DATA PROTECTION AND PRIVACY BILL, 2015

Comments Presented to the Committee on Information and Communication Technologies (ICT Parliament of the Republic of Uganda

Submitted By: Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

9 February, 2018

1. Introduction

The Constitution of Uganda, 1995, under article 27 provides for citizens' right to privacy. Uganda is also party to a number of international instruments that recognise the right, including the Universal Declaration of Human Rights (article 12) and the International Covenant on Civil and Political Rights (article 17).[1]

At the African Union (AU), the African Charter on Human and Peoples' Rights[2] does not provide for privacy and data protection. However, the AU Convention on Cyber Security and Personal Data Protection, which has been signed by 55 member states, is based on the principles of data protection and privacy.[3]

Besides this Convention, there are other initiatives linked to privacy and data protection in Africa, such as the Declaration of Principles on Freedom of Expression in Africa (2002) (Part V),[4] the Resolution on the Right to Freedom of Information and Expression on the Internet in Africa – ACHPR/Res. 362(LIX) 2016,[5] and the African Declaration on Internet Rights and Freedoms.[6]

At the sub-regional level, the Economic Community of West African States (ECOWAS) has adopted a Supplementary Act on Data Protection[7] which calls upon member states to legislate data protection and privacy.

Similarly, the Southern African Development Community (SADC) has a model law on data protection, developed in 2010 to assist member states combat unlawful data collection, storage, processing and transmission.[8]

---

[1] See also the General Comment No. 16 to the ICCPR, para 10, referring to State obligations to put in place measures that allow data subjects at request to have their data corrected or deleted. This General Comments is available at see also the resolution of the UN General Assembly on arbitrary collection of personal data, available at http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1; see also the call for an additional protocol to Article 17 ICCPR at the 35th Annual Conference of International Data Protection Commissioners to create globally applicable standards for data protection, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/13-09-24_International_Law_Resolution_EN.pdf. This foot not is majorly drawn from; Christopher Kuner, "Extraterritoriality and the Fundamental Right to Data Protection," available at https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/

[2] African Charter on Human and Peoples' Rights is available at http://www.humanrights.se/wp-content/uploads/2012/01/African-Charter-on-Human-and-Peoples-Rights.pdf

[3] African Union Convention on Cyber Security and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf

[4] http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html

[5] http://www.achpr.org/sessions/59th/resolutions/362/

[6] http://www.unesco.org/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/Events/netconference_march2015_submissions/reference_from_africaninternetrights_org.pdf.;

[7] The ECOWAS Supplementary Act on Data Protection is available at http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf

[8] The SADC model law on data protection is available at https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL DOCUMENTS/FINAL DOCS ENGLISH/sadc_model_law_data_protection.pdf

Closer to home, the East African Community (EAC) has no particular legislation on data protection and privacy. The EAC only has a Framework for Cyber laws which was developed in 2008.[9]

Whereas article 27 of Uganda's constitution provides for citizens' right to privacy, there is no law to protect an individual's data privacy yet different government departments, as well as private entities, on a regular basis collect individuals' data without any assurance of data protection or guarantee to ensure its privacy.

Some existing legislation, for instance the Computer Misuse Act, 2011 (section 18); Access to Information Act 2005 (section 26); Uganda Communications Act, 2013 (section 79); Electronic Signatures Act, 2011 (section 81); and the Regulation of Interception of Communications Act, 2010 (section 2) prohibit unauthorised access and disclosure of information. However, the provisions in these laws are not elaborate and do not adequately protect personal data.

Indeed, Uganda has in the past had individuals' rights to privacy violated through unlawful data breaches and disclosure. For instance, a number of women have been victims of non-consensual sharing of intimate images, including "revenge pornography", following unlawful access to their personal data.[10] There have also been reported cases of hacking and leaking of emails, with significant financial losses.[11]

Uganda has not ratified the AU Convention on Cyber Security and Personal Data Protection. With only 16 countries in Africa that have enacted Privacy and Data Protection laws, Uganda remains amongst the majority without safeguards in place to regulate the collection, storage and use of data.[12] The publication of a draft bill three years ago was therefore a milestone, and CIPESA welcomes the Parliament of Uganda's call for submissions on the Draft Data Protection and Privacy Bill, 2015. It gives an opportunity for stakeholders to provide input to ensure that the law, when enacted, measures up to internationally acceptable standards of data protection.

Below we highlight some of the positive principles and provisions of the Bill. Furthermore, we indicate areas of concern and suggest amendments to ensure that if the bill is passed into law, there are sufficient safeguards to regulate the collection, storage and use of data towards upholding citizens' right to privacy.

2. The Positives

The introduction of the Data Protection and Privacy Bill, 2015 is commendable due to the following:

i. There is no particular piece of legislation dedicated to addressing the issue of personal data protection in Uganda. This Bill will therefore buttress data protection in Uganda.

ii. The Bill, if passed into law, gives effect to article 27 of the Constitution which, inter alia, under clause 2 provides that, "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property."

---

[9] Further information on the Framework for Cyber laws is available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Harmonizing%20cyberlaws%20-%20East%20Africa%20Community%20.pdf

[10] Naked Ambition: Uganda Celebrities Whose Nude Pictures/ Sex Videos Have Leaked, https://www.howwe.biz/news/lifestyle/622/naked-ambition-ugandan-celebrities-whose-nude-pictures-sex-videos-have-leaked

[11] Leaked Emails: How Hacking Team and Uganda government want to spy on you, http://www.dignited.com/14494/leaked-emails-how-hacking-team-and-uganda-government-want-to-spy-on-you/; and Why Uganda should adopt cyber security breach disclosure Laws, https://www.newvision.co.ug/new_vision/news/1459747/uganda-adopt-cyber-security-breach-disclosure-laws

[12] DLA PIPER, "Data Protection Laws of the World", available at https://www.dlapiperdataprotection.com/ (accessed February 08, 2018); see also, Edrine Wanyama "What African Countries Can Learn from European Privacy Laws and Policies," available at https://cipesa.org/2017/07/what-african-countries-can-learn-from-european-privacy-laws-and-policies/

iii. The Bill is based on the principle of protecting privacy of the individual person.[13] Such protection shows state commitment to protecting and promoting rights of individuals at both the national and international level.

iv. The Bill outlines clearly, the rights of the data subject (i.e. the individual who is the subject of personal data) especially in relation to access to personal information (clause 20); prohibition of processing of personal data for direct marketing purposes (clause 22); compensation for damage caused by the data controller (clause 29) and a complaints mechanisms (clauses 27, 28, 29, 30, 31, 32 and 33).

v. The Bill, if passed into law, will give the data subject power to exercise some level of control over their data including collection, processing, correction and deletion of the same.[14]

vi. The Bill, if passed into law, will show Uganda's commitment to international laws and obligations in line with article 123 of the Uganda Constitution on the Execution of treaties, conventions and agreements.

vii. The Bill, if passed into law, will bar unscrupulous individuals from unlawful collection and processing of data and thereby protect the data subject against harm.[15]

viii. The Bill, if passed into law, will regulate and stop illegal cross border transfers of personal data.[16] This will serve to ensure that data subjects are guaranteed international protection in as far as their data and privacy are concerned.

3. Concerns Requiring Redress

Despite the above positive aspects, the following issues need to be addressed before the Bill is passed into law.

A. Interpretation

Clause 2 of the Bill provides for the interpretation of key terms used in the Bill, and we suggest the addition of a number of terms. Their absence from the Bill could lead to unwarranted data breaches. Hence, the following definitions should be added including:

i. **"Any person"** –includes natural persons and persons in the eyes of the law such as incorporated bodies and companies.

ii. **"Public Record"** defined as all records that have a bearing on or affect public service delivery.

iii. **"National security"** defined as the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests.[17]

---

[13] See for instance, the Long Title to the Data Protection and Privacy Bill, 2015, see also Part II on the principles of Data Protection, Part IV on security of data, part V on the rights of the data subject, Part VII on complaints and Part VIII on offences.

[14] Ibid, Clause 12

[15] Ibid, clauses 4 and 5.

[16] Ibid, clause 15.

[17] See for instance the definition of national security under article 238 (1) of the Constitution of Kenya, 2010, available at http://www.kttc.ac.ke/images/Constitution_of_Kenya.pdf; See also the definition of national security under section 2 of the Access to information Act, No. 13 of 2016 of Kenya, available at http://kenyalaw.org/lex/actview.xql?actid=No.%2031%20of%202016

B. An Independent Data Protection Commission

The Bill needs to provide for an independent data protection commission rather than the proposed National Information Technology Authority Uganda (NITA-U). An independent Data Protection Commission will ensure that that personal data processing is free from external or undue influence such as political pressure that might otherwise compromise the right to privacy of the data subject. The proposed Commission should be a fully-fledged organ with clearly defined roles and functions and leadership roles with representatives from government, private sector, academia, and civil society.

Other countries such as Ghana have established Independent Data Protection Commission under their Data protection laws.[18]

C. Consent to Data Collection and Processing

While clause 4(2) provides that the data subject should give consent to data collection and processing, the consent needs to be qualified for circumstances where collection and procession is done willingly or unwillingly.

Hence, clause 4(2) should read as follows: personal data may be collected or processed without the consent of the data subject where:-
(a)……..
(b)……
(c)…….

Furthermore, the grounds under which consent is deemed to have been fully obtained are not provided for by the Bill. Accordingly, provision should be made that prior to seeking consent, a data subject shall be informed of the circumstances and conditions under which the collection and procession of data will be done.

For instance, under regulation 39 of the European Union's General Data Protection Regulation, data processors and controllers must prior to processing of data inform the data subject of:[19]

a) The identity of the data controller.

b) The specific purposes of the data processing, which must be "explicit and legitimate and determined at the time of the collection of the personal data."

c) The period for which the personal data will be stored or, if that is not possible, the criteria used to determine the retention period.

d) The right to withdraw consent at any time.

e) Data subjects' rights to obtain confirmation regarding their personal data that will be processed, including the right to access, correct, or erase personal data.

f) The risks, rules, safeguards, and rights in relation to the processing of personal data.

g) How they may exercise their rights regarding the processing of their personal data.

---

[18] See for instance section 1 of the the Data Protection Act, 2012 for Ghana, available at https://www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf

[19] See for instance, Allyson Jones Labban, "*Informed Consent Under the EU's General Data Protection Regulation*", available at http://www.smithmoorelaw.com/informed-consent-under-the-eus-general-data-protection-regulation (accessed February 08, 2018). The General Data Protection Regulation (GDPR) is available https://gdpr-info.eu/.

D. Prohibition on collection and processing of special personal data (Clause 5)

While clause 5 prohibits collection and processing of special personal data, it is limited in scope and accordingly, it does not provide for all the possible categories of special personal data. The scope of this clause should be expanded to include information pertaining to:

i. Membership of a trade union/organisation

ii. Racial or ethnic origin

iii. Physical or mental health or other health condition

iv. Commission of an offence or an alleged Commission of an offence.

Exemptions under Clause 5 (2) (3) pertaining to the processing (with consent) of personal data for purposes of journalistic, literary, artistic or scientific purposes should promote creative expression, research and innovation.

E. Correction of Personal Data (Clause 12)

i. The heading of this clause reads only as correction of personal data yet the clause refers to both correction and deletion. The clause heading should be amended to read, "Correction and Deletion of Personal Data".

ii. Clause 12 (a) and (b) should strike a balance between correction and deletion and clearly state circumstances under which data may not be corrected following a request by a data subject. Every request for correction or deletion must be critically analysed before action is taken. . This will help to avoid deliberate deletion or correction of data with the aim of evading justice or contrary to public interest.

In determining whether correction or deletion of data should be effected, the following considerations are important and should be taken to account as they may offer the appropriate guidance:

a. Information of a private nature, such as health and medical records

b. Prior expectation of privacy

c. Information of public interest

d. Information of a public figure

e. Information deletion or correction will do/cause substantial harm

f. The necessity and relevance of information

Further, where, upon assessing the above processes of determining whether to correct or delete personal data, the data controller should inform the data subject within a prescribed time (within 7 days from the date of request) of the decision reached, that is whether to correct or not to correct and whether to delete or not to delete the subject information.

The communication to the data subject should, where correction is preferred, indicate the number of days within which data is to be corrected (3 days from the data of reaching the decision to correct the data).

If the data subject is dissatisfied with the decisions of the data controller, Part VII of the Bill on complaints should apply.

F. Retention of Records of Personal Data (Clause 14)

This clause should make specific reference to existing legal framework on national security and law enforcement so that there can be certainty as to when personal data should be retained and for what purpose as opposed to open exemptions that may be abused by data collectors and processors.

G. Notification of data security breaches (Clause 19)

Under this clause, a data collector, data processor or data controller is to immediately notify the authority where they believe that personal data of a data subject has been accessed or acquired by an unauthorised person. The data subject is to be informed later upon determination by the authority.

This information belongs to the data subject who should be immediately informed of such data breaches. Hence, the clause should cater for the data subject who should be immediately (within 2 days) be informed as soon as the data breach is discovered.

The clause could in the alternative read; Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorised person, the data controller or a data processor shall immediately notify the Authority and the data subject of the unauthorised access or acquisition, and in any event not more than two working days from the date of receipt of knowledge of the breach.[20]

Under clause 19 (3), the means of notifying the data subject of the data breaches especially through posting on the website of the responsible party and publication in the media are likely to aggravate breach of privacy rights. In the circumstances, notification through email, telephone calls and delivery of registered mail to the known residence or postal address of the data subject should be preferred. In using the above means, reasonable steps should be taken to ensure that the data subject actually receives the notification.

H. Regulation

While clause 34 empowers the Minister, by statutory instrument, to make regulations under the proposed law, there should be provision for an oversight role by Parliament in making the regulations.

[20] CIPESA, " CIPESA's Comments on the Draft Data Protection and Privacy Bill, 2014," available at https://cipesa.org/?wpfb_dl=184