PRIVACY INTERNATIONAL

Unwanted Witness
Amplifying voices

Submission of Comments on the Data Protection and Privacy Bill, 2015

About us

This submission is made by Unwanted Witness, and Privacy International (PI).

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, Privacy International works, within its range of programmes, investigates how our personal data is generated and exploited and advocates for legal, policy and technological safeguards. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

Unwanted Witness was registered in 2013 as a non-partisan and non-profit organisation 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.

Contacts

Dorothy Mukasa
Executive Director, Unwanted Witness
dorothy@unwantedwitness.or.ug

Ailidh Callander
Legal Officer, Privacy International
ailidh@privacyinternational.org

Alexandrine Pirlot de Corbion
Programme Lead, Privacy International
alex@privacyinternational.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 25 African countries,[1]and instruments have been introduced by international and regional institutions such as the African Union,[2] the OECD,[3] Council of Europe,[4]and ECOWAS.[5]

We welcome the effort by the Government of Uganda to give life to and specify the right to privacy, already enshrined in Article 27 of the Constitution of Uganda, to deal with modern technologies and data processing.

The Data Protection and Privacy Bill has a number of significant shortcomings. We recommend that to effectively protect privacy and to meet international standards in protecting personal data, that full consideration be given to the areas of concern and improvements outlined below under each Part of the Bill.

[1] See Graham Greenleaf, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey (2017) 145 Privacy Laws & Business International Report, 10-13, UNSW Law Research Paper No. 45available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035
[2] See the African Union Convention on Cyber security and Data Protection, 2014, available at http://pages.au.int/infosoc/cybersecurity
[3] 3See 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/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[4] 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
[5] 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

PART 1 – PRELIMARY

Clause 1 Application of the Act

Clarify who the law applies to

Clause 1 stipulates that the Act applies to "any person, institution or public body collecting, holding or using personal data".

Further clarification is requested in order to define "institution", and if it does not already "institutions" should be extended to include all government bodies.

Additionally, this clause and all of the provisions thereafter fail to explicitly stipulate if and how the Act applies to the private/ corporate sector. Under clause 2, "public body" is widely defined to capture corporations established by an Act of Parliament relating to undertakings of public services, but clause 1 fails to make explicit whether the Act applies to corporations and the private sector even where they are not related to the undertaking of public services. It is vital to achieving comprehensive data protection that the Act also applies to the data processing activities the corporate/ private sector and this is clear on the face of the legislation.

In clarifying the scope of the application of the law, it should be noted that it is widely accepted that processing for domestic or household purposes is exempt from application, we note this is not included on the face of this Bill. Some jurisdictions include further criteria to this exemption. For example, the GDPR also requires that it be "with no connection to a professional or commercial activity" (Rec. 18). In an online world, where the lines between professional and personal are increasingly blurred, consideration should be given to how this exemption is defined and explained to data subjects.

The current Bill fails to clearly establish the territorial scope of application of the law.
In order to provide its residents with access to the highest data protection safeguards and the enjoyment of their fundamental rights, the law should provide for extended jurisdictional scope to apply to any entities established in Uganda or processing personal data of individuals who are in Uganda.

Therefore, the law should apply to:
- processing of personal data by entities, data controllers or processors, established in Uganda, regardless of whether the processing takes place in Uganda or not.
- processing of personal data of individuals who are in Uganda by entities, controllers or processors not established in Uganda, where the processing relates to i) offering goods or services to data subjects in Uganda or ii) monitoring their behaviour within Uganda.

We note that there is no consideration in the Bill for an exemption from any of the provisions for journalistic, academic, artistic, literary or human rights purposes. Consideration should be given to how to reconcile this law with the right to freedom of expression.

Clause 2. Interpretations

Clarify definitions

"Data collector"
This is not a term that is commonly found in data protection frameworks, and we would like to request that the Act provides further clarity on who this actor is which does not fall within the activities/ definitions of 'data controller' and 'data processor'. This term is referred to throughout the Bill but ambiguity as to whom this refers to provides uncertainty as to whom the Act applies to as well as the obligations of actors involved in the processing of personal data.

"Information"
We would like to request clarity as to why the term '*information*' was included under "Interpretations" and if it is to be kept we suggest for this definition to be reviewed to respect legal and technical definitions of what constitutes *information* versus *data and personal data.*

"Personal data"
The definition of personal data in its current form included 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.

Alternative language for suggestion: *"personal data shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*."

We would recommend that the committee addresses this issue of indirectly identifiable data in the law and if necessary adopt measures requiring the independent competent authority to develop guidance and keep this issue under review.

"Authority"

The Bill fails to establish an independent data protection authority.The National Information Technology Authority – Uganda (NITA-U) does not constitute an independent authority given it is under the general supervision of the Minister of Information and Communication Technology (MoICT). The NITA-U Board of Directors, which is the supreme governing body of NITA-U, is

appointed by the Minister of Information and Communication Technology and constituted as the governing body of the Authority.

The Bill must include the establishment of an independent data protection authority to supervise the way in which a body or an individual uses other individuals' personal data. This body is essential in order to ensure the enforcement of the data protection framework.

The Act must stipulate that the independent data protection authority will be given sufficient resources, both financial and human, and remain administratively independent, to effectively and adequately fulfil its mission of enforcing the data protection framework.

This authority must be given the authority by the Data Protection and Privacy Act to conduct investigations, act on complaints by issuing binding orders and impose penalties when it discovers an individual, institution or other body has broken the law. Our views on this are set out in more detail in relation to clause 28 below.

"Processing"
Essential to data protection and privacy law is to establish clearly a comprehensive definition of processing.

The definition of 'processing' should be broad and inclusive rather than exhaustive. We would encourage the committee 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.
Suggested language may be as follows:

> *Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –*
>
> *(a) organisation, adaptation or alteration of the information or data,(b) retrieval, consultation or use of the information or data,(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or*
> *(d) alignment, combination, blocking, erasure or destruction of the information or data.*

PART II – PRINCIPLES OF DATA PROTECTION

Clause 3. Principles of Data Protection

Present clear and coherent principles

Specific purpose

There is no purpose specification principle included for the data processing under the principles in Clause 3. This is not addressed in the Bill until clause 8. This is a key principle of data protection enshrined in the data protection principles of various data protection frameworks around the world, therefore for clarity in the structure of the Bill we recommend that the principle of purpose specification is included within the principles of data protection. The principle should be clear that personal data shall be collected for specified, explicit and legitimate purposes.

Quality of the data
It is unclear what is defined as *quality* in the principles and this is not made clear until clause 11 of the Bill. It is requested that Clause (3) (1) (e) of the Bill be reviewed to specify that the data collected to be "*accurate and, where necessary, kept up to date*".

An additional requirement must be included requiring that every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified without delay.

Security safeguards
We welcome the inclusion of this principle. However, Clause (3) (1) (d) needs to further qualify the type of '*security safeguards'* which should be adopted and therefore we suggest the clause be reviewed to say: "*observe adequate security safeguards in respect of the data."* The details of the security requirements should then be expanded upon further in the detail of the Bill.

Accountability
We welcome the inclusion of an accountability principle in clause 3(1)(a). However, it is imperative that the principle of accountability includes a requirement to be responsible for and to demonstrate compliance with the other data protection principles. Important organisational measures for demonstrating compliance include data protection/ privacy impact assessments, appointment of data protection officers, data protection/ privacy by design and by default requirements and record-keeping obligations. This is currently missing from the Bill but needs to be set out in law and can be supplemented by Codes of Conduct/ Practice and guidance from the Independent Data Protection Authority and as relevant, sector specific guidance, developed through public consultation and collaboration with the Data Protection Authority.

PART III – DATA COLLECTION AND PROCESSING

Clause 4. Consent to collect or process personal data

Clarify conditions for processing and ensure adequate safeguards are in place

Consent is a core condition of data protection which allows the data subject to be in control of when their personal data is processed, and it relates to the exercise of fundamental rights of autonomy and self-determination.

Clause 4 fails to define and provide conditions for 'consent'. It is requested that consent be defined to include requirements that consent be *"freely given", "specific", "informed"* and "*unambiguous*" be included to qualify the consent obtained from the data subject and that this be demonstrated by a statement of by a clear affirmative action signifying an individual's agreement to the processing. The conditions for this consent should be elaborated further in the Bill to ensure that data controllers are able to demonstrate that an individual has consented, that requests are consent are written in a clear, intelligible and easily accessible form and that individuals are free to withdraw their consent at any time, which is to an extent included in clause 4(3).

This would ensure that consent is qualified to mean that the data subject has freely given his/ or her specific and informed indication of his or her wishes thereby signifying her or his agreement for personal data relating to her or him being processed.

Exceptions to the requirement to obtain the prior consent of the data subject should be limited and clearly defined. This creates clarity for individuals and those processing personal data and helps to prevent from abuse.

Therefore, we would suggest that clause 4(2) is amended to ensure that all 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 authorised or required by the law is overly wide in scope and intersects with clause 4(2)(e).
- Subsection (2) (b) (i) refers to 'public duty' but the Bill fails to provide a definition for this term and this should be given further clarification.
- (Subsection 2) (d) refers to 'medial purposes' but the Bill 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.

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

Clarify definitions and conditions for processing

Clause 5 omits to include under "special personal data" various categories of sensitive personal data which are widely recognised in other jurisdictions as well as regional and international data protection standards.

We strongly encourage the committee to consider the different 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

Clause 5(2) provides a specific condition for information controlled under the Uganda Bureau of Statistics Act, consideration should be given to what safeguards are in place to protect sensitive personal data.

The conditions in clause 5(3) permitting the processing of sensitive/ special category personal data should be specific and clearly defined.

Both the exemptions in clause 3(a) and (c) must be subject to the requirement of necessity and clause 5(c) should require that appropriate safeguards are in place.

Furthermore, the Act needs to define what '*given freely'* means and elaborate on definition and conditions of '*consent'* in Clause 5 (3) (b) in relation to the collection and processing of special personal data.

Clause 6. Right to Privacy

Link to the constitutional right to privacy

Article 6 refers to the right to privacy but it omits to make direct reference to the Constitutional protection of the right to privacy under Article 27:

Right to privacy of person, home and other property.

(1) No person shall be subjected to-

(a) unlawful search of the person, home or other property of that person; or

(b) unlawful entry by others of the premises of that person.

(2) No person shall be subjected to the interference with the privacy of that person's home, correspondence, communication or other property.

It has been over 20 years since the promulgation of 1995 Constitution and Uganda has not yet enacted the requisite law to enforce Article 27. A legal framework is needed that would create an enforcement mechanism and provide for redress where infringement occurs.

We recommend that the Bill includes a direct reference to the right to privacy as articulated by Article 27 of the Constitution of Uganda, and that the Government and Parliament further develops legal frameworks to protect privacy.

Clause 7. Collection of data from the data subject directly

Clarify exemptions

Clause (7) (2) (c) reads that "*...personal data may be collected from another person, source or public body where – the data subject consented".* Given our concerns mentioned above on the lack of definition of and conditions for 'consent', this provision must be reviewed to provide clarity on those two points in relational to consent.

Clause (7) (2) (c) reads that "*...personal data may be collected from another person, source or public body where – the collection of the data from another source is not likely to prejudice the privacy of the data subject".* We request that the term '*not likely to prejudice'* be reviewed or amended to provide further clarity as to what this constitutes as well as process for providing evidence for it.

Paragraph (7) (2) (g) reads that "*...personal data may be collected from another person, source or public body where – it is not reasonably practicable to obtain the consent of the data subject"*. The term "reasonably practicable" presents an opportunity for loose interpretation as to what this means and fails to impose a robust threshold on when consent does not have to be sought from the data subject.

Clause 8. Collection of personal data for specific purpose

Include purpose specification in the data protection principles

Purpose specification and use limitation are key principles of data protection. We would therefore recommend that all data protection principles provided for in the law be listed at the onset under Part II – Principles of Data Protection. As we noted, Clause 3 under Part II – Principles of Data Protection currently fails to explicitly provide for principle of purpose specification.

Clause 9. Information to be given to data subject before collection of data

Provide more information in a clear manner

The right of individuals to know what personal data that controllers hold on them is a fundamental component to data protection law.

The UN Human Rights Committee, in interpreting the scope of obligations of states parties to the International Covenant on Civil and Political Rights, noted, back in 1989, that:

> *"In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination." (Human Rights Committee, General Comment No 16 on Article 17 of ICCPR.)*

In addition to the type of information listed in Clause 9 (1)(a)-(i), the data subject should be provided information on:

- all rights of a data subject (including the right to object/ to withdraw consent)
- the purpose of collection and processing;
- how the data is collected and processed including the existence of automated decision-making and/or profiling and meaningful information about the logic involved;

Furthermore, we would recommend amending Clause 9 (2) as follows:

- where the personal data have not been collected directly from the data subject, they should be provided with information about the source of the data;
- further clarity on what constitutes "as soon as practicable". In other jurisdictions a specific timeframe is provided in number of days, for example as soon as possible and at the latest within 30 days.

Consideration should also be given to including requirements as to the form in which this information/ notice is provided i.e. it should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Finally, all the exemptions (a)-(e) provided for in Clause 9 (3) are overly broad and provide for blanket exemptions, these must be subjected to clearly and narrowly defined conditions. At the very latest they should include the requirement of 'necessity' and that the failure to apply to exemption will cause demonstrable harm/prejudice. If data is withheld from an access request on the basis of any such exemption, this should be explained to the data subject.

Clause 10. Minimality and Clause 11. Quality of information

Include data protection principles

As noted above, for the sake of clarity in the structure of the Bill, ensure that these principles – data minimisation and accuracy – are fully reflected in the data protection principles in clause 3.

Clause 12. Correction of personal data

Clarify the right

It is important to make clear from the onset to the data subject the timeframe to exercise their rights, and also the fact they can make suggest demands for free. There should be no cost in exercising this right. While some legislations allow the charging of reasonable costs, that is not the case in other legal frameworks such as under GDPR and this approach should be adopted in Uganda where many still leave in poverty and where even a relatively small cost may be a significant financial burden to the exercise of individual rights.

Clause 13. Further processing to be compatible with purpose of collection

Clarify and limited the provisions

This Clause must clearly reaffirm that in addition to respecting the principle of purpose specification any "further processing" must also comply with all the principles of data protection provided for in the law as well as be subject to all appropriate safeguards. With this in mind Clause 13 (2) (f) must follow on from (e) to read, *"**and** the further processing of the data is in accordance with this Act including the principles for data protection and safeguards it provides for elsewhere in the Act."*

Furthermore, we would like to demand clarity as to what the term "*likely to reveal"* means in Clause 13 (2) (e) (ii). This ambiguity raises concerns. In the era of data link ability, and de-anonymisation of data sets, and with the development of artificial intelligence, we are also concerned that other forms of data can become personal data as they would lead to an individual being uniquely identified and identifiable.

Clause 14. Retention of records of personal data

Limit exemptions and provide adequate safeguards

Storage limitation and data minimisation are key concepts of data protection both from an individual rights and information security perspective. The law should clearly stipulate that data should not be kept for longer than necessary for the purpose for which it was originally obtained. Any exceptions to this must be very limited and clearly defined.

The way it is currently phrased, the exemptions to the limitation of data retention listed in clause 14 (2) (a) to (f) provides 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.

The various provisions under this Clause must be revised to ensure that any data retention policy meet the test of necessity for the purpose specified as well as providing for effective safeguards.

Furthermore, Clause 14 (3) should ensure that any retention be necessary for the purpose specified at the point of collection.

In particular, we would like to raise concerns with the phrasing of Clause 14 (4) and (5) around retention of data in de-identified form and "reconstruction in an intelligible form". If data is to be stored beyond the retention period in an anonymised (and not pseudonymised) form the privacy implications and any consequences for the data subjects must be carefully considered.

Clause 15. Processing personal data outside Uganda

Provide adequate safeguards for transfers

This clause fails to clearly provide a process for data processing outside Uganda and cross-border sharing**.** This process must be further developed 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.

Clause 16. Security measures

Elaborate on security measures

On a general point, we would request that this clause specify and elaborate on security measures that must be undertaken prior to collection of personal data.

Furthermore, we request clarity on the following terms:

- Clause 16 (1) reads that "reasonable" measures must be taken but it is unclear what conditions will be considered to make this assessment;
- Clause 16 (3) reads that "A data controller shall observe *generally accepted information security practices and measures"* but fails to provide further clarity as to what this constitutes and there is a concern that this obligation remains vague.

Clause 17. Security measures relating to data processed by data processor

Ensure responsibilities of data processors

This clause is vague and fails to clearly define the relationship between the data controller and data processor as well as the obligations for each category of actor. There is a need to rectify these shortcomings.

Clause 18. Data processed by operator or authorised person

Clarify terminology

We would like to request clarity as to whom the term "operator" refers to in Clause 18 (1). This term is not defined under "Interpretations" in Part 1.

Clause 19. Notification of data security breaches

Provide a timescale for notification and direct notification to data subjects

The law should also contemplate a timescale for notification to data subjects. In other jurisdictions, a specific timeframe is provided in number of hours after becoming aware of a breach, for example 72 hours.

Finally, we are concerned by Clause 19 (2), which provides that "*Authority shall determine and notify whether the data controller should notify the data subject of the breach."* We 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 the risk of the breach. Consideration should be given to including an obligation to notify data subjects directly.

It is imperative that for a breach notification to be meaningful for data subjects, the notification should be in clear and plain language and includes advice and the tools to take measures to protect from harm and to seek redress from harm suffered.

PART V – RIGHTS OF DATA SUBJECTS

Clause 20. Right to access personal information

Provide a copy of data and more information about processing activities

The right of individuals to know what personal data that controllers hold on them is a fundamental component to data protection law.

Clause 20 (1) (b) however only requires that data controllers give a 'description of the personal data' which is held by the data controller. 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). Consideration should also be given as to the format in which the information should be provided to an individual in order that it is intelligible to them.

Furthermore, the language in Clause 20 (2) remains vague and should clarify and define what is meant by "*in the prescribed form and manner."* This should be clarified on the face of the Bill as opposed to through regulations. It should also be made clear, as with other rights, that the right can be exercised for free.

Finally, we would encourage the committee to consider including a right of data portability in a data protection law in order to ensure that the data subject is placed in a central position and has a full power over his or her personal data. This would permit individuals to request that their data be made available to them in a universally machine-readable format or ported to another service with the specific consent of that individual.

Clause 21. Right to prevent processing of personal data

Clarify the right

The right to prevent processing of personal data in clause 21 requires clarification. Clause 21(5) provides that this right does not apply to data collected or processed in accordance with section 4(2), which excludes any other conditions for processing other than consent. Where personal data is processed on the basis of consent then there should be (as indicated in clause 4(3)) individuals have a right to withdraw consent at any time, there should be no requirement to demonstrate unwarranted substantial damage or distress as a result of the processing. Individuals should still have the right to object to processing under clause 4(2).

Clause 22. Right to prevent processing of personal data for direct marketing

Make the right absolute

The right to object to personal data being processed for direct marketing purposes should be absolute. The data subject should be informed of this right and the controller obliged to cease processing their personal data as soon as this right is exercised.

Clause 23. Rights in relations to automated decision-making

Provide for a prohibition and strengthen the right

Both profiling and automated decision-making may lead to unfair, discriminatory and biased outcomes. There is international recognition of the potential harms, in the words of the United Nations Human Rights Council:

> *"automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights." (UN General Assembly, Human Rights Council: resolution / adopted by the General Assembly, 22 March 2017, A/HRC/34/L.7/Rev.1)*

Clause 23 must be revised as currently the onus is on the data subject but such a right should constitute a prohibition and thus protect data subjects by default. Clarification should also be provided to ensure that the use of the word 'solely' does not include decisions where human involvement is fabricated and consideration should be given to how a meaningful right to explanation of the automated decision can be included within this provision.

Any exemption to this prohibition should be clearly and narrowly defined. This is particularly important as automated decision-making increasingly relies on advanced and complex processing and as a result can be difficult to interpret or audit, yet can still produce decisions that are inaccurate, unfair or discriminatory.

In particular, we are concerned with the broad, wide-ranging exemptions provided for in Clause 23 (4)(a)-(e). As noted above, automated-decision is prevalent and can significantly impact on individuals and the fundamental rights. Exemptions provided for in this section must be revised to ensure they are clearly and narrowly defined.

For a discussion of rights in relation to automated decision-making and profiling in a data protection framework and how these could have been better addressed in the GDPR and accompanying guidance, please see Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR by Frederike Klatheuner and Elettra Bietti, Winchester University Press (2018),[6] as well as the 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 of the Working Party on the Protection of Individuals with regard to the processing of personal data (Article 29).[7]

Clause 24. Rectification, blocking, erasure and destruction of personal data

Clarify the provision

We would like to seek clarity as to how this clause relates to the right of data subjects provided for in '*Clause 12 Correction of Personal Data'* to directly exercise their right in relations to the obligations of the data controller.

[6] Available at: https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45/36
[7] Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47742

PART VI – DATA PROTECTION REGISTER

Clause 25. Data Protection Register

Provide more detail as to the operation of the Register

Given the lack of clarity on the application of the Act as a result of the ambiguity and shortcoming of Clause 1, it is unclear who would be required to register themselves.

Clause 26. Access to register by the public

Ensure the Register is accessible

We would like to seek clarify as to what "inspection" means in this Clause. There is a need to clarify the process and protocols for enabling the public to access the register.

Clause 28. Authority to investigate complaints

Improve enforcement capabilities of the independent authority

This is the only clause which outlines the powers of the 'Authority'. If an independent supervisory authority is established, which requires reviewing the decision of Uganda to appoint the NITA-U as the supervisory authority, it is our position that an independent supervisory authority should have other powers than to investigate and their power to investigate must include the ability to inspect, impose fines and enforcement orders.

This clause also needs to provide further details on the types of remedies that would be available and in particular elaborate on penalties by clearly stating the amounts. It is important that penalties reflect the gravity of the violation, that they have a deterrent effect and that the upper limit of penalties is clearly stipulated in the law in order that controllers and processors understand the potential financial implications of a breach and to act as an adequate deterrent. In order to achieve this deterrent effect, enforcement is key and therefore the factors that the data protection authority would take into account in imposing a monetary penalty, should also be set out in the law.

Accountability and enforcement are key to ensure compliance with the data protection law. An independent supervisory authority with clear and well-defined powers is essential to monitor and regulate compliance, take measures in case of non-compliance and protect the rights of data subjects. Without independent, effective accountability and enforcement, there is reason to doubt

the impartiality, fairness and the effectiveness of this law altogether and it may affect whether those processing take the law seriously and the confidence of the public to rely on the legal framework for protection.

Clause 29. Compensation for failure to comply with this Act

Provide effective remedy and collective redress

We welcome the recognition in Clause 29 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. It is important that the law is clear 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.

As well as a 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.

The law should also include provisions for collective redress. The information and power imbalance between individuals and those controlling their personal data is growing and collective complaints would ensure corrective action by organisations 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.

Clause 30. Appeals

Provide independent oversight

Consideration should be given to whether appeals against a decision of the Authority should be made to the Minister or rather via the Courts.

Clause 33. Offences by corporations

Correction of references

We would like to take the opportunity to point out that reference to Clause 29 and 30 appear to be incorrect. We believe that that the Clauses which must be referred to are Clauses 31 and 32.

Clauses 34. Regulations and Clauses 35. Power of the Minister to amend Schedule

Limit delegated powers to ensure effective Parliamentary scrutiny

We are concerned by the broad regulation making powers given to the Minister. Such a decision removes parliamentary oversight and empowers the executive to take away the rights of individuals without the checks and balances afforded to primary legislation through the parliamentary process. This is particularly concerning in the case of Uganda and the current decision to appoint the NITA-U as the 'Authority' under this Bill. The NITA-U is under the general supervision of the Minister of Information and Communication Technology (MoICT) and its Board of Directors, which is the supreme governing body of NITA-U, is appointed by the Minister of Information and Communication Technology.

Therefore, if the Executive through the Minister is given broad powers to amend the Schedule and make regulations as requested and suggested by the Bill, and they are in direct control of the 'Authority' that they would ultimately have complete control of the data protection regime in Uganda.

These two clauses must be amended to limit such broad powers and ensure necessary Parliamentary oversight and public scrutiny.

Removal of these powers and providing detail in the Bill and Schedules would also provide clarity and foreseeability to those processing data and individuals as to what their obligations and rights are.