Submission of Comments on the Data Protection and Privacy Regulations, 2020.

About us

This submission is made by Unwanted Witness (UW) with the support of Privacy International (PI)

Unwanted Witness was registered in 2013 as a non-partisan and non-profit organization that use different media tools to amplify voices of the poor and vulnerable groups and add an active voice to initiatives that work towards demanding and promoting democratic governance.

Privacy International was founded in 1990. It is the leading charity promoting the right to privacy across the world. Based in London but working internationally through an international Network of partners which campaigns for legal and technological solutions to protect people and their data from exploitation.

Contacts

Dorothy Mukasa
Executive Director, Unwanted Witness
dorothy@unwantedwitness.org

Sempala Allan Kigozi
Legal Officer, Unwanted Witness
allan@unwantedwitness.org

Overview

Privacy is a fundamental human right. Protecting privacy in the modern era is essential to effective and good democratic governance. This is why data protection laws exist in over 120 countries worldwide including 28 African countries, and instruments have been introduced by international and regional institutions such as the African Union,[1] the OECD,[2] Council of Europe,[3] and ECOWAS.[4]

We welcome efforts by the Ministry of Information, Communications, Technology and National Guidance for formulating the draft Data Protection and Privacy Regulations, 2020 as mandated under section 39 of the Data Protection and Privacy Act, 2019.

The regulations are intended to the institutional mechanism for the enforcement of the data protection law, that gives life to and specify the right to privacy, already enshrined in Article 27 of the 1995 Constitution of Uganda, to deal with modern technologies and data processing.

The Data Protection and Privacy Regulations, 2020 has a number of shortcomings, and thus recommend that for effective protection of privacy and to meet international standards in protecting personal data, full consideration be given to the areas of concern and improvements outlined below.

Specific comments on the draft Regulations

3. Establishment of Personal Data Protection Office

We take the opportunity to once again express our concerns with the establishment of National Information Technology Authority – Uganda (NITA-U) as the data protection authority by the Data Protection and Privacy Act, 2019. We reject the NITA being appointed as the data protection authority for obvious concerns around independence from the Executive. Whilst Section (3)(2) alludes to the need to separate the activities of the Personal Data Protection Office (thereafter 'Office') from the affairs of NITA and tries to provide some safeguards but we are still not reassured by how these activities will be separated and managed independently in practice.

---

[1] See the African Union Convention on Cyber security and Data Protection, 2014, available at http://pages.au.int/infosoc/cybersecurity

[2] See the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013, available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonald ata.htm

[3] See the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 1981, available at http://conventions.coe.int/Treaty/en/Treaties/html/108.htm

[4] See the Supplementary Act on personal data protection within ECOWAS, February 2010, at http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf

We reject that the Board of NITA plays such a key role in the management and oversight of the Office given that the Board is appointed by the Minister of Information and Communication Technology and constituted as the governing body of the Authority. More safeguards need to be articulated to ensure the separation of powers and roles between NITA and the Personal Data Protection Office.

In addition, there is no information on the resources, both in terms of financial management and staffing, despite references to Office being given what it needs to undertake its mandate. Questions remain about the practical assurances being adopted to ensure the office has the resources it requires to effectively function and undertake its mandate such as an annual budget.

4. Additional functions of Personal Data Protection Office

This was already missing in the Act and the Draft Regulations fail to include in this section which outlines the powers and functions of the Office the ability of the Office to impose penalties/sanctions. It is thus unclear who will be responsible for the implementation of Part VII – Complaints and Investigations, and other sections which refer to the imposition of financial penalties.

5. National Personal Data Protection Director

In sub-section (5) of Section 5 there is no mention on the process for investigating and decision around reasons for terminating an appointment. Given link between NITA and the Executive, there is need a transparent process around this to ensure that such terminations are not politically motivated.

8. Objection to collection and processing of data

As we had highlighted when assessing Act Section 7(2) of the Act against international recognized data protection principles and standards this section of the Act still provides for too broad exemptions which must be narrowed down. Failure to limit the scope of broad exemptions risks undermining public trust if it seems that the government can evade from its obligation under the Act for the listed reasons without further justification. Blanket exemptions are not acceptable and the drafting of the regulations is a unique opportunity to clarify how to interpret those exemptions narrowly and specifically.

Sub-section 3 of Section 8 defines “public interest” in relations as to what a person can “reasonably expect”. This is not a good test as it places the onus on the data subject to have an understanding and control over how their personal data is being processed, and given the opacity of data processing activities individuals are not in a position to hold the information they need to make a comprehensive assessment.

9. Personal data relating to children

We would like the Ministry to clarify the language of ‘age verification’ and to provide further details on how this will be implemented. There is a need for the regulation or further guidance to

be developed on the need to adopt a risk-based and proportionate approach to age verification. Age-verification tools are still a developing area, and measures must be taken to guarantee data protection obligations are complied with in relation to collection and retention of that data, including data minimisation, purpose limitation, storage limitation and security obligations. Data collected for age-verification purposes must not be used for any other purpose.

13. Data collectors, data processors and data controllers to register with Office

The Data protection office should prescribe data collection thresholds for registration of data collectors, data controllers and data processors, and in making such determination, consideration should be put on(a) the nature of industry;(b) the volumes of data processed;

28. Processing personal data outside Uganda

As we had flagged in relations to the provisions on the transfer of person data outside of Uganda in the Act, the process outlined in Section 28 of the Regulations must be reviewed to include the involvement of the independent authority in assessing adequacy, the principles and specific safeguards processing must comply with as well as how it will comply with the rights of data subject including notification. Having said if the authority in charge of the Act remains the Office set-up within NITA, we would request that further measures be taken to separate the role of the Office in providing guidance on the processing personal data outside Uganda from the affairs of NITA.

We would like the Minister to clarify what does "nature" mean here under sub-section (2) of Section 28 of the Regulations.

29. Publication of personal data security practices and procedures

We would like the Minister to clarify how sub-section (3) will be implemented in practice in terms of checking enforcement and verifying that all data collectors, data processors and data controllers have complied with the demands when it comes to security.

31. Notification of data security breaches

Section 31 does provide a clear timeframe for notification and merely states "immediately" but without providing further details. Section 31 of the Regulation must be reviewed and a clear timeframe provided for in his section.

Section 31 also needs to provide a clear timeframe for notifying data subjects as provided under sub-section (5)(b). As we had highlighted with regards to clauses on data breaches in the Act w**e** are concerned that this process means that the data subject will be notified too late and will thus be unable to take necessary measures to mitigate risks of the breach. Consideration should be given to including an obligation to notify data subjects directly.

33. Right to access personal information

As the Minister is well aware questions of identity are complex in Uganda as a result of the way the digital identity system is being rolled out including concerns of backlogs and access to register for an identity car. As such any provision which requires providing a proof of ID is a not risk free in Uganda. The regulation lists some options of types of identity but must consider this not to be exclusionary or discriminatory given the situation on persons obtaining an identity in Uganda.

Part VII – Rights of Data Subjects

For all of these rights provided for in Part VII of the Draft Regulations there is a timeframe for the data processor to inform the data subject of its decision but there is no timeframe provided on how the data controller has to actually undertake the task of giving access to the data to a data subject, stopping the processing following the data subject objecting and/or withdrawing consent, to correct data as requested by the data subject, to delete data requested by the data subject, and prevent further processing.

33. Right to access personal information

Clause 24 (1) (b) of the Act merely required that data controllers give a 'description of the personal data' which is held by the data controller, and the Draft Regulations make a similar request but this is not sufficient. Individuals must be given copies of their data. The information provided to individuals requesting access should also be expanded to ensure that they are provided with all the information they are entitled to under their right to information but at the time that they are requesting access i.e. in relation to their specific personal data and not just a system in general (which is information that might be provided via a privacy notice).

The Draft Regulation should also make clear in what format the information should be provided to an individual and demand that this information be provided in a manner intelligible to them.

34. Right to prevent processing of personal data

Given the shortcomings of the Act with regards to the right to prevent processing of personal data under clause 25, the Draft Regulations must provide further clarification. There should be no requirement to demonstrate unwarranted substantial damage or distress as a result of the processing when exercising the right to prevent processing of personal data. Individuals should still have the right to object to processing under section 25.

42. Director may seek assistance in investigation

We are concerned about the broad nature of this provision which we foresee would permit law enforcement authorities, i.e. the police and intelligence/security agencies from being involved. Further clarify and guidance is required as to what this section entails in practice, and what measures are taken to ensure the rights of data subjects are protected throughout this process.

44. Appeals

We are concerned that the appeals process would be managed through the Minister, i.e. the Executive branch, especially given lack of independence already from NITA. There is a need to ensure independent oversight of such appeals through the Courts.

General comments on the draft Regulations

In addition to the above, we would like to bring to your attention various shortcomings in the Act which are not being addressed in the Draft Regulation.

Application of the Act

There are various elements which were missing and unclear in the Act with regards to the scope of application of the law which the regulations must address to clarify and avoid misinterpretations, these include:

- Clause 1 of the Act focuses on "Ugandan citizens" which raises concerns as to the rights of people with other legal statuses (migrants, refugees, etc.) who are data subjects in Uganda. What rights do they enjoy if they are not protected by the Act?
- There is no consideration in the Act for an exemption from any of the provisions for journalistic, academic, artistic, literary or human rights purposes. The draft Regulations should consider how to reconcile the Act with the right to freedom of expression.
- The definition of personal data in the Act under "Interpretations" fails to include data that can be used to identify someone both directly or indirectly. Including a more precise definition would therefore capture more processing activities and regulate more collection and other processing. The draft Regulations should clarify what constitutes 'personal data' personal data
- The definition of processing in the Act under "Interpretations" should have been broad and inclusive rather than exhaustive as it currently written. The draft Regulations must clarify what constitutes processing and in doing so take a more comprehensive approach to think innovatively and progressively to respond to current and future technological advancements in this definition. With this in mind, we would like to put forward the idea of specifically integrating the 'generation' of data as an activity which must be regulated and overseen, and for which individuals must be awarded protection.

Consent

Some of the exemption for requiring consent remained overly broad in the Act, and the draft Regulation must provide further details to address this shortcoming to ensure the rights of data subject guaranteed. In particular in relations to exemptions provided for under clause 7(2) of the act to ensure that the other conditions for processing (clause (2) (a), (c), (d) and (e)) are subject to the requirement that the processing be necessary for the purpose of that specific exception:

- Subsection (2) (a) which permits any collection or processing where the collection or processing is authorized or required by the law is overly wide in scope and intersects with clause 7(2)(e).

- Subsection (2) (b) (i) refers to 'public duty' but the Act fails to provide a definition for this term and this should be given further clarification.
- (Subsection 2) (d) refers to 'medical purposes' but the Act fails to provide a definition for this term. It is essential to further clarify what this could constitute by defining it either in the "Interpretations" or to further clarify it in this clause.

Processing of 'special categories of data'

Clause 9 of the Act omitted to include under "special personal data" various categories of sensitive personal data which are widely recognized in other jurisdictions as well as regional and international data protection standards.

The draft Regulations should address this shortcoming and provide guidance to ensure this clause of the Act includes all of the categories listed below and integrate them within the definition of sensitive personal data to ensure they are subject to a higher standard of protection.

At the very least, the law should adopt these standards to include:

i. racial or ethnic origin
ii. political opinions
iii. religious or philosophical beliefs
iv. trade union membership
v. genetic data
vi. biometric data
vii. data concerning health
viii. data concerning a natural person's sex life or sexual orientation
ix. criminal convictions and offences

Data retention

The regulation does not address shortcomings of the Act in relations to the international recognized principle and standards on data retention. The way it is currently phrased in the Act, the exemptions to the limitation of data retention listed in clause 18 (2) (a) to (f) provide broad powers to retain data for law enforcement and national security purposes, without reference to data retention laws that regulate those activities. This means that in accordance with this Bill there are no limitations to data retention for the purpose of law enforcement, and national security.

Sanctions and penalties

There is mention of currency points in various sections on the draft Regulations but there is limited information on how this would be decided, especially given the lack of clarity already noted about whether this falls within the powers and functions of the Personal Data Protection Office.

Secondly, the fines and penalties provided for in Regulation 13 (2), 14 (5), 28 (5), (32), 40 (7), and 46 are too small to deter any offender from violating the Act.

Compensation

We welcomed the recognition in Clause 33 of the Act that individuals can receive compensation as a result of damage and/or distress caused as a result of a data controller and/or data processor failing to comply with their data protection obligations.

As the law was not clear on the matter, it is important that the draft Regulations clarify that individuals are entitled to seek compensation for material and non-material damage i.e. there need be no pecuniary damage as a result of a breach.
Furthermore, the Regulations should clarify that the right to compensation individuals should have an overall right to an effective remedy for a violation of data protection provisions and this should include having access to the courts.

Collective redress

The Act did not provide the opportunity for collective redress which we had advocated for and which would align with the global recognition of such a process.

The information and power imbalance between individuals and those controlling their personal data is growing and collective complaints would ensure corrective action by organizations processing personal information, which would benefit all those affected. Provision should therefore be made in the process to allow individuals to be represented by qualified representatives and for certain qualified bodies, such as non-profit groups working in the field of data protection, to make complaints and seek remedies.

Delegated powers

The regulations need to address the concerns raised by Clause 39 on 'Regulations' and Clauses 40 on 'Power of the Minister' to amend Schedule of the Act. Currently under these clauses the Executive through the Minister is given broad powers to amend the Schedule and make regulations as requested and suggested by the Act, and they are in direct control of the 'Authority'. This means that they are ultimately in complete control of the data protection regime in Uganda.

The Act failed to reflect this concern and limit this power of the Executive but the draft Regulations must clarify and limit such broad powers and ensure necessary Parliamentary oversight and public scrutiny.

Transparency

Transparency is a key principle of data collection and yet the draft Regulations do not provide guidance on how to ensure this tenet provided for in Clause 3(e) of the Act i.e. an annual transparency report, which would be a good requirement for any on who collects and processes data.