UGANDA COMMUNICATIONS COMMISSION

COMMENTS TO THE ICT COMMITTEE OF PARLIAMENT ON THE DATA PROTECTION AND PRIVACY BILL 2015

The Uganda Communications Commission (UCC) welcomes the opportunity to comment on the Data Protection and Privacy Bill.

UCC associates itself with views of most Ugandans that the enactment of a law on data protection and privacy is long overdue. We are confident that a comprehensive law on the collection and processing of personal information would give effect to the right to Privacy as envisaged under Article 27(2) of the Constitution of Uganda.

UCC is generally happy that the proposed provision of the Bill will balance the concerns for both the business players and the right to privacy of the customers. The law will bring about a strong, more coherent data protection framework, backed by strong and coherent enforcement that will allow the Ugandan digital economy to thrive.

We welcome the protections offered by the Bill in terms of export of data, breach notification requirements, data subject access rights, automated decision making, compensation and the right to erasure and provision of sanctions for breach of the law.

We note the following;

1. **Clause 2 - Distinction between Data collectors and Data controllers and Processors**

   We propose that the definition and all reference to 'data collectors' be deleted in line with international practice and law that only define Data Controllers and Processors.

   Explanation

   The Data Protection and Privacy Bill in its definition section, Clause 2, distinguishes between Data Collectors, Data Processors and Data Controllers. This nomenclature is inconsistent with international best practice which provides for two broad categories of Data Controllers and Data Processors, which definitions cover what the bill refers to as 'Data Collectors'.

2. Clause 5 – Prohibition on collection and processing of special personal data

Clause 5 (1) - Current Text

A person shall not process or collect personal data which relates to the religious or philosophical beliefs, political opinion or sexual life of an individual.

Proposed Text

A person shall not collect or process data which reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs, or genetic data, biometric data and financial data or data concerning health or sexual life of a natural person for the purpose of uniquely identifying a natural person.

Explanation

Clause 5 of the Bill imposes additional obligations on data processors and controllers when dealing with special personal data. Under the Bill, special data is categorized as any information relating to 'the religious or philosophical beliefs, political opinion and sexual life of an individual'.

This categorization however does not include 'genetic, ethnicity, biometric, health or financial data.' Including these as special personal data would not only enhance protection of sensitive data from abuse but align the law with, Article 9 of the EU General Data Protection Regulation (GDPR) and other international best practice.

This is particularly key in light of recent events of unauthourised disclosure of personally identifiable health and financial information by some data processors and controllers.

3. Clauses 29, 32(2), 33 – Penalties

Current text

Clause 29 – Compensation for failure to comply with the Act.

(1) Where a data subject suffers damage or distress through the contravention by the data collector, data processor and data controller of the requirements of this Act, that data subject is entitled

to compensation from the data collector, data processor or data controller for the damage or distress.

(2) In proceedings against a person under this section, it is a defence to prove that the person took reasonable care in all the circumstances to comply with the requirements of this Act.

Clause 32 – Sale of personal data

(1) A person shall not sell or offer for sell personal data of any person.
(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty five currency points or imprisonment exceeding ten years or both.

Clause 33 – Offences by corporations

Where an offence under Section 29 or 30 is committed by a corporation, the corporation and every officer of the corporation who knowingly and willfully authorises or permits the contravention is liable for the offence.

Explanation

Clause 29, stipulates compensation for damages and distress without specifying any quantum. While Clause 32(2) of the Bill provides a financial penalty for sell of personal data, it is specific to sell of personal data and does not cover any other form of breach in the proposed law.

It is recommended that the quantum of these sanctions be tiered for natural and legal persons, with natural persons at the lower end of the spectrum and corporate persons at the higher end of the spectrum.

It is prudent that the law provides for commensurate, effective, proportionate and dissuasive penalties. Corporate entities are not only the biggest collectors of our personal data and information, but potentially the biggest offenders of data privacy rights and usually stand to benefit the most from such breaches, and hence, they ought to be subjected to higher standards.

The Anti-Money Laundering Act, Section 136 adopted a similar tiered approach to sanctions for natural and legal/juridical persons.

Similarly, we observe the current proposed quantum for penalties at two hundred forty five currency points across the board is low, we

recommend that the quantum of the penalty be increased as captured in the text below;

Proposed Text

Penalties

(1) A person who commits any offence prohibited under this Act is liable on conviction to:—

a) in the case of a natural person, imprisonment for a period not exceeding ten years or a fine not exceeding five hundred currency points or both;
b) in the case of a legal person by a fine not exceeding five thousand currency points.
c) if a continuing offence, by a fine not exceeding two hundred fifty currency points for each day on which the offence continues;

(2) Where it is necessary, for the purpose of convicting a person who has committed an offence, to establish the state of mind of the legal person, it shall be sufficient to show that a director, officer, employee or agent of the body corporate, acting in the course of employment of the director, employer or agent, had that state of mind.

4. Include special provision on Children and PWDs

Explanation

The Bill does not address the special needs to children and PWDs.

We propose that a special clause is added to provide for higher obligations on persons who deal with data on children and people with special needs. This fundamentally important because children and some PWDs may not be able to adequately protect themselves against data abuse.

Article 8(1) of the GDPR requires that where a Child's personal data is being processed on the basis of consent, that consent must be given or authorised by a parent.

Article 6(f) of the GDPR refers to situations where a data subject is a child as a particular example of where the legitimate interest ground for use of data collected for a different purpose may not be available.

The Article 29 Working (as it then was) also emphasised the requirement for controllers to have regard for the best interests of the child, as set out in the United Nations Convention on the Rights of the Child.

Practically, this would mean ensuring, default privacy-friendly settings are adopted, that minors are not targeted with direct marketing material, and that parental prior consent is obtained.

Proposed text

1. *A data controller or processor shall ensure, that where the personal data of children and people with mental disability is collected or processed;*

    a) *Explicit consent of the parent or guardian is obtained*

    b) *That the minor or PWD is not targeted with direct marketing material*

    c) *That adequate protection safeguards are put in place*

5. Data Portability

Explanation

The Data Protection and Privacy Bill in its current form does not provide for data portability as envisaged in Article 20 of the GDPR.

A data subject should be able to transfer his/her data from one controller or service provider to another if they so wish. This would not only enhance the rights of data subjects over their own data but improve competition among service providers.

This right would also allow data submitted from one business to be transferred another where technically feasible.

We propose that a section is added to allow for persons to have the choice to transfer their data from one service provider to another.

Proposed Text – Right to Data Portability

(1) *A data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is carried out by automated means.*

(2) In exercising his or her right to data portability pursuant to section 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

(3) The right to data portability referred to in section 1 shall not adversely affect the rights and freedoms of others.

6. Clause 32 - Sale of personal data

Current Text

Clause 32 – Sale of personal data

(1) A person shall not sell or offer for sell personal data of any person.
(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty five currency points or imprisonment exceeding ten years or both.

Explanation

Clause 32(2) of the Bill prohibits sale of data. The law ought to balance individual rights to privacy with not only business but other innovative uses of data, rather than hinder or encumber trade, perhaps sale of data should be regulated rather than totally prohibited.

We need to encourage the use of data for innovative and social good or for example where consent has been granted. Therefore, rather than prohibit sale of data, we recommend that the clause provides for a mechanism through which data sale or reuse can be regulated in order to facilitate utilisation of data, without compromising the rights of the data subjects.

The Minister may come up with comprehensive Regulations governing the sale of data, as envisaged under Clause 34 of the Bill.

Proposed text

Clause 32 – Sale of personal data

*(1) A person shall not without the **explicit consent** of the data subject sell or offer for sell personal data of the data subject.*

7. Data Protection/ Information Officers

The Bill could also consider obliging Public Controllers and Processors (Public bodies that hold data) and those that transact with significant amounts of personal information to appoint natural or corporate personalities responsible for Privacy and Data Protection - Mandatory data protection officers (DPOs).

In the alternative the head of a responsible public institutions could be held accountable as 'Information Officer' similar to the concept of the 'Accounting Officer', with relevant technical staff underneath, in line with the South African approach.

Proposed Text

(1) The controller and the processor shall designate a data protection officer in any case where:

a) The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b) The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to special personal or personal data relating to criminal convictions and offences referred.

(2) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of privacy and data protection.
(3) The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
(4) The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Authority.

8. Information fiduciaries

Explanation

Furthermore, the concept of 'information fiduciaries' should be taken into consideration.

In the law, a fiduciary is a person or business with an obligation to act in a trustworthy manner in the interest of another. Information Controllers and Processors could for example be required to comply with a set of fair information practices, including providing security and privacy guarantees.

This would enhance the accountability of Data Controllers and Processors to Data subjects.

Proposed Text - Accountability

(1) *The data controller shall be responsible for, and be able to demonstrate;*

a) *Implementation of data protection policies and measures to ensure that an organisation's data processing activities comply with the Act.*
b) *Data protection by design and data protection by default.*
c) *Record-keeping obligations*
d) *Cooperation with the Authority*
e) *Implementation of data protection impact assessments (DPIAs) for operations that present specific risks to individuals due to the nature or scope of the operation.*
f) *Prior consultation with the Authority in high-risk cases.*

Godfrey Mutabazi
Executive Director