



UGANDA: DATA PROTECTION AND PRIVACY BILL, 2015 LEGAL ANALYSIS

OPPORTUNITIES & GAPS

**UGANDA:
DATA PROTECTION AND PRIVACY BILL, 2015
LEGAL ANALYSIS**

OPPORTUNITIES & GAPS

TABLE OF CONTENTS

| | |
|---|---|
| 1. INTRODUCTION | 4 |
| 2. BACKGROUND TO THE DATA PROTECTION AND PRIVACY BILL, 2015 | 6 |
| 3. EXISTING LEGAL FRAMEWORK | 7 |
| 4. SALIENT CLAUSES IN THE BILL | 9 |

INTRODUCTION

The government of Uganda has now introduced a comprehensive law to deal with data protection and privacy of the individual. The Privacy and Data Protection Bill, 2015 (hereinafter referred to as the "PDP" Bill) is now awaiting approval by Cabinet and introduction to Parliament for debate and ultimately enactment. At this stage of the legislative process, the citizens and CSOs are given chance to contribute to the proposed law. It is therefore necessary to identify gaps and submit proposals for amendments before enactment as well as making appreciation of progressive clauses and advocating for retention of the same in the state that is desirable for the data and privacy of the individual.

The purpose of this brief is to review the Bill, provide an analysis of each Part of the Bill, clearly highlighting the positive aspects. It is also principled on identifying and analyzing the existing gaps with the aim of making concrete recommendations for an improved Bill.

Article 27 of the Constitution of the Republic of Uganda, 1995 (Constitution) guarantees the right to privacy of person, home and other property. In particular article 27(2) of the Constitution provides that a person shall not be subjected to interference with the privacy of that person's home, correspondence, communication or other property.

Whilst there is no comprehensive law giving effect to article 27, large amounts of data concerning individuals are collected, stored or processed regularly by various institutions in the private and public sector including banks, hospitals, hotels, insurance companies, the Uganda Citizenship and Immigration Control Board, the Uganda Revenue Authority, Uganda Registration Services Bureau, the Electoral Commission, utility service providers and telecommunications companies under the SIM card registration exercise. As these are taking place in a legal void, with no established safeguards for data storage, protection, processing and usage.

Though with no clear legal framework on data protection and privacy, section 18 of the Computer Misuse Act, 2011 'prohibits the unauthorized disclosure of information save for purposes of the Act or for prosecution of an offence under any written law or in accordance with an order of Court against a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material. A contravention of the section

is punishable on conviction to by fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both. It is important to note that in majority cases, data collected is of a personal nature. Personal data is very vulnerable to abuse and misuse. This vulnerability requires a proper legal framework to protect personal as well as provide a mechanism for clear governance and data processing for personal data.

With the rapid and dynamic development of technological advances in the area of information and communication technology, vast amounts of personal information are being transmitted, collected, stored and used on daily basis. This has opened up an opportunity for processing and misuse of personal data both by Government and private individuals and artificial persons including incorporated companies and organizations. Constant abuse of personal data is not any less than a violation of data and privacy rights.

2

BACKGROUND TO THE DATA PROTECTION AND PRIVACY BILL, 2015

Data protection and privacy laws have been enacted in over 100 countries. In January 2015, the total number of countries with data privacy laws was 109.¹ In Africa some of these include Angola, Benin, Burkina Faso, Ghana, Mauritius, Morocco, Senegal, Tunisia, and South Africa among others.

Thereafter, various regional and sub-regional mechanisms for data protection have been put into place.

In 2014, the African Union at its 23rd session adopted the Convention on Cyber Security and Data Protection.² The Convention on Cyber Security and Data Protection was a concretization of the States' Parties efforts, in which a Draft Convention on Cyber Security was drafted in 2012 on the directive of the Assembly of Heads of State and Government of the African Union.

In 2010, the Council of Ministers of the East African Community (EAC) approved the EAC Legal Framework on Cyber Laws and directed the Partner States to implement it by enacting national legislation to provide for the protection of personal data amongst other considerations.³

With regard to countries in the East African Community, only Kenya has developed a draft Data Protection Bill that has been approved by its cabinet and is before parliament for enactment. In regard to the republic of Tanzania the Constitution highlights privacy in Article 16 only in its generic form. The Tanzanian Parliament is yet to develop a specific law on data protection and privacy. Rwanda is at the same stage as Tanzania.

1 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529 and http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.

2 African Union Convention on Cyber Security and Personal Data Protection, available at http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf (accessed November 19, 2016).

3 See for instance, United Nations Conference on Trade and Development, "Harmonizing Cyberlaws and Regulations: The Experience of the East African Community", UNCTAD/DTL/STICT/2012/4/Corr.1, available at http://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf (accessed November 19, 2016).

3

EXISTING LEGAL FRAMEWORK

A review of the current legal framework indicates that data protection and privacy are not adequately addressed. Whereas aspects of data protection have been provided for in some sectorial laws, the overall legal regime is piecemeal and protections only currently apply to specific sectors. The said laws include the following:-

- (a) Constitution of the Republic of Uganda, 1995
Article 27 provides for the right to privacy of person, home and other property and that no person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.⁴
- (b) The Access to Information Act 2005 (Act No 6 of 2005)⁵
Section 26 protects information relating to individuals in the possession of the State or agency of the State from disclosure for private reasons.
- (c) The Uganda Communications Act, 2013 (Act No. 1 of 2013)⁶
The Act under section 79 requires operators to ensure that there is no unlawful divulgence, interception or disclosure of private data.
- (d) The Electronic Signatures Act, 2011 (Act No. 7 of 2011)⁷
Section 81 of this Act prohibits a person under any powers conferred under the Act from disclosing confidential information obtained through access to any electronic record, book, register, correspondence, information document, other material or grant access to any other person.

4 Available at <http://www.wipo.int/edocs/lexdocs/laws/en/ug/ug002en.pdf>

5 Available at http://www.freedominfo.org/documents/uganda_ati_act_2005.pdf

6 Available at <http://www.ict.go.ug/sites/default/files/Resource/UCC%20Act%202013.pdf>

7 Available at <http://www.ulii.org/ug/legislation/act/2011/7/Electronic%20Signatures%20Act%2C%202011.docx> ; <http://www.gateway.co.ug/the-uganda-electronic-transactions-act-no-8-2011/>

- (e) The Computer Misuse Act, 2011 (Act No. 2 of 2011)⁸
Section 18 prohibits a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, from disclosing to any other person or from using the information for any other purpose other than that for which he or she obtained access.
- (f) The Regulation of Interception of Communications Act, 2010⁹
The Act under section 2 regulates lawful interception of certain communications in the course of their transmission.

Notwithstanding the above,, there is no comprehensive law to safeguard the data collected or ensure that it is only collected fairly and lawfully, for lawful purposes, to the relevant or adequate extent, in accuracy, with adherence to scope of storage, taking to consideration all the rights of data subjects while ensuring that data collectors take all necessary measures for protection against unauthorized access, damage or loss as well as guaranteeing international protection of personal data, so that there is no unauthorized transfer. In the absence of a legal framework to govern the integrity and circumstances relating to the use, storage and processing of data, the risks of abuse and misuse of collected data is inevitable.

8 Available at <http://www.ulii.org/ug/legislation/act/2010/2/Computer%20Misuse%20Act%202011.docx>; http://chapterfouruganda.com/sites/default/files/downloads/Computer-Misuse-Act-2011_0.pdf ; and <http://www.ulrc.go.ug/content/computer-misuse-act-2011>

9 Available at <http://www.ulii.org/ug/legislation/act/2010/18/Regulation%20of%20Interception%20of%20Communication%20Act,%202010.docx> ; and <http://www.ulrc.go.ug/ulrcsite/sites/default/files/Regulation%20of%20Interception%20of%20Communications%20Act%202010.pdf>

4

SALIENT CLAUSES IN THE BILL

The main objective of the Bill, as indicated in the preamble, is to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information. It is also intended to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers; and to regulate the use or disclosure of personal information; and for related matters.¹⁰

PART I - PRELIMINARY

The proposed Bill is important in as far as it gives effect to article 27 of the Constitution of the Republic of Uganda, 1995, attempts to offer safeguards for personal data protection, spells out rights as well redress mechanisms for individuals in case of infringement of rights related to personal data.

Further, the Bill applies to written and electronic records in possession of any person, institution or Public body collecting, processing, holding or using personal data. This is because personal data in whatever form should be protected from abuse. (Clause 1). It is also important to note here that the Bill covers personal data of a natural person (individuals) only.¹¹

By providing a detailed list of specific objectives of the Bill, Part I is very clear in its objectives and is exhaustive in scope of coverage on the right to privacy. It does not therefore present any challenges in as far as the objectives and purpose are concerned. This is also reflected in the long title which communicates that the Bill in the given technological developments, which have led to an increase in data collection, processing and usage, is necessary for ensuring appropriate safeguard.

10 Long Title to the Data Protection and Privacy Bill, 2015.

11 See for instance the meaning of “personal data” under Clause 2 of the Data Protection and Privacy Bill, 2015. It refers to data which is only practical of individual persons.

Interpretation

Clause 2 Interpretation

Clause 2 in as far as it labours to explain the meaning of the different terms used in the Bill. This is welcome in as far as it provides certainty on how the law is to be applied. However, there are certain terms used in the Bill that require definition. Defining the terms would further simplify the application of the law. The following terms if defined will lead to a better law:

“any person” (Means both natural persons and incorporated institutions under the laws of Uganda)

“institution” (includes both private and public body whether incorporated or not and includes all government ministries, departments, agencies and organs.)

“public record” (means any record kept by an authority in relation to physical planning and housing and a record of information in relation to that authority for purposes of effective social service delivery.

Immediately after the interpretation section, we propose the introduction of proviso for independent commission, centered on personal data and privacy protection ideal. This will serve to ensure that personal data is managed centrally by an independent commission. Thus, we propose the deletion of NITA-U from the Bill and replacement of NITA-U with a Data Protection Commission.

The independent commission could provide for among others the; objects and functions of the commission, the governing body of the commission, for instance, a board, a determination of the tenure of office for members of the board as well as the managerial issues of the board. ,

For instance, the term “Authority” is defined under the interpretation section as the National Information Technology Authority (NITA). However 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. It is of utmost importance that collection and storage of data is managed by an independent commission instead of the National Information Technology Authority (NITA-U).

Further, though the National Information Technology Authority, Uganda act, 2009, provides that the authority shall be the centralized data centre (section 5 (1)), national data bank (section 5 (5)), carry out data protection (section 5 (6)), there is no clear justification as to why personal data

collections should be placed under NITA-U under the Data Protection Bill. Moreover, the National Information Technology Authority, Uganda Act, 2009 is more centered on communication and information technology than personal data protection and privacy rights. Further still, data protection and privacy rights are not evident in the NITA-U as spelt out in section 4 of the Act.

In the alternative, NITA-U may be retained as the centralized data centre but IT should not play the oversight roles. Another independent body should be charged with oversight over personal data:

PART II – PRINCIPLES OF DATA PROTECTION

This part of the Bill seeks to implement the internationally accepted principles of data protection.¹² These principles under the Bill are traceable in Clause 3.

Clause 3, details the principles of accountability, collection limitation, purpose specification, quality of data processed, transparency and participation, retention period, and security safeguards with respect to any person who collects, processes, holds or uses personal data. Thus, Clause 3 of the Data Protection and Privacy Bill lays down the different principles to guide the data collector, data processor and controllers to protect data subjects. These include:-

- (i) A person who collects data shall be accountable to the data subject for data collected, processed held or used;
- (ii) Personal data should be collected and processed fairly and lawfully.
- (iii) The data collector, data processor and data controller is accountable to the data subject for data collected, processed held or used;
- (iv) The data collector, data processor and data controller is required to collect, process, use or hold adequate, relevant and not excessive or unnecessary personal data;
- (v) Personal data should be retained for the period authorized by law or for which the data is required;
- (vi) The data collector, data processor and data controller shall ensure quality of information collected, processed, used or held;
- (vii) The data collector, data processor and data controllers shall ensure transparency and participation of the data subject in the collection, processing, use and holding of the personal data; and
- (viii) The data collector, data processor and data controller shall observe security safeguards in respect of the data.

¹² The internationally acceptable principles on privacy can be found at: OECD, "OECD Privacy Principles", available at <http://oecdprivacy.org/> (accessed November 19, 2016).

The human rights implication of Clause 3 is that it seeks to secure the rights of the data subject to ensure that the data collector, data processor and controllers do not abuse the integrity, and participation rights of the data subject. Thus, Clause 3 to a larger extent adheres to data protection principles, in light of which it is progressive and core to safeguarding the rights of the data subject. Clause 3 therefore adequately addresses the recognized principles of data protection as set out in the OECD Guidelines as a standard benchmark.¹³

PART III – DATA COLLECTION AND PROCESSING

Part III of the Bill deals with data collection and processing. This part of the Bill seeks to detail the factors to consider including; obtaining consent of the data subject, prohibition on collection and processing of special personal data

Clause 4: Consent to Collect or Process Personal Data

Clause 4, requires consent to be given by the data subject before collection or processing of personal data. Hence, a person shall not collect or process personal data without the prior consent of the data subject.

The Clause 4(2) of the Bill provides for the purposes for which data may be collected as including the following:

- (a) defense or public security;
- (b) prevention, investigation, indictment or prosecution of criminal offenses or execution of penal convictions or security measures;
- (c) population census;
- (d) for medical purposes;
- (e) compilation of personal data directly or indirectly; and
- (f) processing salaries, pensions, taxes, levies and other payments..

The requirement for the data subject to give consent is in line with the principle of participation (of the data subject) during the data collection, processing and control as given in Clause 3. The strength of this provision could be improved by qualifying consent. 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.

13 OECD, note 12.

Clause 5: Prohibition on Collection and Processing of Special Personal Data

Clause 5 prohibits collection of special personal data, which is referred to as 'sensitive' data in other jurisdictions and means that a person shall not collect or process personal data which relates to the religious or philosophical beliefs, political opinion, health or sexual life of an individual. Nevertheless, special personal data may be collected by the Uganda Bureau of Statistics, for purposes of development and maintenance of a national statistical system to ensure collection, analysis and publication of integrated, relevant, reliable and timely statistical information.¹⁴ Further, a data collector or data processor may collect or process collect and process special personal data in exercise of a right conferred by the law, where the data subject freely consents, for exercise of legitimate purposes of a body or association of a nonprofit, political, philosophical, religious or trade union purposes and for membership purposes to a body or association for that sole purpose without disclosure to a third party unless consent of the data subject is sought.¹⁵

Though Clause 5 makes commendable strides in protecting processing of special personal data, it does not expand to all of the necessary categories. If it is to be regarded as comprehensive in offering protection, the following must be added:

- 1) racial and ethnic origin,
- 2) whether the data subject is a member of a trade union or other membership organisation,
- 3) his or her physical or mental health or condition,
- 4) the commission or alleged commission by him or her of any offence, and
- 5) any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.

The inclusion of 'tribe' or 'ethnic' origin, into special personal data would go milestones in buttressing article 21 of the Constitution, which prohibits discrimination on such grounds.

A key weakness is that Clause 5 does not apply to information collected under the Uganda Bureau of Statistics Act yet the Uganda Bureau of Statistics practically collects all information pertaining to a particular individual. It is unclear if the data collected under the Uganda Bureau of Statistics Act is also protected by data protection standards. Indeed there is no provision for protection of personal data under the Uganda Bureau of Statistics Act. This poses a high risk of misuse of personal data.

14 See for instance the Long title of the Uganda Bureau of Statistics Act Chapter 310; see also Clause 5 (2) of the Data Protection and Privacy Bill, 2015.

15 Clause 5 (3) a., b. and c (i), (ii) and (iii) of the Data Protection and Privacy Bill, 2015.

Clause 5 is key and fundamental to personal data collection and processing. Personal data relating to religion or political party affiliation among others can be injurious to the data subject. Unwarranted disclosure of the same would amount to a clear violation of the right to privacy of the data subject.

In light of the exceptions set out in Clause 5 (2) (3), the Bill does not exempt personal data processing for special purposes like publication by any person of any journalistic, literary or artistic material and freedom of expression. The failed exemptions of above scope of works is likely to; limit freedom of expressions, attract heavy fines to journalists and researchers. The aforementioned for instance runs contrary to international standards. We therefore propose that the following be added to the exemptions laid down in Clause 5:

Clause 5 (3) (d) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material;¹⁶

Clause 5 (3) (e) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest;¹⁷ and

Clause 5 (3) (f) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.¹⁸ A special purpose may include the need for the information for journalism, art or literature.¹⁹

Clause 5 (3) (g) data processed by a natural person for generally personal or household purposes through social media, internet or any other medium of fora.²⁰

Clause 5 (3) (h) personal data processed for the purposes of making judicial, Ministerial, government departments and agencies appointments or for conferring honours.²¹

Clause 5 (3) (i) data processed for Legal advice and proceedings where such data is in connection with legal proceedings or prospective legal proceedings, is necessary for obtaining legal advice or for establishing, exercising or defending legal rights.²²

16 Information Commissioner's Office, "In brief – are there any exemptions from the Data Protection Act?" available at <https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/> (accessed November 19, 2016).

17 Information Commissioner's Office, note 16.

18 United Kingdom, "Data Protection Act, 1998", section 32 (1).

19 Information Commissioner's Office, note 16.

20 Information Commissioner's Office, note 16.

21 Information Commissioner's Office, note 16.

22 Information Commissioner's Office, note 16.

Clause 6: Protection of Privacy

Clause 6 of the Bill upholds the right of privacy by requiring a data collector, data processor or data controller to collect or process the data in a manner which does not infringe the privacy of the person to whom the data relates.

The human rights implication of Clause 6 of the Bill is that it is intended to secure the right to privacy as provided for by article 27 of the Constitution. Whilst we welcome this provision, 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 a Data Subject

Clause 7 enjoins a person collecting personal data to collect it directly from the data subject and sets out conditions that must be proved if data is to be collected from a secondary source. As such, data may be collected from a secondary source if: the data is contained in a public record, data subject has deliberately made the data public, data subject has consented to the collection of the information from another source, collection of data does not prejudice the privacy of the data subject and collection of the data is necessary.

Clause 7 seeks to secure and guarantee the rights of the data subject since the data collector, processor or controller cannot 'by-pass' the data subject, as it is a legal requirement that before collecting personal data, a person collecting data shall collect the data directly from the data subject upon receiving consent as upheld in Clause 4.

The further implication of this provision is that it is illegal for a data collector to collect information about an individual from another source not being the individual subject save where collection of such data is within the exemptions laid down in Clause 7(2). Where the contrary happens, the data subject may have recourse in the courts of law. This is a progressive provision and should be maintained and passed.

Nevertheless, it is important to observe that the term public record is not defined in the Bill. The question therefore is what a public record is and what constitutes a public record? Though the Bill defines a public body in Clause 2 'Interpretation', it does not extend explanations to public records. This Clause if passed may be used to wrongly disclose information of the data subject from what are not public records. The term public record should therefore be defined in the Bill in order to provide certainty as to what it is and its scope of application.

Clause 8: Collection of Personal Data for Specific Purpose

Under Clause 8 of the Bill, personal data should be obtained only for a specified and lawful purpose or purposes, and shall not be further processed in any manner incompatible with that purpose or purposes. This Clause upholds the principle of purpose limitation which is crucial to prevent a secondary use of personal data, and minimize risks of mission creeps.

Clause 9: Information to Data Subject before Collection of Personal Data

Clause 9 of the Bill obliges the person collecting or processing personal data to inform the data subject about particulars of the data collector and any other necessary information. Thus Clause 9 seeks to ensure that the data subject is informed as to what data is collected, for what purpose and by whom, as well as their right to access the data.

Clause 9 further secures and entrenches democratic principles in the Bill. By requiring a person collecting personal data to inform the data subject about for example the nature of the data being collected, the data subject is in position to know and understand the reasons why the information is needed. The subject is accordingly in position to give out only the required and relevant information during the exercise. This serves to protect the data subject from disclosure of information without clear knowledge as to what it is to be used for.

Clause 10: Minimality

Clause 10 of the Bill is to ensure that the amount of personal data is not excessive in relation to the purpose or purposes for which they are processed by requiring the data collected to be relevant or necessary and thereby affording protection to the data subject.

Clause 11: Quality of Information

Clause 11 is to the effect that personal data should be accurate and, where necessary, kept up to date. The Bill requires a data controller to take reasonable steps to ensure the accuracy of personal data which it holds, and to take steps to correct inaccurate data when requested to do so by a data subject.

Hence, Clause 11 deals with the right of the data subject to have quality information kept or maintained in respect of their data by requiring the person collecting personal data to ensure that that data is complete, accurate, up-to-date and not misleading having regard to the purpose for its collection or processing.

Clause 12: Correction of Personal Data

Clause 12 requires the data controller to correct or delete any inaccurate information or data on request by the data subject, and the controller shall comply with the request. It seeks to ensure the privacy of the data subject by having only correct/accurate information kept or maintained about them by the data controller.

Nevertheless, while the title of Clause 12 reads: "Correction of personal data", it covers both correction and deletion. We therefore recommend that:

The title of Clause 12 should read as follows; "Correction and Deletion of Personal Data". A broader provision for deletion of information on the request of the data subject may lead to violation of the right to information contrary to the access to information Act, 2005 and may as well affect freedom of expression.²³ To strike a balance, where deletion or correction is preferred, the following should be taken to consideration and should be included for checks and balances under Clause 12 (1) (a) and (b)

- (i) Whether the information in question is of a private nature;
- (ii) Whether the applicant had a reasonable expectation of privacy, including the consideration of issues such as prior conduct, consent to publication or prior existence of the information in the public domain;
- (iii) Whether the information at issue is of public interest;
- (iv) Whether the information at issue pertains to a public figure;
- (v) Whether the information is part of the public record;
- (vi) Whether the applicant has demonstrated substantial harm;
- (vii) How recent the information is and whether it retains public interest value;

Clause 12 (c) should therefore be introduced. It should preferably read as follows:

In reaching a decision as to where data should be corrected or deleted, the factors should be considered:

- (i) Whether the information in question is of a private nature;
- (ii) Whether the applicant had a reasonable expectation of privacy, including the consideration of issues such as prior conduct, consent to publication or prior existence of the information in the public domain;
- (iii) Whether the information at issue is of public interest;
- (iv) Whether the information at issue pertains to a public figure;

23 Article 19, "Uganda: Data Protection and Privacy Bill", July 2016. Available at <https://www.article19.org/data/files/medialibrary/38451/Uganda-Data-Protection-and-Privacy-Bill-FINAL.pdf> (accessed September 23 , 2016)

- (v) Whether the information is part of the public record;
- (vi) Whether the applicant has demonstrated substantial harm;
- (vii) How recent the information is and whether it retains public interest value.²⁴

We also suggest inclusion of Clause 12 (6) between Clause 12 (5) and Clause 12 (6). The Clause should read as follows:

A request for data correction or deletion shall not be done where public interest overrides the interest of the data subject.²⁵

Clause 13: Processing of Data to be Compatible with Purpose of Collection

Clause 13 states that (any) further processing (of personal data) shall be compatible with the purpose of collection.

The purpose of Clause 13 is to avoid or minimize the abuse of personal data by the data controller by limiting the use of data for other purposes that originally intended.

Clause 14: Retention of Records of Personal Data

Under Clause 14 of the Bill personal data processed should not be kept for longer than is necessary for that purpose.

Clause 14 prohibits any person who collects personal data from retaining the personal data for a period longer than is necessary to achieve the purpose for which the data is collected and processed, unless certain factors such as authorization by law, retention for a lawful purpose, information is required by a contract between parties and the data subject has consented. Clause aims at minimizing abuse of personal data as would be the case if personal data were to be held for prolonged days or years beyond or longer than is necessary. However, the list of exemptions is very broad. the exemptions to the limitation of data retention listed in 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 limitation to data retention for the purpose of law enforcement, and national security. This Article must make reference the legal frameworks that allow data retention for law enforcement and national security purposes.

²⁴ Article 19, AUganda: Data Protection and Privacy Bill, note 23.

²⁵ Article 19, Uganda: Data Protection and Privacy Bill, note 23.

Clause 15: Processing Personal Data outside Uganda

Clause 15 deals with processing of personal data outside Uganda. The Clause enjoins the data controller or data processor to secure the integrity of personal data processed outside. To that effect, Clause 15 is intended to ensure that personal data that goes beyond the boundaries of Uganda has at minimum the same legal protection as is in Uganda.

The Bill further provides for the criteria of processing data to a country outside Uganda and such; the country should have adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The Clause also seeks to secure the integrity of the data subject.

PART IV – SECURITY OF DATA

Part IV of the Bill is concerned with security of the data given by the data subject. The purpose of this part of the Bill is to secure personal data and the infrastructure, i.e. the databases.

Clause 16 deals with security measures relating to data processed by a data processor. A data controller shall not permit a data processor to process personal data unless the data processor establishes and complies with the security measures specified in the Bill.

Similarly, Clause 17 requires that a data controller does not permit a data processor for a data controller unless the operator established and complies with the security measures specified under the Bill. Where there is contract between a data controller and a data processor relating to processing of personal data, the data processor shall establish and maintain the confidentiality and security measures necessary to ensure the integrity of the personal data.

Further, Clause 18, requires an operator or a person who processes personal data on behalf of a data controller to do so only with the prior knowledge or authorization of the data controller and shall treat the personal data which comes to the knowledge of the operator or other person as confidential. The data processor is also barred from disclosing the data unless required by law or in the course of discharge of duty.

Clause 19 requires a data controller, data processor or data controller to notify the relevant authority in the event of data security breaches. The authority shall determine and notify the data controller whether the data controller should notify the data subject of the

breach. Where notification of data subject is preferred, it shall be by registered or electronic mail or website or publication in the mass media. Notification gives the data subject opportunity to take protective measures against the consequences of unauthorized access or acquisition of data. The information may include, if known to the responsible party, information relating to the breach.

Clauses 16–19 are intended to make secure the information given by the data subject, collected by the data processor and stored by the controller. Hence, as Stated in the Memorandum of the Bill, Part IV of the Bill, deals with security of data and requires a data controller to secure the integrity of personal data in the possession or control of that person by adopting appropriate, reasonable, technical and organizational measures to prevent loss, damage, or unauthorized destruction and unlawful access to or unauthorized processing of personal data.

Further, Part IV further requires a data controller, data processor or data controller to notify the Authority (NITA-U) where the personal information relating to an individual has been accessed or acquired by an unauthorized person and any remedial action taken.

Part IV, is accordingly adequate and comprehensive in addressing the issues pertinent to security of personal data.

PART V – RIGHTS OF DATA SUBJECT

This Part of the Bill deals with the rights of data subjects. This is a very important Part of the Bill as rights of data subjects are key in any legislation dealing with data protection and privacy.

Clause 20 stipulates that a data subject has a right of access to personal information relating to the data subject, this is in line with the right to information. This right to access enables the data subject seek for correction or deletion of any inappropriate data. Further, Clause 21 is to the effect that the data subject has a right to prevent processing of their personal data. The role of NITA-U (the Authority) to accept the request of the data subject is very prominent here, and needs to be examined, in light of questions about the independence of the NITA-U.

Clause 22 prohibits the processing of personal data for direct marketing purposes. Clause 23 gives the rights of a data subject in respect of automated decision taking which is currently on the rise. Clause 24 has a host of remedies to a data subject such as rectification, blocking, erasure and destruction of personal data, the import of Clause 24 is to set the record clean, and to avoid having an inaccurate record of the information.

Clause 29 on compensation remedies seeks to ensure that a data subject who suffers damage or distress through the contravention by a data controller of the requirements of this law, is entitled to damages/compensation, by the data controller. This is also aimed ensuring that only accurate data is on record and that such data is used for the specified purpose.

The Bill provides for the institutional framework and procedures to administer, receive complaints and settle disputes relating to personal data protection under clauses 27, 28, 29, 30, 31, 32 and 33. It is proposed that the National Information Technology Authority-Uganda (NITA-U) established under the National Information Technology Authority- Uganda Act, 2009 (Act No. 4 of 2009) should be mandated to administer and implement this law since data protection is one of the functions of the Authority. However, we argue that NITA-U does not constitute an independent authority as necessary, and call for the adoption of one under this Bill as outlined above.

PART VI – DATA PROTECTION REGISTER

This Part provides for the data protection register. This register is useful for integrity and security, plus central access center purposes.

Clause 25 requires that there shall be a data protection register to be kept and maintained by the data protection register. Clause 26 allows access to the register by the public. This Clause seeks to empower the members of the public to complain in case of any inaccuracies on the register.

PART VII – COMPLAINTS

This Part of the Bill deals with complaints.

Clause 27 deals with complaints against breach and non-compliance with the Act, which must be lodged with the Authority (NITA-U).

Clause 28 obliges the Authority to investigate all complaints received.

Clause 29 provides for compensation in the event of failure to comply with this Act, which compensation should be paid within a reasonable time.

Under Clause 30, a person aggrieved with a decision of the Authority under the Act may appeal to the Minister.

The complaints mechanism dealt with in Part VI is useful in securing the rights of the data subject which may be violated. It also offers a degree of certainty as to the avenues for filing complaints whenever an individual is dissatisfied.

PART VII – OFFENCES

This Part of the Bill outlines offences, which are punishable under the Bill. The Bill provides for an enforcement mechanism that will allow individuals to enforce their rights.

Clause 31: Unlawful Obtaining and Disclosure of Personal Data

Clause 31 outlines the offence of unlawfully obtaining and disclosure of personal data held or processed by a data controller. Clause 31 (2) prescribes a sentence upon conviction of a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both. The prison sentence and penalty prescribed is too harsh. Given the exclusion of prescribing exemption to data that may be processed of, artistic works, research, journalistic, academics and literary works. The space of freedom of expression will be narrowed and those who collect or process data for journalistic, literary or artistic material will face heavy fines that are prohibitive of their work and professions.

We therefore propose a reduction of the prison sentence prescribed by Clause 31 (2) from ten years to three years or five years at maximum. Equally, the fine the penalty attracts should be reduced from the maximum prescribed two hundred and forty currency points to a maximum one hundred currency points.

Additionally, in the spirit of the fair trial and the presumption of innocence, it would be in the interest of justice to provide for defences where there has been unlawful obtaining and disclosure of personal data. We therefore propose the introduction of Clause 31 (2) between Clause 31 (1) and Clause 31 (2). The Clause should read as follows:

Clause 31 (2) Subsection (1) does not apply to a person who shows—

- (a) that the obtaining, disclosing or procuring—
 - (i) was necessary for the purpose of preventing or detecting crime, or
 - (ii) was required or authorised by or under any enactment, by any rule of law or by the order of a court,
- (b) that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person;
- (c) that he acted in the reasonable belief that he would have had the consent of the data

- controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it; or
- (d) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.²⁶

Clause 32 creates an offence in respect of sale of personal data, which seeks to minimize abuse of personal data.

Clause 33 of the Bill creates Offences by Corporations.

Once the Data Protection and Privacy Bill is passed into law then there will be adequate measures for the protection and privacy of personal data. This will lead to increased confidence by the citizens when transacting in various forms especially where they may be required to disclose their personal data to corporate entities. Likewise corporations will be deterred from breach of the law for fear of huge compensatory orders to data subjects under Clause 29.

The Minister is given power to make Regulations under this Act/Bill in Clause 34 and also power to amend the Schedule with the approval of Cabinet, by statutory instrument, to amend Schedule 1 under Clause 35.

CONCLUSION

Currently, Uganda lacks a comprehensive law to protect personal data of persons in conformity with the provisions of Article 27 of the Constitution on the right to privacy of a person. It is therefore timely and necessary that Uganda enacts a law on data protection and privacy. The proposed Bill is intended to complement the existing laws on electronic transactions, communications and access to information by providing for protection privacy and personal data. However, this protection should balance the prerogatives of the State and other entities that collect and use information in delivery of services. In order to achieve the objectives outlined in Clause 1 of the Bill, and to ensure that that Uganda adopts a data protection framework that meets internationally respected data protection principles and standards, we call upon the Ugandan Cabinet and the Parliament to consider the concerns outlined in this document along with the relevant recommendations, and to immediately take the necessary measures to review the Bill accordingly.


²⁶ United Kingdom, "Data Protection Act 1998", section 55.


Plot 41 Gaddafi Road
P.O.Box 71314 Clock Tower K'la


Tel: +256 414 697 635

Email: info@unwantedwitness.or.ug

www.unwantedwitness.or.ug

 Unwantedwitness-Uganda

 @unwantedwitness

 unwantedwitness