Uganda's Draft

Data Protection and Privacy Regulations, 2020

September 2020

Introduction

The right to privacy is a fundamental human right that should have guaranteed protection nationally and across borders. Uganda being party to a number of international human rights instruments that guarantee this right, including the Universal Declaration of Human Rights (article 12) and the International Covenant on Civil and Political Rights (article 17), enacted the Data Protection and Privacy Act in 2019. The Act entered into force on February 25, 2019 following presidential assent. Its enactment marked a major step towards giving effect to article 27 of the Constitution of the Republic of Uganda, 1995. The draft Data Protection and Privacy Regulations, 2020 (regulations) which were published in August 2020, therefore come as another milestone towards specifying the procedural aspects for effective implementation of the Act. CIPESA welcomes the publication of the regulations, having earlier made submissions on the Data Protection Bill 2014 and 2015 and the Data Protection Act, 2019.

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) hereby offers some observations on the draft regulations in response to a call for submissions from the ICT ministry.

The Positives

Among others, the proposed regulations positively address the following:

1. They give effect to section 39 of the Act and thereby provide certainty in regards to implementation and enforcement of the provisions of the Act.

2. They spell out the roles, duties and obligations of the data collectors, controllers and processors while dealing with personal data. Thus far, enforcement of rights of the data subject in case of breach has been clarified especially in Part VII (regulations 32, 33, 34, 35, 36 and 37), which buttress the rights of the data subject.

3. They expound on the establishment of the Data Protection Office (regulations 3, 4, 5, 6 and 7) to manage personal data and specify the different roles and functions of the office. Breach of the specified roles and functions will entitle aggrieved data subjects to a remedy.

4. Furthermore, the regulations, specifically regulation 4, expand on the functions of the Data Protection Office (DP Office) to include coordination and guidance, capacity building, monitoring and regulating standards, undertaking research and issuing recommendations on interpretation of data protection rules. Specifying these functions and processes of securing personal data is key to ensuring that privacy of the individual is not only protected but also assured.

5 The regulations also provide some checks and balances during data collection and processing (regulations 8). Furthermore, the data subject may give their views and opinions including during the data protection impact assessment prior to collection or processing (regulation 10). This serves to ensure that the data subject is protected from unlawful actions that would wantonly lead to data breaches.

6 In order to protect children, regulation 9 reflects section 8 of the Act which seeks to ensure that data in relation to children is collected in a manner that does not violate their right to privacy.

7 The regulations, under part V (regulations 13, 14, 15, 16, 17, 19, 20, 21, 22, 23, 24, 25 and 26), provide for the procedures and basis upon which data collectors, processors and controllers may be permitted to collect, process and control individuals' data. Moreover, under regulation 18, a certificate of registration has a validity of 12 months from the date of registration. This is a preventive measure against unscrupulous individuals who would unlawfully collect and use individuals' data in violation of their right to privacy. Furthermore, it potentially provides an opportunity for evaluation of formerly authorised data collectors, processors and controllers before any further certificates are granted to them.

8 The regulations, in detailing aspects of data collection and processing (regulations 8, 9, 10, 13, 14, 24, 27, 28, 32, 33, 34, 35, 36 and 37) are also alive to the data subject's right to rectification or deletion of data upon request, especially where the data is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. This will serve to ensure that the individual has some control over their personal data.

9 The regulations, 14 (2) (k) and (3) and 28 (1-5), further protect data subjects whose data may be transferred across national borders by putting in place checks and balances on measures for data protection outside Uganda, and the data subject's consent before such data is processed. This guarantees protection of data subjects against unauthorised data processing. Moreover, this reflects article 44 of the General Data Protection Regulation (GDPR) on cross-border data flows and processing.

10 The data security practises and procedures in Part VI (regulations 29, 30, 31) provide standardised safeguards for data security. This aims to ensure that individuals' data is securely stored and protected by data collectors, data processors and data controllers. Moreover, data subjects are entitled to file complaints against data processors who are not compliant with the regulations. This is a measure that serves to enhance privacy of the data subject.

11 Furthermore, regulation 31 provides for immediate notification of the National Information Technology Authority Uganda (NITA-U) by the data collector, processor or controller where there is data breach under section 23 of the Act. This potentially facilitates real-time response and action against privacy breaches.

12 The regulations prescribe forms for data controllers, processors and controllers to make applications and for data subjects to lodge complaints in case of data breaches. This provides clarity on the procedures and steps to be undertaken by both the applicants and complainants. The forms further make the processes simple and clear.

Concerns for Redress

While the draft regulations are a major step towards ensuring the protection of privacy of the individual, they raise a number of issues that should be immediately addressed. The following section presents the key concerns.

Establishment of Personal Data Protection Office

Regulation 3 reiterates section 4 of the Act on the establishment of the Data Protection Office (DP office). Consequently, the DP office has some level of proposed independence from the National Information Technology Authority Uganda (NITA-U). However, the supervision of the DP office by the NITA-U board raises questions as to whether the office will be run independently. Moreover, there is no clear guarantee that the two offices are functionally different. Worse still, the regulations do not provide for independent financing of the DP office. By implication, the DP office is supposed to rely on finances from NITA-U, which potentially presents issues of cases of conflict of interest amongst the Board Members since they cannot easily handle matters of the DP office independent of those of NITA-U.

We therefore recommend that the regulations provide for the following:

- An independent Board for the DP office be established and appointed pursuant to section 4 of the Act. The board should be charged with the sole purpose of overseeing the management and administration of the DP office. This, if implemented, will lead to a more independent, accountable and transparent DP office.
- Provision for the financing and management of the DP office, including the scope of its powers. This will ensure that the DP office and its affairs are managed and operated independently from the direction of NITA-U. Given that the DP office is statutorily under NITA-U, an arrangement can be made to distinctly cater for the finances of the DP office in the NITA-U annual budget.

Management of Personal Data Protection Office

Regulation 5 reflects section 4 (2) and (3) of the Act in as far as it provides for the office of the data protection director and their appointment by the Minister. However, Regulation 5(5) gives NITA-U wide discretionary powers over the appointment of the director, with potential grounds for termination including broadscope for "any other reasonable ground" under regulation 5(5)(g). This may be abused for political reasons where the director may not be inclined to the wishes of the appointing authority. Moreover, the mode of appointment and termination potentially undermines independence of the director in execution of duties and functions.

We therefore recommend:

- The deletion of Regulation 5(5)(g), that is, "any other reasonable ground"

Objection to collection and processing of data

Regulation 8 alludes to section 7 of the Act by spelling out the grounds upon which a data subject may object to collection or processing of their personal data and accordingly notify the data collector, data processor or data controller of the objection. This is key to ensuring individual autonomy over their data.
However, Regulation 8(2)(b) is very wide in scope as it exempts the data subject's consent in respect to "legitimate interest" of a data processor or data controller. Moreover, legitimate interest in Regulation 8(3) is so widely defined that it provides numerous scenarios under which the data subject may not object to the collection and processing of personal data. Notably, the regulation defines legitimate interest as:

> *"the processing of personal data in a manner that the data subject would reasonably expect or where there is a compelling justification for the processing and includes the processing of data to prevent fraud, maintain network and information security, prevention of crime or threats to public security, internal administrative purposes, corporate governance requirements."*

These provisions undermine individual autonomy over personal data. Moreover, the interests of the data collector, data processor or data controller are placed above those of the data subject by waiving objection of the data subject to collection or processing of their data. These provisions run contrary to the internationally established data protection standards which provide for fair and lawful processing, ensuring transparency and accountability in participation of the data subject and adhering to the minimality principle.

We therefore recommend:

- The provision of clear guidelines for determining legitimate interest. The guidelines should further provide for auditing or endorsing of the legitimate interest by NITA-U before processing data is conducted.

Personal Data Relating to Children

Regulation 9 is wanting, in requiring data collectors, data processors and data controllers to establish systems to ascertain the age of persons whose personal data is to be collected, processed or stored, and the manner of obtaining consent of a parent or legal guardian. This shifts the duty of the authority to put in place procedural measures for securing personal data relating to children to data collectors, processors and collectors who are usually more concerned about getting data than securing it. It is highly doubtful that data collectors, processors and controllers can establish standard minimum measures for securing such data.

We therefore recommend:

- A clear guideline on how ascertainment of the age of persons will be made. This could be through the prescription of a specific form in the regulations that details the different aspects to be captured before data is collected from or about children. The guidelines will be essential for ensuring that parental consent is complete especially where the child does not understand the exercise. Further, they will offer guidance for extra safeguards for data relating to children.
- Provision for the use of clear and simple language whenever processing of data relating to children is concerned. This should be done including in communication or in gatherings or disseminating information.

Data Protection Register

Regulation 11 provides for a register which shall be maintained in accordance with section 29 of the Act. However, the requirement that the register may be in electronic or manual form presents uncertainties, since the DP office may choose the manual over the electronic. This may fail to take into consideration the current technological advancement where the world is highly digitised. It may also make records storage tedious while also making it harder to dispose of data which has served its purpose, such as through deletion.

On the other hand, we are also aware and concerned that a sole, electronic form of storage may lead to loss of data, which could include evidence in matters of law enforcement if unscrupulous individuals gain access to the register or record and destroy the data.

We therefore recommend:

- That the regulations provide for storage in both electronic and manual form.
  The regulation could therefore read as follows:

  "(1) The Data Protection and Privacy Register kept and maintained by the Office under section 29 of the Act shall be in both electronic and manual form."

Information contained in Register

Regulation 12 of the draft regulations provides that information to be contained in the register should include details of data collectors, processors and controllers and the purpose for which the data is collected. However, the regulation does not include the period for which the data should be stored. This could lead to unlawful storage of data beyond the performance of the intended purpose, which violates data protection principles and the rights of the data subject.

We therefore recommend:

- The addition of paragraph (e) on R.12(2) to as follows:
  "(e) the period for which the data is collected or processed."

Request to correct or delete personal data

Regulation 27 treats data being obtained unlawfully on an equal footing with inaccurate, irrelevant, excessive, out of date, incomplete or misleading data. Correction and updates are upon request of the data subject. Under Regulation 27 (2),(3),(4) the data controller may reject a request for correction or deletion. This potentially undermines the autonomy of the data subject over unlawfully obtained information.

We therefore recommend:

That the issue of personal data obtained unlawfully be dealt with differently from inaccurate, excessive, out of date or misleading data. There should be clear steps and measures by the data subject where personal data is obtained in an unlawful manner. Unlawfully obtained data need not be deleted on request as it should not be in possession of data controllers in the first place since it amounts to violation of the right to privacy.

Processing personal data outside Uganda

While regulation 28 makes attempts to regulate cross border data transfer and processing, it is not elaborate and exhaustive in its provisions. For instance, it will be important for data protection if the regulations provide details on aspects of transfers based on adequate level of protection and appropriate safeguards. These would work to ensure that data subjects are accorded an adequate level of protection within the internationally established principles, commitments, and human rights standards.

We therefore recommend:

- A more detailed provision for circumstances under which personal data may be processed in other countries including in:
  (i) Transfers based on adequacy decisions; and
  (ii) Transfers based on appropriate safeguards.

This will put the proposed regulations at the standard of the GDPR, specifically articles 45 and 46 which provide for data transfers based on adequacy decisions and appropriate safeguards.

Right to access personal information

Regulation 33, in line with section 24 of the Act, provides for the data subject's right to access personal information. However, Regulation 33(2) limits proof of identity of the data subject to (a) a national identification card or aliens identification card; (b) a passport or any travel document; or (c) a drivers licence. This may be delimiting since not all Ugandans may have the aforementioned documents. Moreover, some identity documents may be lost, yet the replacement process is long and burdensome.

We therefore recommend:

- The expansion of the documents required before one can access their personal information to include:
  - (i) Voter's card
  - (i) School Identity Card
  - (ii) Employer's identity card
  - (iii) Resident's identity card

Complaints Handling by Data Collectors, Data Controllers and Data Processors

Regulation 38 provides for development of a complaints handling system by every data collector, data controller and data processor. Such a system is important. However, multiple systems do not guarantee uniformity in the bid to protect the data subject.

We therefore recommend:

- Common and standardised guidelines which data collectors, data controllers and data processors should either use or emulate should be provided. This will provide certainty in the complaints handling system and will buttress data security.

Seeking assistance in investigation by the Director

Regulation 42 provides that the national personal data protection director may seek assistance in investigations for purposes of information gathering. This is important since soliciting information singularly through investigations may be hard. However, the regulation prescribes that assistance may be sought from any person or authority. This is so wide and may lead to abuse of the process especially where political sentiments and motives are involved. The provision should therefore be specific on the individuals or authority from whom assistance should be sought.

We therefore recommend:

- Provision for specific individuals or authorities from whom assistance in investigations should be sought.

Conclusion

The regulations are long overdue and should be issued to provide certainty as to how the Data Protection and Privacy Act, 2019 should be implemented. However, this should be done after paying attention to the concerns that need to be addressed. Addressing the concerns will buttress the intent and facilitate the effectiveness of the country's data protection legislation.

CIPESA

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