICATIONS FOR MARGINALISED GROUPS

October 2017

THE DATA PROTECTION AND PRIVACY BILL, 2015:
ITS IMPLICATIONS FOR MARGINALISED GROUPS

17th October 2017

A publication of Human Rights Awareness and Promotion Forum (HRAPF)

Human Rights Awareness and Promotion Forum (HRAPF)

Plot 390 Prof. Apolo Nsibambi Road, Namirembe, Kampala
P. O. Box 25603, Kampala.
Telephone: +256-414-530683
Email: info@hrapf.org
Website: www.hrapf.org
Facebook: hrapf.uganda
Twitter: @hrapf_uganda

CONTENTS

1. INTRODUCTION

The Data Protection and Privacy Bill 2015 (hereafter DPPB) was published in the Uganda Gazette on 20th November 2015[1] and tabled before Parliament on 20 April 2016.[2] The Bill was presented by the Information and Communication Technology (ICT) Minister, Hon. John Nasasira.[3] The Bill has been assigned to the Parliamentary Committee on Information and Communication Technology and was scheduled to be debated in August 2017.[4]

The main objective of the Bill is to give effect to Article 27 of the Constitution of the Republic of Uganda, 1995 which protects against interference with the privacy of a person's home, correspondence, communication or other property.[5] The Bill also aims to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information, providing for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers and regulating the use or disclosure of personal information among other related matters.

The Bill in as far as it seeks to regulate the collection of private data has implications for marginalised persons particularly those who are seen as immoral and criminalised, including LGBTI persons, sex workers and drug users. This analysis therefore considers the Bill as it is, highlights problematic provisions for marginalised persons, and makes recommendations.

• HRAPF acknowledges the role of Mr. Francis Tumwesige Ateenyi in making the first draft of this analysis. Everything else was done by HRAPF and all errors and mistakes are our own.

1 See Uganda Gazette No. 68 volume CVIII dated 20th November 2015.

2 Unwanted Witness UW Brief: Uganda's Data Protection and Privacy Bill 2015 is tabled before Parliament available online at https://unwantedwitness.or.ug/uw-brief-ugandas-data-protection-and-privacy-bill-2015-tabled-before-parliament/ (accessed on 23rd July 2017).

3 Unwanted Witness 'Uganda: Data Protection and Privacy Bill, 2015 Legal Analysis – Opportunities and Gaps' (2016) 4.

4 Interview with Mr. John James Ssentumbwe, Clerk to the Committee on Information and Communication Technology, 6th June 2017.

5 Article 27(2).

2. BACKGROUND

Article 27 of the Constitution of Uganda 1995 guarantees the right to privacy by prohibiting interference with a person's home, correspondence, communication or property. The laws that Parliament has passed in respect to data authorise collection of personal data with little real protection of the right to privacy of the individuals about whom the data is collected. These laws include: the Interception of Communications Act 2010; the Registration of Persons Act 2015; the Uganda Communications Commission Act 2013; the National Information Technology Authority Act 2009; and the Access to Information Act 2005. Apart from state institutions established under the laws listed above, many other bodies also collect and store private data about individuals. These institutions include: banks, credit reference bureaus, telecommunication companies, professional bodies, security agencies, embassies, and schools and universities, hospitals, hotels, online technology giants like Google, Facebook, and Twitter; as well as employers. All these bodies have no particular laws that regulate how they receive, store and dispose of information in their possession, and there have been instances where data has been lost,[6] or somehow fallen into the hands of those who are not supposed to have it, including using personal documents to wrap items sold on the streets. [7] A vacuum therefore exists as regards protection of such data collected and due regard for the right to privacy of the individuals about whom the data is collected cannot be ensured.

According to the memorandum of the DPPB, the Registration of Persons Act 2015 and the Regulation of the Interception of Communications Act 2010 do not comprehensively regulate the way in which all categories of institutions, such as banks, hospitals and hotels, collect and store personal information. There is therefore need for a comprehensive law to ensure the preservation of the integrity of collected information and to ensure that it is only used for the purpose for which it had been collected. Currently, there exists a danger that data of a personal nature will be abused in the absence of a legal framework to determine the circumstances and conditions for its use, storage and processing. The Bill is intended to address this absence of a comprehensive law to safeguard personal data by regulating how personal information is collected or to ensure that it is only used for the purposes for which it is collected.

---

6 For example, in July 2016 passports and original visa application documents of individuals from Uganda who had applied for UK visas were lost enroute from the UK High Commission in Pretoria to Kampala. Although the persons affected were reportedly to be compensated, it still remains that personal information was lost and could have gotten into wrong hands. See for example 'UK to pay Ugandans for lost passports, travel documents' Daily Monitor, July 26, 2016. Available at http://www.monitor.co.ug/News/National/UK-to-pay-Ugandans-for-lost-passports-travel-documents/688334-3310508-a38t3k/index.html (accessed 17 October 2017).

7 See for example 'Do Ugandan job seekers have any right to privacy?' Daily Monitor October 7 2010. Available at http://www.monitor.co.ug/OpEd/Commentary/689364-1027566-92e25rz/index.html (accessed 17 October 2017).

The Bill is largely aimed at giving effect to Article 27(2) of the Constitution by providing principles for data protection and recognising the rights of persons in respect of whom personal information is collected. To achieve this, the Bill proposes that the National Information Technology Authority of Uganda (NITA) should monitor persons and bodies collecting data to ensure that personal information is collected, processed, stored and used in accordance with the Constitution and considering the rights of persons whose personal information is collected. Uganda is also part of the East African Community and is obliged to give effect to the EAC's Legal Framework on Cyber Laws, [8] which the Bill aims to do.

This analysis seeks to establish whether the DPPB lives up to its promises, particularly as regards protection of information concerning marginalised persons. It examines the provisions of the Bill in light of the Constitution and international data protection standards and makes observations on the adequacy, effectiveness and enforceability of the Bill.

3. ANALYSIS OF THE DIFFERENT PARTS OF THE BILL

The Bill is divided into eight parts, and this analysis covers each part in turn:

3.1 Part I: Preliminary

Part I, which contains clauses 1 and 2 covers the scope and application of the proposed law (once enacted) and guides the interpretation of the key terms and phrases used in the text.

Clause 1: Application

This clause provides that the law will apply to any person, institution or public body collecting, processing, holding or using personal data.

Implications for marginalised persons

Although clause 1 does not go into details of all the bodies covered, the use of the term 'any' ensures that the provision is wide enough to cover any entity that collects private data, including private individuals and organisations and therefore none can claim that they are excluded. This is therefore a welcome provision for marginalised groups, as all persons who collect information from them, including organisations, will be subjected to the principles under the Act.

---

8 For further information on this Framework, see presentation by United Nations Conference on Trade and Development presented at the 2013 CTO Cybersecurity Forum and available at http://www.cto.int/media/events/pst-ev/2013/Cybersecurity/Cecile%20Barayre.pdf (accessed 17 October 2017).

Recommendation
The clause should be adopted as it is.

Clause 2: Interpretation
This clause defines key terms used in the Bill. It starts with a definition of 'authority' to mean, the National Information Technology Authority.' This authority, commonly known as NITA is established under the National Information Technology Uganda Act, 2009 [9] as an autonomous body responsible for providing 'first level technical support and advice for critical Government information technology systems including managing the utilisation of the resources and infrastructure for centralised data centre facilities for large systems through the provision of specialised technical skills' among other functions.[10] The clause also defines 'data' as 'information which is processed by means of equipment operating automatically in response to instructions given for that purpose' or that which forms part of an accessible record. 'Personal data' is data from which a person can be identified that is recorded in any form. This could be data relating to nationality, age, marital status, educational level, occupation, financial transactions, an identification number, symbol, identity data or data regarding an expression of opinion about the individual.

Implications for marginalised persons
NITA is primarily concerned with Information Technology matters and has broad mandate under the NITA Uganda Act.[11] The task of safeguarding data could best be handled by a designated, specialised body. The Act, in assigning NITA as the authority responsible for safeguarding data may cause this important duty to be overlooked in favour of the functions which NITA was created to perform. Unwanted Witness already considered this and also recommended a new body. [12]

The definition of personal data is sufficient since it also includes data collected without using computers, and applies to any accessible record. This definition is in line with the Organisation for Economic Development and Co-operation (OEDC)' s definition in the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[13] which regards personal data as 'any information relating to an identified or identifiable

9 Act 4 of 2009.

10 According to section 5 of the National Information Technology Authority Uganda Act, 2009, the other functions of NITA include the coordination, supervision and monitoring of the utilization of information technology in the public and private sector; advising Government on all matters of information technology development, usability and accessibility including information technology security; the regulation and enforcement of procurement standards for information technology in Government Ministries and the creation and management of the national data bank.

11 The National Information Technology Authority, Uganda Act 2009.

12 See Unwanted Witness, n2 above, 11-12.

13 OECD 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

individual.'While these guidelines are not binding, they provide the international minimum standards as regards protection of data privacy. The Bill in its current form identifies a closed list of characteristics to which 'personal data' relates Personal characteristics such as sexual orientation and gender identity are not specifically included in this closed list and can therefore be interpreted as being excluded.

Recommendation

The definition of 'Personal data' should be broadened in line with the definition of the OECD to mean 'any information relating to an identified or identifiable individual.'

The definition of 'Authority' should be changed to refer to a body specifically created to handle Data protection and privacy matters rather than NITA. This could be called the Data Protection and Privacy Authority.

3.2 Part II: Principles of data collection

Part 2 of the Bill has one clause on principles.

Clause 3: Principles of data collection

This clause outlines principles of data protection and obliges NITA to ensure that data collectors, processors and controllers abide by them.[14]

The principles are: accountability to the data subject; fairness and lawfulness; adequacy and relevancy of the data collected or processed; retaining the data for the period required only; ensuring quality of information, transparency and participation of the data subject; and observation of security safeguards.[15]

Implications for marginalised persons

The principles set out in the clause adhere to the OEDC Guidelines, which ensure protection of the privacy of everyone, including marginalised persons. The Guidelines set out a number of basic principles of national application to privacy legislation including the Collection Limitation Principle; the Data Quality Principle; the Purpose Specification Principle; the Use Limitation Principle; the Security Safeguards Principle; the Openness Principle and the Individual Participation Principle. This is commendable. However, while the principles of data protection are well laid out in the Bill, the Bill does not set out how compliance will be monitored and enforced and what the sanctions for breach of these principles should be. According to Guideline 19(d) of the OEDC Guidelines states should provide adequate sanctions and remedies where the above stated principles are not complied with. Thus without these sanctions, this part of the Bill appears more as a declaration of principles than a law capable of imposing statutory duties on persons dealing with private data.

---

14 Clause 3(2).

15 Clause 3(1).

Recommendation

The Bill should spell out enforcement mechanisms and sanctions for contravention of the data protection principles including administrative sanctions such as suspension or de-registration of the non-compliant persons or entities; or criminal offences and related punishments.

3.3 Part III: Data collection and processing

The third part of the Bill deals will all matters relating to the collection and processing of data including the issue of consent to collect or process personal data, the protection of privacy and the prohibition on collecting and processing special personal data. This part of the Bill also regulates the collection of personal information and the processing of personal data outside of Uganda. The clauses are as follows:

Clause 4: Consent to collect or process personal data

Clause 4 prohibits collection or processing of personal data without the consent of the data subject. However the provision lists numerous exceptions where consent may be dispensed with including: where the collection or processing is authorised or required by law, where it is necessary for performance of a public duty, national security, prevention or punishment of a breach of law, performance of a contract to which a data subject is a party, medical purposes or compliance with legal obligations. Where a data subject objects to the collection of data, the data collector or processor must stop the collection except where data is being collected or processed under the listed exceptions.

Implications for marginalised persons

While it is acceptable to put exceptions to the requirement of consent to the collection of personal data, the OECD guidelines require that such exceptions should be as few as possible and should be made known to the public. The exceptions given in the Bill are many and broad and some would be a blatant violation of the right to privacy. For example, the exception of collecting personal information without consent of the data subject for medical purposes seems unreasonable and unjustified. That being said, even the OECD Guidelines leave it up to the individual states to determine which exceptions best apply in their contexts. In Uganda, the yardstick for such exceptions is provided in Article 43 of the Constitution, which provides for circumstances when enjoyment of rights can be limited. The general yardstick is that the limitation should be demonstrably justifiable in a free and democratic society. The proposed exceptions in the Bill remain broad and prone to abuse, especially for marginalised and criminalised communities like sexual minorities and drug users. Their right to privacy could easily be invaded under the pretext of performing public duties or preventing and investigating crime. To avoid the possible abuse of these exceptions, it should clearly be provided that information collected under this section without the consent of the data subject should not be used for any purpose other than that for which it was collected. A similar provision exists in clause 13 but it is a general provision that applies to the whole of the Act. There is need for the deliberate emphasis of the limited use and disclosure of personal data collected without consent. It should also be added that the data subject

should be told that their personal data was collected for a particular purpose, at a time when the data controller deems it fit and proper to do so.

Recommendations

3 new sub-clauses should be included in clause 4 stating as follows:

> (4) Every data subject shall be informed of data collected without his or her consent at a point when such knowledge cannot prejudice the purpose of the data collection or compromise the accuracy of the information.
>
> (5) Data collected under sub-section (2) shall not be used for any purpose other than that for which it was collected.
>
> (6) Any data collector, controller, processor or any other person who contravenes sub-section (5) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty five currency points or imprisonment not exceeding ten years or both.

Clause 5: Prohibition on collection and processing of special personal data

Clause 5 prohibits collection or processing of special personal data relating to religious or philosophical beliefs, political opinion or sexual life of an individual. The clause also creates wide ranging exceptions including: where the data is collected under the Uganda Bureau of Statistics Act; the data subject freely consents to the collection; or the data is collected or processed in performance of a public duty. Other exceptions include data collected for legitimate activities of a non-profit organisation; a political, religious, philosophical or trade union organization; or for a membership body whose information is not disclosed to third parties.

Implications for marginalised persons

The exclusion of collection of data on the 'sexual life' of an individual is a very welcome provision particularly to sex workers and LGBTI persons as it helps them not to be subjected to prejudice. Prohibition of collection of data designated as 'special' is a standard exclusion in data collection regimes. This category comprises of especially sensitive data which may prejudice an individual if not handled carefully. However, the clause also provides numerous conditions and circumstances under which the exempted data may be collected. Of great danger are the exceptions that allow employers to collect such special personal data in fulfilment of a right or obligation or collection of data for the legitimate activities of a body or association. Such body or association can include NGOs. It should be noted that many employers and NGOs are in the private sphere, and are left to their own means of governance. These wide sweeping exceptions would give such private actors space to collect even unnecessary personal information, especially when it comes to unpopular and criminalised minorities like LGBTI persons and sex workers. An ill-informed suspicion on the part of the employer

or a body of a person's sexual orientation for example could prompt unnecessary collection of personal data under these exceptions. As guided by the OECD guidelines, exceptions under this law should be as few as possible to mitigate abuse. Since there is already an exception created for public purposes under the Uganda Bureau of Statistics Act, any other special personal data that has to be collected as an exception to this section should only be with the informed consent of the data subject. In order to give informed consent, the data subject should be informed of the kind of information being collected and the purpose of the data collection before the data is collected.

Recommendation

The clause should be redrafted by replacing clause 5(3) with:

(1) A data collector, data processor, and data controller may collect or process information specified in sub-section (1) where the information is given freely and with the informed consent of the data subject.

Clause 6: Protection of privacy

Data collectors, processors and controllers are obliged not to infringe the privacy of individuals in respect of whom the personal data they are handling relates.

Implications for marginalised persons

This is an emphasis of the right to privacy guaranteed under Article 27 of the Constitution and a re-statement of the fact that at the heart of data protection is the right to privacy that should be upheld and respected. This is a favourable provision which will go a long way in protecting the right to privacy of marginalised persons.

Recommendation

The clause should be adopted as is.

Clause 7: Collection of data from data subject

Clause 7 requires collection of personal data directly from the data subject. Exceptions to this requirement include the following instances: where the data is contained in a public record; the data subject has deliberately made the data public; the data subject has consented to the collection of data from another source where such collection from another source will not prejudice the privacy of the data subject; or where it is not practical to obtain the consent of the data subject. The other exceptions relate to national security, enforcement of a law imposing a pecuniary penalty, enforcement of legislations on revenue collection, conduct of judicial proceedings and for prevention, detection or punishment of breach of the law. The clause also contains an exception where 'compliance would prejudice a lawful purpose for the collection'.

Implications for marginalised persons

While the clause is commendable in as far as it tries to protect the privacy of an individual, the exceptions proposed are very broad and prone to abuse. There is no doubt that most of the exceptions, for example information required in an investigation, are reasonable. However, there needs to be safeguards to ensure that as much as possible, the privacy of the individual is not unnecessarily compromised and that the exceptions are limited. There is also need to ensure that the affected individual, as far as practicable, is aware of the collection of this information and its use. The Commonwealth Model Bill on the Protection of Personal Information[16] provides good guidance on how to limit instances where personal information is collected from other sources.

For criminalised communities, it would be easy for persons to divulge their personal data under the pretext of investigations or any other exception under this clause. It should be noted that the issue of source of personal information feeds into the issue of consent and knowledge of collection of personal information by the data subject and should therefore be treated with utmost care.

Recommendation

The clause should be amended to include the recommended wording in the Commonwealth Model Bill on the Protection of Personal Information. The clause should therefore read as follows:

(1) *A person shall collect personal data directly from the data subject.*

(2) *Notwithstanding subsection (1) personal data may be collected from another person, source or public body where-*

- (a) *the data is contained in a public record*
- (b) *the data subject has deliberately made the data public*
- (c) *the data subject consents to having the data collected from the person/organisation who has custody or control of it*
- (d) *the data subject consents to having the person/organisation that has custody or control of the information disclose it*
- (e) *the person/organisation that has custody or control of the information is authorised by law to act on behalf of the data subject and consents to the disclosure of the information*
- (f) *the person or organisation is authorised by law to collect information in a manner other than directly form the data subject.*

(3) *At or before the time, or if that is not practicable, as soon as practicable after, a person/organisation collects information under subsection (2), such person/*

16 Available online at http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_6_ROL_Model_Bill_Protection_Personal_Information_2.pdf (accessed 17 October 2017).

organisation shall take such steps as are, in the circumstances, reasonable to ensure that the data subject is aware of –

(a) *the purpose for which the information is being collected*
(b) *the fact that the collection of the information is authorised or required by or under law; and*
(c) *the intended recipients of the information.*

Clause 8: Collection of personal data for specific purposes

Clause 8 requires a data collector to collect the data for a lawful purpose which is 'specific, explicitly defined and is related to the functions or activity of the person or public body.'

Implications for marginalised persons

This clause is positive as it ensures that data that is collected is relevant to the purpose of its collection. For marginalised persons whose activities are criminalised, this provision is meaningful in that it curbs the volume of personal data that can be collected and the purposes for which this data may be used. Only data which is strictly necessary for the purpose of the collection should be collected.

Recommendation

The provision should be adopted as it is.

Clause 9: Information to be given to a data subject before collection of data

Clause 9 imposes an obligation on the data collector to provide the following information to the data subject before data collection: the nature of the data required; the address of the data collector; whether the supply of the data is discretionary or mandatory; consequences of failure to provide the data; recipients of the data; nature and category of the data; the data subject's right of access to and right to request rectification of the data collected; and the period for which the data will be retained. The requirement to furnish this information to a data subject still persists even if data is collected from a third party. Again, the exceptions listed in clauses 4 and 7 and already alluded to in this clause apply to dispense the requirement to inform a data subject.

Implications for marginalised persons

The requirement that individuals be given what is called a fair processing notice is a fundamental part of fair processing obligations and emphasises the need to protect the privacy of the data subjects. This is very important for marginalised and criminalised communities, as the information given may actually be self-incriminating. However, the exceptions in this clause are unjustified to the extent that they take away the right of the data subject to be informed that their data is being collected.

Even if personal data was required for revenue purposes, enforcement of a public duty or judicial proceedings, the data subject should be informed as soon as practicable. The exceptions would be relevant in instances where the data is being collected from another source other than the data subject or if the information is being collected without the data subject's consent. All these scenarios are ably addressed in the clauses discussed above and should be sufficient. For any data that is to be collected from the data subject with their consent, fair processing notice should be a requirement.

Recommendation
The exceptions under clause 9(3) are unjustified and the clause should be deleted from the Bill.

Clause 10: Minimality
Clause 10 requires a data controller to only process personal data that is relevant and necessary, and expressly prohibits processing of personal data that is in excess of what is authorised by or required for a particular purpose.

Implications for marginalised persons
This provision is important as it curtails the discretion given to data collectors to determine the nature of personal data they need for a particular purpose. Unnecessary and invasive collection of data like people's sexual orientation for suspected LGBTI persons would be minimised.

Recommendation
The provision should be adopted as is.

Clause 12: Correction of personal data
According to clause 12, a data subject may ask a data controller to correct or delete personal data which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading information which was obtained illegally or which the controller no longer has authority to retain. The data controller is obliged to comply with the request but where they are not able to comply or reach an agreement with the data subject, the data controller is required to attach to the record an indication that a request for correction has been made and not complied with. The data controller is also required to give written reasons for non-compliance to the data subject. Where the data controller complies, they are required to inform persons to whom data has been disclosed.

Comment
Under this section, a data controller who does not comply with the request for correction or deletion of data is only required to 'attach to the record an indication that a request for correction has been made and not complied with'. The Bill does not provide for any remedies or way forward for the data subject.

Recommendation

The clause should be revised to provide that where the data subject and data controller cannot reach an agreement, the data subject should be given a timeline within which to appeal the decision taken, and a timeframe for resolution of the issue given.

Clause 13: Further processing to be compatible with purpose of collection

Under clause 13, where data is collected and held for a specific purpose, further processing must only be in connection with that purpose. The clause deems further processing to be compatible with the purpose where: there is consent from the data subject, the data is publicly available or has been made public, further processing is required by law, for judicial proceedings, detection, prevention or punishment of the breach of law, national security, public health or enforcement of law which imposes a pecuniary penalty. The Bill also permits further processing where it is required for historical, statistical or research purposes provided that the person processing it ensures that further processing is carried out for the purpose for which it was originally collected and that it is not published in a manner likely to reveal the identity of the data subject.

Implications for marginalised persons

This clause protects the data privacy of persons by preventing abuse of collected data and is overall a positive provision. However, the clause should be treated with caution because it provides in subsection (3)(c) that further data processing will be deemed to be in line with the purpose for which the data was collected if it is necessary for the detection, prevention, prosecution and punishment of an offence or breach of the law. The implication of such a provision on persons who hold unpopular beliefs/ opinions and unpopular and criminalised social groupings such as LGBTI persons, drug users and sex workers is that whereas their personal data may be gathered for innocuous purposes, if an initial analysis of that data were to reveal some of these aspects of their lives, this clause may be used as a reason to violate their privacy and subject their data to further processing quite unrelated to the purpose for which it was collected.

It is necessary that this clause, for purposes of protecting data subjects, be modified with a proviso that specifically precludes further processing of data in relation to or for purposes of ascertaining the religious or philosophical beliefs, political opinion or sexual life of the data subject. This will ensure that data collectors and processors, especially those working with the state in law enforcement, shall work with only that data that is reasonably relevant to their work and not unnecessarily infringe upon the privacy of individuals just because they happen to be of an unpopular or unconventional persuasion, whether sexual or otherwise. This will in fact bring the provision more in line with the principle of minimality under clause 10 of the Bill which requires a data controller to possess only that data strictly relevant for the purpose for which it is collected or as authorised by law.

Recommendation
The clause should be amended to include a sub-clause providing that further processing of data shall not be done regarding data that relates to religious or philosophical beliefs, political opinion or sexual life of the data subject.

Clause 14: Retention of records of personal data
Clause 14 re-iterates that a person who collects data must not retain data beyond the period that is necessary to achieve the purpose for which it was collected except where retention is required under the legal exceptions similar to those provided in clauses 4, 7 and 9 already discussed. Clauses 14(4) and (5) enjoin the data controller to destroy or delete records of personal data or de-identify the personal data upon expiry of the retention period and the destruction should be in a manner that prevents reconstruction.

Comment
As with clause 13, this provision is protective of data subjects but the danger is in the exceptions, particularly regarding the retention of personal data for purposes of detecting, preventing, investigating, prosecuting and punishing an offence or breach of law. The danger of allowing such provisions to pass into law without a clause modifying their applicability is that laws in Uganda have traditionally been used, especially where they are broad or vague, to perpetrate egregious violations of human rights. This is particularly relevant in the case of criminalised and marginalised communities like LGBTI persons, sex workers and drug users who are normally arrested and detained under various penal laws, even without a sound basis for such arrests. Having their personal data collected and possibly retained for broad reasons like investigations would open them up to malicious and pervasive arrests and violations.

Recommendation
A provision should be put in place limiting the applicability of the above exceptions to data that does not relate to religious or philosophical beliefs, political opinion or sexual life of the data subject.

Clause 15: Processing personal data outside Uganda
Clause 15 requires those who process data outside Uganda to ensure that the countries in which they are processing it have adequate measures in place for the protection of the personal data which are at a minimum equal to the protection provided under the proposed law.

Comment
This clause in its current form is a good provision targeting those that collect data in Uganda for processing and use outside the country. This is good for marginalised persons whose personal data may be exposed or exploited by those outside of Uganda. However, the clause certainly raises enforceability questions as it is not addressed how it will be implemented when the person has already left the jurisdiction.

Recommendation
The clause should be revised to provide that those processing data outside Uganda must show the adequacy of the protection measures of the countries in which they are processing it before permission may be given by the relevant authorities for such data to be collected.

3.4 Part IV: Security of data
Part IV of the Bill deals with security of data and requires the adoption of appropriate measures to prevent the loss, damage, unauthorised destruction and unlawful and unauthorised processing of personal data. This Part of the Bill also requires a data collector to notify the NITA where an unauthorised person has accessed personal information of an individual. The following clauses are of importance:

Clauses 16 -18: Security measures
Clauses 16 to 18 impose obligations upon data controllers to ensure the integrity of personal data in their possession or control through the adoption of appropriate measures. This is intended to prevent loss, damage, unauthorised destruction, unlawful access or unlawful processing.[17] The measures include having contractual obligations with data processors to ensure that they do the right thing, and to reject a processor until he/she complies with the requirements of the Bill.[18] A data processor or operator acting for a data controller is enjoined to process data only with the prior knowledge and authorisation of the data controller and to treat all personal data with confidence. Disclosure of such data should only be in instances where it is required by law or in the course of performing duties.[19]

Implications for marginalised persons
These are good provisions that protect personal data including that belonging to marginalised and criminalised communities, who would particularly be concerned about their data being lost and accessed by persons who should not access it, as this may have implications on their wellbeing, and may be the difference between their retaining their freedom and being arrested.

Recommendation
The clauses should be retained as they are.

Clause 19: Notification of data security breaches
Clause 19 requires data collectors, processors and controllers to notify NITA of any breaches including where personal data is accessed by an unauthorised person and

17 Clause 16.

18 Clause 17.

19 Clause 18.

to make notification of any remedial action taken. It is, however, the preserve of NITA to determine whether the data subject should be notified. Where it is decided that the data subject be informed, the Bill requires that communication could be done by registered mail, electronic mail, placement on the website of the responsible party or publication in mass media. Still, the notification has to be in such a way that it enables the data subject to take protective measures against consequences ensuing from unauthorised access. NITA may also order publication of the breach where it believes that such publication would protect the person affected by the breach.

Comments

The clause provides for notification of NITA and not the data subject in the event of breaches of security of data. It is then for NITA to determine whether the data subject should be informed or not. As part of the fair processing principle, individuals should be informed about their data which is controlled/processed third parties and this should not be left to NITA for determination. As provided in subsection 4 of the clause, the purpose of this notification is to enable the data subject take protective measures to guard against the consequences of the unauthorised access. The provision that allows the Authority to decide whether or not the data subject should be informed of a breach of their privacy and confidentiality presupposes that the Authority is best placed to determine if and how a data subject may be affected by the breach. This is against the spirit of the protection of the privacy of the data subject in as far as it gives room for the Authority to excuse certain breaches of privacy and confidentiality of individuals on grounds that are not even specified at law. This provision will be used to infringe upon the privacy of individuals mostly by state operatives who may unlawfully access data of individuals viewed by the state as subversive because of their dissenting views, opinions or beliefs and upon the tacit approval of the Authority that is supposed to protect the privacy of their data if such a provision is included. In addition, it is not clear how this part of the Bill will be enforced. There are no sanctions or enforcement mechanisms for compliance.

Recommendation

In recognition of the fact that notification of data breaches to the data subject is meant to enable them to take precautionary measures against the consequences of such breach, this provision should be amended to provide that, where any breach occurs, the data processor, data collector or data controller should immediately notify the data subject as well as the Authority. In this manner, the data subject will be given the autonomy to decide whether or not the breach will affect them, rather than leaving it to the Authority to take such a decision over the privacy of an individual. It is vital that, in a law such as this that is intended to safeguard the privacy of individuals, the autonomy of those individuals is respected above all.

The Bill should also clearly spell out sanctions for non-compliance and an enforcement procedure for this part of the proposed law.

3.5 Part V: Rights of data subjects

This part deals with matters relating to the rights of data subjects including the right to access personal information, the right to prevent the processing of personal data and rights in relation to automated decision taking and destruction of personal data. The clauses are analysed together one by one.

Clause 20-24: Rights of data subjects

Under clause 20 (1) and (2) a data subject may, upon proof of identity request the data controller to confirm whether they hold personal data about him or her and give a description of the personal data which is held including information about any third parties who have had access to the personal data. However clause 20(3) permits the data controllers to refuse to comply with the request unless the data subject provides information reasonably required by the data controller to identify the person or locate the requested information. Clause 20(4) creates another limitation concerning personal data which may lead to disclosure of information related to another person who may be identified from the personal data. Such data cannot be disclosed unless the affected third party consents to the disclosure or it is reasonable to provide the personal information without the consent of the third party. Clause 20(8) expounds on the factors which should be taken into account when determining whether it is reasonable to disclose information under clause 20(4) and these include: any duty of confidentiality owed to the third party; steps taken to seek the consent of the third party; whether the third party is capable of giving consent and any express refusal or consent by that third party. The Bill provides in 20(9) that data requests under this provision should be complied with promptly and within 30 days.

Under clause 21 a data subject has a right to write to a data controller or processor asking them to stop processing personal data which is likely to cause substantial damage or distress to the individual. The data controller has fourteen days from receipt of the notice to write back informing the data subject that he has complied or intends to comply with the request or if they are not complying give reasons for the non-compliance. Reasons for non-compliance must be communicated to NITA which may or may not order the data controller/processor to comply with the request.

Clause 22 empowers the data subject to write to a data controller preventing the use of personal data for direct marketing. Again the data controller has 14 days to respond on whether they have complied, intend to comply or giving reasons for non-compliance. However NITA retains the authority to direct the data controller to comply where it is satisfied that the complaint is justified.

Under clause 23, a data subject may write to the data controller to ensure that any decision affecting him significantly is not based solely on the processing by automatic means. The data controller is obliged to inform the data subject that a decision was solely made by way of automation means and also notify them of their right to require the decision to be reconsidered. After receiving a notice for reconsideration, the data controller is obliged to comply within 21 days. There are exceptions to the foregoing requirements provided in clause 23(4) regarding instances where the decision

concerns consideration of whether to enter into performance of a contract with the data subject. The other exceptions concern where automation decision making is required or authorised by law or prescribed by the Minister of ICT. As with other requirements, NITA retains the authority to order compliance.

Lastly, under this part, clause 24(a), a data subject may complain to NITA to order the data controller to rectify, update, block, erase or destroy data which is inaccurate. Such an order can only be made upon NITA satisfying itself that the data is inaccurate. Where the data has been erased, blocked, rectified or destroyed the data controller is obliged to notify third parties to whom the data has previously been disclosed.

Implications for marginalised persons

'Subject access', which is the right to access one's personal information processed or held by a data processor or controller, is a central part of data protection regimes. This part of the Bill spells out all the key components of subject access including the right to know where one's data is held, the directing of requests to prevent use of personal data for marketing, the directing of requests in respect of automated decisions among others.[20] Compliance is ensured by granting authority to NITA to make an order to that end in a number of instances.

The issue, however, concerns the range of exceptions in this part of the Bill. Obligations to perform a contract should not be part of the statutory exceptions. Private contracts are entered into by parties who voluntarily provide all the information they require from each other and there is no need for statutory interference in the manner proposed.

Secondly, there is a possibility that data controllers and processors will charge fees to allow access. The risk is that the fees could be prohibitively high and scuttle the right of access.

Further, the manner in which clause 20(3) is drafted, encourages data controllers and processors to impose additional conditions and this could be abused by imposition of onerous requirements making it impossible for individuals to access their data.

Lastly, a data controller or processor should not have a right to use personal data for direct marketing unless the data subject consents as it is currently stated.

Recommendations

1. The exception concerning performance of contractual obligations should be deleted.

---

20 See https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf (accessed 17 October 2017).

2. The Bill should impose, or provide for making of regulations which impose, a maximum amount chargeable by data controllers and processors for access to information.

3. The Bill should list the requirements for data access and not leave data controllers and processors with wide discretion to do so.

4. A data controller should seek permission from the data subject to use personal data for direct marketing.

3.6 Part VI: Data Protection Register

This part of the Bill deals with the establishment of the Data Protection Register and provides that it should be accessible to the public.

Clause 25: Data Protection Register

Under this Clause, NITA is required to register every person, institution or public body collecting or processing personal data and the purpose for which such data is collected or processed in the Data Protection Register which shall be kept and maintained by NITA. The manner in which data collectors and processors apply for registration will be provided for in the Regulations.

Implications for marginalised persons

This clause is acceptable as it allows NITA to have a list of entities that collect personal data but without encumbering such providers to register as usually they are registered under the different laws governing the different sectors.

Recommendation

The clause should be adopted as it is.

Clause 26: Access to Register by the public

This clause provides that NITA shall make the information contained in the Data Protection Register available for inspection by any person.

Comment

It is a progressive step to make information about persons, institutions or public bodies collecting or processing personal data publicly available. The register should be freely available to members of the public. However, the clause should be revised to expressly provide for free access and inspection. Furthermore, the list of registered collecting and processing bodies should be published in the Uganda Gazette and national newspapers at least once annually as well as on the NITA website.

Recommendation
The clause should be amended to expressly provide that access to the register shall be free of charge and that the register will be annually published. It should read as follows:

(1) *The Authority shall make the information contained in the Data Protection Register available to inspection by any person, at no cost.*

(2) *The Authority shall ensure that the Register is published in a Gazette once a year and that it is permanently displayed on the Authority website.*

3.7 Part VII: Complaints, Compensation and Appeals
Part seven of the Bill deals with complaints in cases of non-compliance with the Act, authority to investigate complaints and consequences for failure to comply. The part will be analysed as a whole.

Clauses 27-30: Complaints, Compensation and Appeals
Clause 27(1) allows the data owner or any other person to complain to NITA about violation of their rights or contravention of the provisions of the proposed law by a data collector, data processor or data controller. Conversely, clause 27(2) provides for complaints by data collectors, processors and controllers about violation of the proposed law. Clause 28 mandates NITA to investigate all complaints received and to make orders to data collectors, data processors and data controllers to remedy any breaches or take action to restore the integrity of the data and the rights of the data owners. In addition to the remedies provided for in clause 28, clause 29 provides for compensation payable by data collectors, processors and controllers to a data owner who suffers damage or distress due to non-compliance with the provisions of the proposed Act. Clause 29(2) however provides that it is a defence to prove that the person against whom a complaint is registered took reasonable steps to comply with the requirements of the proposed law. Clause 30 creates a right of appeal to the Minister of Information and Communications Technology by any person who is not satisfied with the decision of NITA. Such an appeal must be filed within 30 days.

Implications for marginalised groups
There is lack of harmony between the Bill and provisions of the National Information Technology Authority 2009 (NITA Act) under which NITA is established. The NITA Act does not bestow on NITA the quasi-judicial powers envisaged in the Bill neither does it create any tribunal or administrative branch of NITA to adjudicate matters of the nature envisaged under the Bill. Similarly, the Bill does not create any such tribunal and seems to assume that all is already settled under the NITA Act. This begs the question: who exactly at NITA will be responsible for hearing and adjudicating complaints and making and enforcing orders under clauses 27, 28 and 29?

On the issue of appealing to the Minister, since Ministers are partisan political figures, the process of appealing a decision of a technical body to a political figure, does not

augur well with the administration of justice, more so for groups or persons that may be marginalised or criminalised. In addition, the process of appeal seems to stop with the Minister, with no option granted to an aggrieved party to appeal to a court of law.

Recommendation

There is need for the Bill to establish a new authority rather than NITA to handle issues under this Act. The clause should also provide for appeals to a court of law, in case a party is aggrieved with the decision of the Minister.

3.8 Part VIII: Offences

Offences are covered under clauses 31-33. All will be dealt with together:

Clauses 31-33: Offences

Clause 31 prohibits knowingly or recklessly obtaining or disclosing personal data held by a data controller or procuring the disclosure to another person of information contained in personal data. Clause 32 prohibits selling of personal data. The punishment for persons found guilty of contraventions under both clauses is a fine fixed at a maximum of Uganda Shillings Four Million and Eight Hundred Thousand (UGX 4,800,000) or a jail sentence not exceeding ten years. Clause 33 deals with breach by corporations and imposes criminal liability not only on the corporation but also the corporation's officers who authorise or carry out the prohibited acts.

Implications for marginalised groups

Clause 33 of the Bill which was public in the Gazette on 20th November 2015 makes reference to 'an offence under section 29 and 30' which is an apparent typographical error given that those clauses deal with compensation and appeals respectively and not offences. The proper provisions should be 31 and 32.

Significantly, the Bill provides for enforcement of criminal sanctions against individuals and corporations but not government bodies and public officials. Since a significant volume of personal data is or will be held by a host of public agencies such as the National Registration Authority (NIRA), Uganda Revenue Authority (URA), Uganda Citizenship and Immigration Control Board, Petroleum Authority of Uganda (PAU), Uganda Registration Services Bureau (URSB), the Uganda Police Force (UPF), Uganda Communications Commission (UCC), among others, data misuse in such institutions should equally be punished. The Bill is not clear on how NITA will impose let alone enforce sanctions against government bodies of equal standing.

Recommendation

Clause 33 should be revised to correct the typographical error. The clause should also be expanded to provide for punishment for misuse of personal data by government institutions and public officials.

4. GENERAL OBSERVATIONS

The following matters should also be considered when discussing the Bill:

i) Exclusion of data collected by an individual for personal use

Compilation of personal data by an individual for private domestic or personal use is an exemption to data protection obligations which is recognised by other jurisdictions [21]. An example of such use would include a personal diary, contacts list, a list of one's friends' birthdays, among others. The Bill does not provide for domestic use as an exemption and this would impose onerous obligations on individuals.

Recommendation

The Bill should provide for domestic use as an exception to data protection obligations.

ii) The lack of effective enforcement mechanisms and sanctions

The proposed law generally lacks a coherent and effective sanctions and enforcement mechanism. It instead makes declarations of intent without backing them up with biting provisions which poses the risk that the whole data protection regime based on the proposed law may fall flat and fail to serve its purpose.

Recommendation

The Bill should make provision for an effective enforcement regime.

iii) Transitional clauses

The Bill contains no transitional clauses. This would be important to define the status of personal data which has already been collected and is held by various governmental agencies and private companies.

Recommendation

The Bill should provide for transitional clauses to the effect that the proposed law shall apply to personal data already collected and held as if the same was collected and held under the Act and institutions holding such data shall comply accordingly.

iv) The Status of NITA

NITA should not be the designated body to handle matters under the Bill. NITA is specialised only in the Information Technology area and it has various critical functions

---

21 For a commentary on UK's Data Protection Act see ps://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/#domestic. A similar exemption appears in section 67 of the Data Protection Act 2012 of Ghana.

under the NITA Act. A new and independent body would be required for this role. Additionally, NITA does not have a tribunal and yet there are tribunal-like functions required of the designated Authority responsible for overseeing the implementation of the Bill.

Recommendation

Establish a new independent body to take on the roles of NITA under the Bill.

5. CONCLUSION

The DPPB is a timely initiative to provide regulation for personal data and give meaning to Article 27(2) of the Constitution. However, provisions creating unnecessary exceptions should be left out if the Bill's principles are to have meaning. The Bill should also be more alive to the need to protect the personal information of marginalised and criminalised persons.

Contact us:

Human Rights Awareness and Promotion Forum (HRAPF

Plot 390 Prof. Apolo Nsibambi Road,Namirembe, Kampala
P. O. Box 25603, Kampala.
Telephone:+256-414-530683 Toll Free: 0800130683
Email:info@hrapf.org Website:www.hrapf.org
Facebook:hrapf.uganda
Twitter:@hrapf_uganda