CIPESA's Comments on the Draft Data Protection and Privacy Bill, 2014

Presented to the National Information Technology Authority - Uganda (NITA-U) and the Ministry of ICT, Republic of Uganda

February 09, 2015

The Collaboration on International ICT Policy in East and Southern Africa (CIPESA) welcomes the move by the Uganda Government through the National Information Technology Authority (NITA-U), Ministry of Information Communication and Technology (MoICT) and the Ministry of Justice and Constitutional Affairs (MOJCA) to secure digital citizens' privacy and data online by drafting the Data Protection and Privacy Bill, 2014. Following an analysis of the Bill, below are initial comments on areas of concern and gaps in the Bill that need to be addressed:

Section 4(2) gives broad grounds on which an individual is obliged to provide personal data. The vague terms in relation to data being collected and processed for matters of "national security" and "for the proper performance of a public duty by a public body" (**subsection 2 b (i))** need to be clearly defined to avoid misinterpretation and abuse. These phrases also appear in **Section 7.**

Section 6 requires an elaboration on what would constitute a "infringement of privacy". The lack of clarity creates a potential gap for the abuse of personal data by data collectors and processors.

Section 9 does not stipulate nor provide any guarantees on the safe keeping of the collected information to protect against misuse by unauthorised parties or for illegal purposes. These need to be clearly stipulated in the Bill.

Section 10 is not clear on what data qualifies as 'necessary' or 'relevant' and as such has no basis upon which to define 'excess data'. Clear parameters need to be provided for the kind and amount of data to be sourced and utilised by data collectors and processors.

Section 12(3) should include the reason why a data controller has not complied with the data correction request. There should also be set timelines for data controllers to comply with correction requests under **sub-section 2**. Further, in subsection 4, a timeline for a data controller to inform a person of the correction made on their data needs to be set.

Section 12 should also state the appeal mechanisms in case of denial of a correction of data request by a data subject. It should indicate the legal or alternative recourse a data subject has and the penalty for non-compliance with a data subject's request. For instance, if the data controller does not correct personal data upon request by the data subject, what recourse does the data subject have? Is it the courts of law, or the Authority? There should be a specified higher authority to which the data subject can file an appeal.

Section 14 is not clear on the data retention period and who determines this period. There should be clear specification of circumstances under which data collected is retained other than for national

security/investigation and court related purposes. The Bill should accommodate the principle for the 'Right to be forgotten'.[1]

Section 15 should state what happens when a data controller and a data processor do not provide for security measures for data stored. Penalties for defaulters need to be clearly stated here.

Section 18 attempts to support data subject notification in the event of a security breach. However, a specific period within which a data controller shall notify the data subject in the event of a security breach should be stipulated, rather than simply stating that the data subject should be notified "immediately". We therefore recommend to have this article changed to read as follows: *"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."***

Still under this section, notification of a breach through publishing on the website or in mass media may further compromise an individual's privacy. These measures should not be employed if any details about the particulars of the individual or of the breaches are to be communicated. Instead, telephonic notification may be added to email and to the last known residential or post address. The notification should, wherever applicable, be done through multiple channels.

Section 19 (2) should indicate the prescribed fee to be paid. We suggest that this fee should be a nomimal UGX 1,000 to make such requests affordable to all citizens. Besides, in instances where requests are made using electronic means such as via email, we suggest that requesters are exempted from making any payments at all.

Further, a clear definition of 'prescribed manner' under which data requests can be made needs to be provided.

This section also needs to indicate the formats in which personal data can be released, namely verbal, print, or electronic.

Sub-s**ection (9)** should indicate a timeline within which a data subject must receive a response from the data controller. The maximum **30 days proposed** for a data controller to comply with a request is too long and should be reduced to no more than 10 working days.

The 14 days provided under **Section 20 (2)** for notification of compliance, notification of intent or non-compliance to prevent processing are too many, as within that period further processing could potentially be ongoing. A clause for suspension of further processing within 48 hours of receipt of a request should be added, with the 14 days being the timeline applied thereafter for notice of compliance, notification of intent or non-compliance to requests.

[1]Right to be forgotten; http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

Collaboration on International ICT Policy in East and Southern Africa (CIPESA)
156-158 Mutesa II Road, 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

In the event of non-compliance with a request to prevent further processing and the Authority is not satisfied that the data subject is justified, there should be a clearly defined appeal process made available to the data subject. This also applies to **Section 21** which focuses on the right to prevent the processing of personal data for direct marketing**.**

Section 23 should be more specific on compensation for not adhering to this Act. As it is, there is no clarity on how compensation will be determined nor does it indicate the means for compensation. These should be included.

We also propose the establishment of an independent tribunal rather than the Authority as proposed in the Bill to settle cases that may arise in the event of no consensus between the data controller and data subject.

Section 26 needs to specify the formats in which the public can access information in the Data Protection Register. Suggested formats include: electronic, physical or both.

In addition the Authority should issue quarterly public reports on registered data collectors and the nature of any breaches recorded.

Under Part VIII on Offenses, a clause should be added that specifies the penalty for a data processor/ collector who through omission (such as negligence) or commission fails to secure a data subject's data, leading to its falling into unauthorised hands.

The fine of **120** currency points or five year imprisonment or both is financially lenient for unlawful disclosure. We therefore propose for an increment in currency points to **1000**. This penalty should also apply to a data processor/ collector for failure to secure data as aforementioned.

General comments:
The Bill should also seek to address:

- The establishment of mechanisms for obtaining consent from data subjects for further processing of their personal data;
- Set specific limits to retention period of personal data records;
- State provisions for third party jurisdiction i.e. processing and storage of data beyond Uganda's borders.

For further details on this submission, please contact:

Juliet N. Nanfuka
Communications Officer
Email: juliet@cipesa.org
Contact: +256 77 394 9345