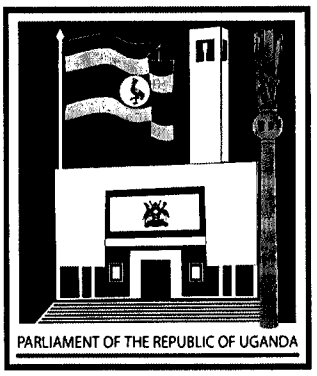


PARLIAMENT OF UGANDA

REPORT OF THE SECTORAL COMMITTEE ON INFORMATION, COMMUNICATION TECHNOLOGY AND NATIONAL GUIDANCE ON THE DATA PROTECTION AND PRIVACY BILL, 2015

OFFICE OF THE CLERK TO PARLIAMENT

November, 2018

1.0 INTRODUCTION

The Data Protection and Privacy Bill, 2015 was read for the first time on 20th April 2016 and referred to the Committee on Information, Communications, Technology and National Guidance in accordance with Rules 127 and 128 of the Rules of Procedure of Parliament. The Committee scrutinized the Bill and hereby presents its findings and recommendations.

2.0 BACKGROUND TO THE BILL

The Data Protection and Privacy Bill, 2015, is premised on Article 27 of the Constitution of Uganda that provides for the protection and promotion of the right to privacy of a person, home and other property. Whereas Article 27(2) of the Constitution provides that no person shall be subjected to the interference of the privacy of that person's home, correspondence, communication or other property, there is currently no comprehensive law to safeguard personal data by regulating how personal information is collected or to ensure that it is used only for the purposes for which it is collected.

Laws like the Regulation of Interception of Communications Act, 2010[1] and the Registration of Persons Act, 2015[2] among others have some provisions relating to regulation of collection and safeguarding of personal information. The frameworks provided under these laws are mere examples of the numerous scenarios of collecting personal information and how it may be safeguarded. In the absence of a comprehensive law regulating and safeguarding the collection and use of personal information, there is need to provide a comprehensive framework for data protection in Uganda.

3.0 OBJECT OF THE BILL

The Bill seeks to protect the privacy of the individual which also covers personal data by regulating the collection and processing of personal information; 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.

4.0 METHODOLOGY

During consideration of the Bill, the Committee, held consultative meetings and received memoranda from the following stakeholders;

[1] Act 18 of 2010
[2] Act 4 of 2015

1. The Ministry of Information, Communications Technology and National Guidance (MoICT)
2. National Information Technology Authority (NITA)
3. Ministry of Justice and Constitutional Affairs (MoJCA)
4. Uganda Law Society (ULS)
5. Human Rights Awareness and Promotion Forum
6. United Nations Pulse Lab
7. Uganda Human Rights Commission (UHRC)
8. Human Rights Center Uganda
9. The Unwanted Witness
10. Uganda Communications Commission (UCC
11. Telecommunication Companies (MTN, UTL, Africell)
12. The National Association of Broadcasters
13. Multichoice Uganda
14. Star Times Uganda
15. Vision Group of Companies
16. Uganda Manufacturers Association (UMA)
17. Uganda Chamber of Commerce
18. Uganda Hotel Owners Association
19. Uganda National Examinations Board (UNEB)
20. Uganda National Council for Science and Technology
21. The Uganda Business and Technical Examinations Board
22. Uganda Medical Doctors Association.
23. Allied Health Professionals Council
24. Uganda Bureau of Statistics (UBOS)
25. National Identification and Registration Authority (NIRA)
26. Uganda Registration Services Bureau (URSB)
27. Ministry of Public Service
28. Uganda Library and Information Association
29. Ministry of Lands Housing and Urban Development
30. Bank of Uganda (BOU)
31. Uganda Bankers Association (UBA)
32. Uganda Insurers Association
33. Uganda Prisons Service; and
34. Bytelex Advocates

b) The Committee benchmarked the Bill against the Data Protection Act, 2017 of the Republic of Mauritius and the Protection of Personal Information Act, 2013[3] of the Republic of South Africa where laws on data protection and privacy have been enacted and are being implemented.

c) In scrutinizing the Bill, the Committee put into consideration the Second National Development Plan 2015/16 –2019/20 whose objective is to improve the information systems to be secure, reliable and capable of responding to security threats, by developing and implementing strategies to protect consumers of ICT services. The Committee made reference to the Sustainable Development Goals and considered other cross cutting issues such as gender and equity.

d) The Committee also reviewed the Bill in the context of international practices embodied in several regional data protection instruments such as the General Data Protection Regulations (2018) of the European Union, the African Union Convention on Cyber Security and Personal Data Protection, (2014) as well as the guiding principles under the East African Community Legal Framework on Cyber laws.

5.0 OBSERVATIONS

The Committee studied the Bill and considered the concerns raised by the various stake holders and came to the following observations:

5.1 GENERAL OBSERVATIONS

5.1.1 The Right to Privacy

Privacy is envisioned as a multidimensional concept which has been recognized both in law and common expression. The Constitution of the Republic of Uganda[4] guarantees the right to privacy which forms an integral part of fundamental human rights. Uganda is also party to a number of International Instruments that recognize the right. These include; the Universal Declaration of Human Rights[5] and the International Convention on Civil, and Political Rights.[6] It should however, be noted that this right is not absolute and thus should be regulated to ensure that its protection does not prejudice other Constitutional rights.

5.1.2 The Concept of Data Privacy and Protection

The Concept of Data Privacy requires that personal data should not be availed to other persons without consent. It encompasses an individual's right to control the collection, use, storage, processing and disclosure of his or her personal information. This information, which is usually of a personal nature may easily be abused or misused in

[4] Article 27 of the 1995 Constitution of the Republic of Uganda
[5] Article 12
[6] Article 17. General Comment No. 16 to the ICCPR, which refers to the obligations of States to enact measures deriving from data protection law (such as providing individuals with the right to request rectification or deletion of their personal data, see para. 10).

the absence of a comprehensive legal framework. The Bill therefore aims to safeguard persons against misuse of personal data by proposing administrative, technical and physical deterrents.

5.1.3 Convergence of Technologies

The rapid and ever dynamic technological advances have made personal data easily accessible which has increased concerns over privacy rights and hence the need for a law ensuring data protection. Over the years the amount of data collected by government and private institutions as well as individuals has become enormous. There is, however, no central register for the various data collectors, processors and controllers to facilitate appropriate regulation of the data collected. The Bill therefore provides solutions to these lacunas.

5.1.4 Challenges necessitating the law on data protection

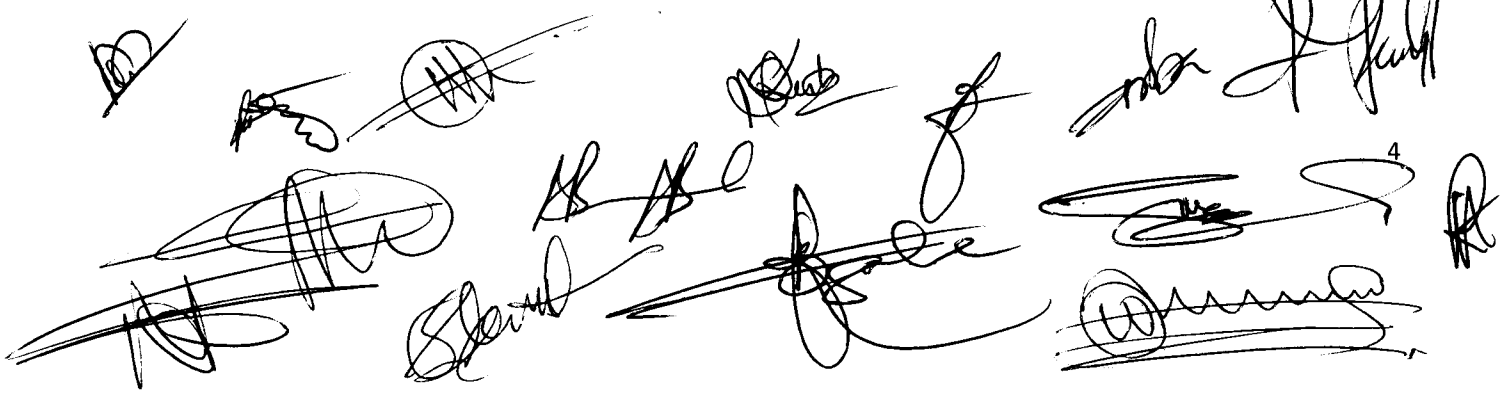
Uganda currently faces a number of challenges which necessitate a law on data protection and privacy. Some of these include; the fragmented regulatory framework on data protection and privacy, abuse and disclosure of personal data, use of personal data for direct marketing and high data illiteracy levels among others.

The Committee was informed that various institutions collect information which requires disclosure of personal data such as biometric details, place of birth, place of origin, names of parents, spouses or dependents, health status of individuals to mention but a few. This information often ends up with business for example telecommunication companies, food stores, advertising agencies among others which send unsolicited messages or publish this data in print media hence infringing on the privacy of the data subjects. The Data Protection and Privacy Bill once passed into law will mitigate such challenges.

5.1.4 Study visits to the Republic of Mauritius and The Republic of South Africa

During consideration of the Bill, two delegations from the Committee undertook study visits to the Republic of Mauritius and South Africa to benchmark on Data Protection and Privacy.

The delegations interacted with several stakeholders. These included Officials from the respective Data Protection Regulators, Telecommunication Operators, Communication Regulators and Data Protection Advocates. The information acquired guided the Committee during the consideration of the Bill.



5.1.5.1 Lessons learnt from the study visits

a) The delegations from both Mauritius and South Africa found that the Laws regulating data protection are based on the need to protect the right to Privacy of a person, both natural and artificial. This is indeed the same policy behind the proposed law in Uganda since it intends to enhance Article 27 of the Constitution[7].

b) The delegation to Mauritius was informed that alongside the policy to protect the right to privacy, the other motivating factor was the need to enhance the country niche into a Business Process Outsourcing Hub for its business partners in Europe and Asia. Consequently, the Mauritius Data Protection Act 2017 was to a large extent influenced by the General Data Protection Regulations of the European Union.

c) In South Africa, the motivation for the law was due to discussions that followed the enactment of their Access to Information Act. In this regard South Africa decided to establish the Information Regulator to oversee the operation of both the Access to Information Act and the Protection of Personal Information Act 2017.

d) Transition to compliance with the new laws on data protection and privacy has been relatively smooth, However, from the regulatory and compliance point of view, the two countries are still faced with the following challenges;
   - Absence of Regulations to clarify on interpretation of the Mauritius Data Protection Act, 2017 which has affected it's operationalization;
   - Inadequate funding and understaffing of their respective Data Protection Offices.

e) One of the key international standards for data protection laws is the requirement to have data protection officers in both private and public institutions that collect, control and process personal data.

5.1.5 The Sustainable Development Goals and Data Protection (SDGs)

Goal 17: *Strengthen the means of implementation and revitalize the global partnerships for sustainable development.*

Indicator 17.18 requires that by 2020, developed countries should enhance capacity building to developing countries to increase significantly the availability of high- quality, timely and reliable data disaggregated by income, gender, age, race, ethnicity, migratory status, disability, geographic location and other characteristics relevant in national contexts.

[7] Providing for the Right to privacy

In order to achieve this goal, tracking progress on the SDGs requires the collection, processing, analysis and dissemination of an unprecedented amounts of data and statistics at a sub-national, national, regional and global level[8]. However the absence of a common set of principles on data protection, privacy and ethics in several countries around the world makes it harder to use big data for development and humanitarian goals. These gaps also complicate efforts to develop standardized, scalable approaches to risk management and data access[9]. Subsequently, a coordinated approach is required by developing countries, Uganda inclusive, to ensure the enactment of regulatory frameworks for safe and responsible use of big data.

5.2 SPECIFIC OBSERVATIONS

5.2.1 REGULATION OF DATA PROTECTION AND PRIVACY

The Bill, under its memorandum proposes the National Information Technology Authority (NITA- U) to monitor persons and bodies collecting data and ensure that personal information is collected, processed, stored and used in accordance with Article 27(2) of the Constitution. This position is restated under Clause 2 that defines the Authority under the Bill to be the National Information Technology Authority.

The Committee received concerns about the mandate of NITA- U in respect of Data Protection and Privacy. Furthermore, concerns were raised on the capacity and independence of NITA- U to ably oversee the implementation of the law and ensure safety of personal data.

Consequently, proposals were made from entities such as the Human Rights Awareness and Promotion Forum, Uganda Law Society and Bank of Uganda to the effect that a new body should be established under the law to handle matters of data protection.

The Committee however observed that there is need for the government to reduce on the fragmentation of entities providing similar public services. The Committee further observed that the creation of a new entity would bear a financial implication on the sector which was not envisioned upon the award of a Certificate of Financial Implication.

The Committee reviewed the National Information Technology Authority Act[10] and found that Section 5 establishes NITA- U as an autonomous body corporate with perpetual succession which guarantees its independence and autonomy. Further, under Section 5 of the Act, NITA- U's core functions are to set, monitor and regulate standards of Information Technology, and ensure data protection among others. Its role as an information security advisor is complementary to the implementation of the data protection legislation.

[8] The Sustainable Development Goals Report, 2018 United Nations, New York.
[9] Finding the balance: Right to privacy and the drive to innovate in the UN, Robert Kirkpatrick, Mila Romanoff, Gina Lucarelli, Jens Wandel May 3, 2017
[10] Act No. 4 of 2009

The Committee is therefore in agreement with the provision under the memorandum of the Bill that NITA - U be the Authority to oversee the Act. However, the Committee notes that it is necessary to strengthen the regulatory role of NITA - U under the Bill by creation of an Independent Data Protection Office that reports to the Board.

Recommendation

The Committee recommends that;

a) ***NITA - U creates an Independent Data Protection Office which should report directly to the Board.***

b) ***The functions of the Data Protection Office be clearly specified under the Bill to give clarity to the responsibilities of the office in regard to data protection and privacy.***

c) ***All institutions that collect, control and process personal data designate a data protection officer who shall be responsible for ensuring compliance with this Act.***

5.2.2 APPLICATION OF THE BILL

Clause 1 proposes that the Bill should apply to any person, institution or public body collecting, processing, holding or using personal data.

The Committee observed that the Bill limits its application to the territorial boundaries of Uganda and does not provide for extra-territorial application. The Committee further observed that there has been an evolution to an inter-connected global digital society, where the services of different operating systems are universal in nature and the concept of cross-border data transfers has become the norm. However, there is no universal law that safeguards data protection apart from few international and regional legal instruments for example; the European Union General Data Protection Regulation (GDPR), 2018.

At the regional level, the African Union Convention on Cyber Security and Personal Data Protection and the East African Community Legal Framework on Cyber laws only provides guidelines and direct partner states to enact legislation providing for protection of personal data. Consequently, countries like Kenya, Tanzania and Uganda have draft laws on data protection and privacy, hence data protection and privacy is regulated by general privacy policies, end-user licenses and agreements for applications and operating systems.

The Committee also found that most of the servers on which personal data is collected and processed are not resident in Uganda but rather stored in the countries of residence of the data collectors or processors. This greatly increases the vulnerability of such data hence necessitating the expansion of the application of the Bill to ensure protection of the citizens' data.

Recommendation

The Committee therefore recommends that Clause 1 of the Bill be amended to widen the scope of application of the law to apply to all data collectors, processors and controllers handling data belonging to Ugandans outside the territorial boundaries of the country.

5.2.3 PROTECTION OF PERSONAL DATA RELATING TO CHILDREN.

Article 34 (1) of the Constitution of the Republic of Uganda[11] provides that laws shall be enacted in the best interest of children. Despite the fact that children have the same rights as adults over their personal data, they need particular protection when their data is being processed because they may be less aware of the risks involved.

The Committee noted that the Bill does not have clear provisions that guarantee the privacy of children as far as consent is concerned. The law should be strengthened to ensure that parental or guardian consent is sought when collecting or processing personal data of children.

Recommendation

The Committee recommends that a clause be inserted in the Bill to provide for protection of personal data relating to children to ensure that their right to privacy is equally upheld.

5.2.4 PRINCIPLES OF DATA COLLECTION AND PROCESSING

The internationally recognised principles of data protection are;

i) **Consent and legitimacy of personal data processing-** This principle is to the effect that processing of personal data is deemed to be legitimate where the data subject has given his/her consent. This requirement of consent may however be waived under exceptional lawful circumstances and for the protection of fundamental rights and freedoms of the data subject.

[11] 1995 (as amended)

ii) **Lawfulness and fairness of personal data processing-** This principle ensures that that the collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently.

iii) **Purpose, relevance and storage of processed personal data:-** this principle ensures that;

a) Data collection shall be undertaken for specific, explicit and legitimate purposes, and not further processed in a way that is incompatible with the purpose;

b) Data collection shall be adequate, relevant and not excessive in relation to the purpose for it is are collected and further processed;

c) Data shall be kept for no longer than is necessary for the purpose for which the data was collected or further processed;

d) Beyond the required period, data may be stored only for the specific needs of data processing undertaken for historical, statistical or research purposes under the law.

iv) **Accuracy of personal data-** This principle provides that Data collected should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it was further processed, is erased or rectified.

v) **Transparency of personal data processing-** This requires mandatory disclosure of information on personal data by the data controller.

vi) **Confidentiality and security of personal data processing-** This ensures that personal data is processed confidentially and protected. Where processing is undertaken on behalf of a controller, the latter shall choose a processor providing sufficient guarantees. It is incumbent on the controller and processor to ensure compliance with security measures.

Observations

a) The Committee observed that the principles enlisted under Part II of the Bill are in tandem with the international and regional principles and the guidelines provided under General Data Protection Regulations (2018) of the European Union, the African Union Convention on Cyber Security and Personal Data Protection (2014) as well as the East African Community Legal Framework on Cyber laws.

b) The Committee observed that the principle of consent is a core condition of data protection which allows the data subject to be in control of when their personal data is collected and processed. This in turn promotes the exercise of the fundamental rights of autonomy and self-determination. The Committee however noted that the Bill does not make mention of the type of consent required from the data subject.

c) The Bill under Clause (5) (1) provides for several categories of personal data, thereunder referred to as *"special personal data"* that should not be collected by any person other than the Uganda Bureau of Statistics. The Committee however observed that there are other categories of data such as health status of individuals as well as financial information of an individual that should be included under *"special personal data"* due to the nature of their sensitivity.

Recommendations

i) The Committee recommends that the term consent be defined under Clause 2 of the Bill.

ii) The Committee recommends that Clause 5(1) of the Bill providing for special personal data be amended to include health status and financial information of the data subject.

5.2.5 DATA PORTABILITY; THE RIGHT TO TRANSFER AND SHARE PERSONAL DATA

The concept of data portability connotes transmission of personal data from one data collector, controller and processor to another without hindrance from the controller to which the personal data has been provided. It allows data subjects to move, copy or transfer personal data easily from one controller to another in a safe and secure way without affecting its usability.

The Committee noted that the Bill allows individuals to access their personal data, however, this is limited to ensuring accuracy and correction. The Bill does not provide for free portability of personal data from one controller to another which in turn limits the data subject's control over their personal data. The Committee is of the considered view that the Bill be reconciled with policies already in place that provide for this concept for example the Regulation on Credit Reference Bureau Service.

Recommendation

The Committee therefore recommends that the concept of data portability be provided for within the Bill in order to ensure full maximization of data collected to reduce duplication of similar information collected by different data collectors and processors.

5.2.6 PENALTIES

The Committee observed that the Bill under Part VIII provides for penalties for the offences there under. The Committee however observed that the fines levied therein are not deterrent enough for corporations and thus there is need to provide for additional penalties.

Recommendation

The Committee therefore recommends that a fine of not more than 4% of the corporation's annual gross turnover be imposed in addition to any other penalties imposed under the Bill in case of breach.

5.2.7 OFFENCES

The Committee noted that the Bill emphasizes criminal liability of persons who breach the law by providing for the offences of; unlawful obtaining and disclosure of personal data, and sale of personal data. The Bill however does not provide for the offences of unlawfully destroying, deleting, misleading, concealing or altering personal data despite being prevalent breaches.

Recommendation

The Committee recommends that the Bill should extend criminal liability to persons who unlawfully destroy, delete, mislead, conceal or alter personal data by providing for an offence and prescribe penalties for the same.

5.2.8 TRANSITIONAL CLAUSE

The Committee noted that the Bill does not provide for a transitional clause despite introducing new obligations thereunder. Compliance with its provisions will require the different stakeholders to review their internal systems and processes. Furthermore, it is a generally acknowledged principle that when a new law is introduced, the affected organisations and individuals need a reasonable period of time to consider and adapt to the new legislation.

Recommendation

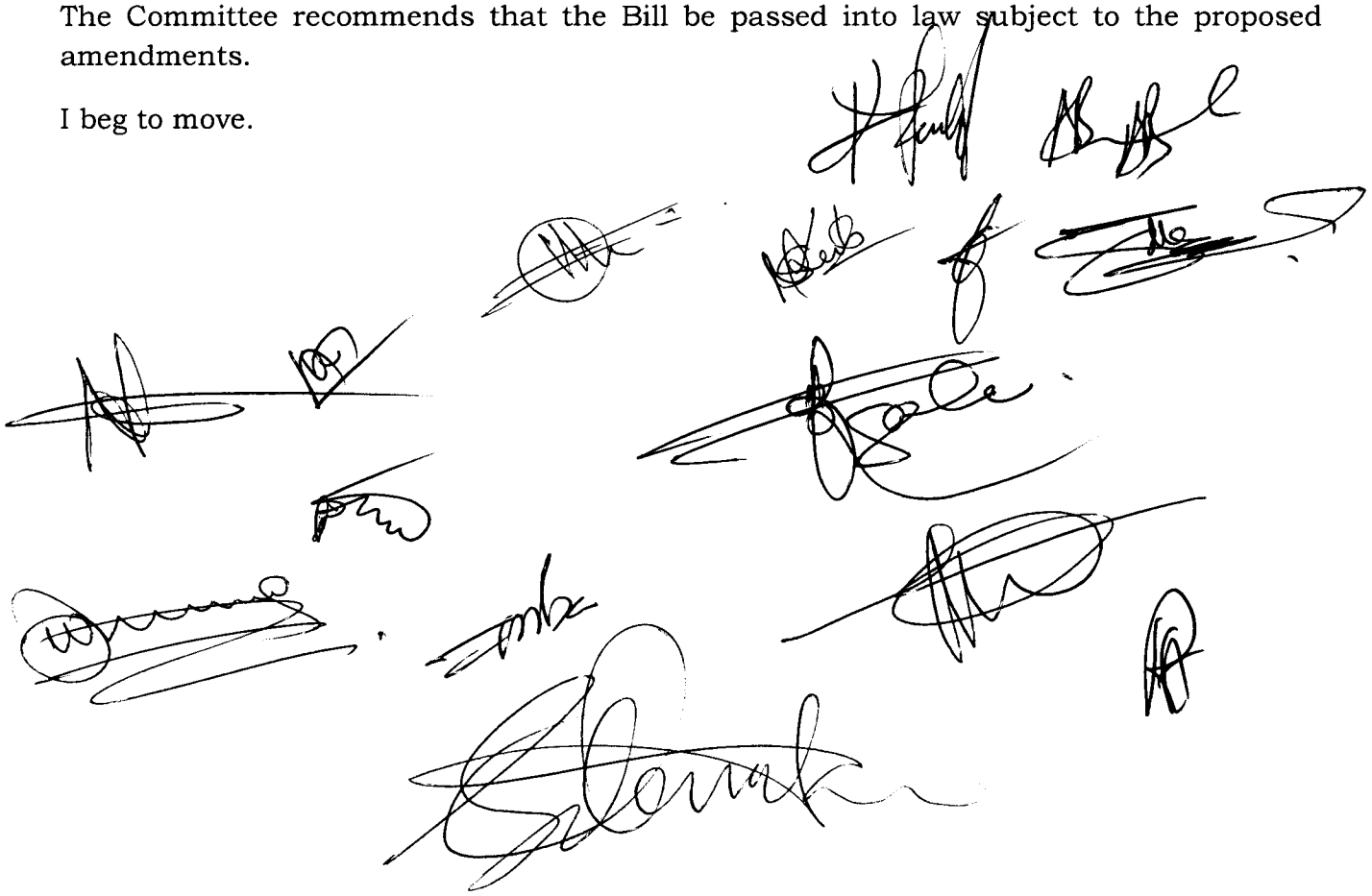
The Committee recommends that a transitional provision be included in the Bill to allow data collectors, controllers, and processors and the other stakeholders sufficient time to align their mandates and processes with the new law.

6.0 CONCLUSION

The Committee urges that massive sensitization be undertaken by the Ministry of ICT and National Guidance to raise awareness among the different government ministries, departments and agencies, private entities and the general public of the new law in order to ensure compliance.

The Committee recommends that the Bill be passed into law subject to the proposed amendments.

I beg to move.



SIGNATURE SHEET FOR MEMBERS OF THE COMMITTEE ON ICT AND NATIONAL GUIDANCE ON THE DATA PROTECTION AND PRIVACY BILL, 2015

NO.	NAME	CONSTITUENCY	SIGNATURE
1.	**Hon. Nyakecho Annet**	**Tororo North**	
2.	**Hon. Amoru Paul**	**Dokolo North County**	
3.	Hon. Kahima Moses Mugabe	Ruhaama County	
4.	Hon. Ruhunda Alex	Fort Portal Municipality	
5.	Hon. Acidri James	Maracha East County	
6.	Hon. Masika Apollo	Bubulo County East	
7.	Hon. Musana Eric	Buyaga East	
8.	Hon. Omony Oscar	**Youth Representative** Northern	
9.	Hon. Wakabi Pius	Bugahya County	
10.	Hon. Nakate Lillian Segujja	District Woman Representative	
11.	Hon. Nsamba Oshabe Patrick	Kassanda County North	
12.	Hon. Nakawunde Sarah	District Woman Representative	
13.	Hon. Tinkasiimire Barnabas	Buyaga County	
14.	Hon. Taban Amin	Kibanda North County	
15.	Hon. Seguya Lubyayi John Bosco	Mawokota County South	
16.	Hon. Abigaba Cuthbert Mirembe	Kibale	
17.	Hon. Oguzu Lee Denis	Maracha County	
18.	Hon. Tumuheirwe Fred Turyamuhweza	Rujumbura County	
	Hon. Akora Maxwell Ebong	Maruzi County	
	Hon. Waira Kyewalabye James Majegere · Sitingo	Bunya County East	

	Hon. Atiku Bernard	Ayivu County	
	Hon. Mukitale Biraahwa Stephen	Buliisa County	

PROPOSED AMENDMENTS TO THE DATA PROTECTION AND PRIVACY BILL, 2015

1. Amendment to Clause 1

Amend Clause 1 by substituting it with the following:-

"1. Application

This Act shall apply to a person, institution or public body collecting, processing, holding or using personal data within or outside the territorial jurisdiction of Uganda."

JUSTIFICATION

To provide for extra territorial application of the Act.

2. Amendment to Clause 2

Amend Clause 2 by;

(i) Inserting immediately after the word "Authority" the following;

"consent" means any freely given, specific, informed and unambiguous indication of the data subject's wish which he or she, by a statement or by a clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her;

(ii) Substituting for the definition of "personal data" with the following;

"Personal data" means information about a person from which the person can be identified that is recorded in any form and includes data that relates to-

(a) the nationality, age or marital status of the person;

(b) the educational level, or occupation of the person;

(c) an identification number, symbol or other particulars assigned to a person;

(d) identity data; or

(e) other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual.

JUSTIFICATION

1. To define the words since they are important aspects of the bill.
2. For clarity

3. NEW CLAUSE

Insert a new Clause immediately after Clause 3 to read as follows;

3. "Establishment of the Personal Data Protection Office.

(1) There is established a Personal Data Protection office responsible for personal data protection under the Authority which shall report directly to the Board.

(2) The Personal Data Protection office established in subsection (1) shall be headed by a National Personal Data Protection Director appointed on such terms and conditions as may be specified in his or her instrument of appointment.

(3) The National Personal Data Protection Director shall be a person of high moral character, proven integrity and with the relevant qualifications and experience relating to the functions of the Office.

(4) The Personal Data Protection office shall consist of such other officers as may be necessary for the proper functioning of the office appointed on such terms and conditions as may be specified in the instruments of appointment.

JUSTIFICATION

To establish a Personal Data Protection Office responsible for the implementation of the Act.

4. NEW CLAUSE

Insert a new Clause immediately after the new Clause above to read as follows;

4. "Functions of the Personal Data Protection Office.

(1) For purposes of this Act and in addition to its functions under any other law, Personal Data Protection Office shall-

(a) Oversee the implementation of and be responsible for the enforcement of this Act;

(b) Promote the protection and observance of the right to the privacy of a person and of personal data;

(c) monitor, investigate and report on the observance of the right to privacy and of personal data;

(d) formulate, implement and oversee programmes intended to raise public awareness about this Act;

(e) receive and investigate complaints relating to infringement of the rights of the data subject under this Act;

(f) establish and maintain a Data Protection and Privacy Register

(g) perform such other functions as may be prescribed by any other law or as the office considers necessary for the promotion, implementation and enforcement of this Act;

(2) The Office shall have all powers necessary for the performance of its functions under this Act.

(3) The Office in performing its functions under this Act shall not be under the direction or control of any person or Authority.

JUSTIFICATION

1. To spell out the functions and powers of the Office in implementation of the Act.

5. NEW CLAUSE

Insert a new Clause after the Clause providing for the functions of the Data Protection Officer to provide as follows;

5. "Data Protection Officer

For purposes of this Act, and in so far as it applies to an institution, the head of the institution shall designate a person as the Data Protection Officer responsible for ensuring compliance with this Act."

JUSTIFICATION

To designate a responsible officer for personal data protection and to ensure they take responsibility in the management and protection of personal data.

6. Amendment to Clause 4

Amend Clause 4 by substituting for Clause 4 the following-

"4. Consent to collect or process personal data.

(1) A person shall not collect or process personal data without the prior consent of the data subject.

(2) Notwithstanding subsection (1) personal data may be collected or processed without prior consent of the data subject where the collection or processing of personal data is;

(a) required by law;

(b) authorised by court of competent jurisdiction;

(c) necessary for-

(i) the proper performance of a public duty by a public body; or

(ii) prevention, detection, investigation, prosecution or punishment of an offence or breach of law

(d) for medical purposes;

(e) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(3) The consent or objection by the data subject required under sub-section (1) shall be in the prescribed form.

JUSTIFICATION

1. National security is already covered under Clause 4(2)(b)(iii).
2. The use of court also enhances the principle of accountability.

7. NEW CLAUSE

Insert a new Clause immediately after Clause 4 to read as follows;

"Personal data relating to children.

A person shall not collect or process personal data relating to a child unless the collection or processing thereof is;

(a) carried out with the prior consent of the parent or guardian or any other person having authority to make decisions on behalf of the child;

(b) necessary to comply with the law; or

(c) for research or statistical purposes.

JUSTIFICATION

To safe guard the privacy of personal data of children.

8. Amendment to Clause 5

Amend Clause 5 by;

1. substituting Sub-Clause (1) with the following;

"(1) A person shall not collect or process personal data which relates to the religious or philosophical beliefs, political opinion, sexual life, financial information, health status or medical records of an individual."

2. In Sub-Clause 3, replacing the words *"information"* with the words *"personal data" to read as;*

"(3) A data collector, data processor and data controller may collect or process personal data specified under sub-section(1) where-"

JUSTIFICATION

1. To include health status, financial information and medical records as special personal data.
2. for consistence.

9. Amendment to Clause 6

Redraft Clause 6 to read as follows;

"A data collector, data processor or data controller shall not collect, hold or process personal data in a manner which infringes on the privacy of a data subject."

JUSTIFICATION

1. For consistency, because a person to whom data relates is a data subject.
2. For clarity.

10. Amendment to Clause 7

Amend Clause 7 as follows;

1). In sub-Clause (2)(c) replace the words "the information" with "personal data".

2). In sub Clause (2), delete paragraphs (e) (ii), and (v).

3). Replace paragraph (2)(g) with the following;

"(g) it is for the purpose of historical, statistical or scientific research and the data is not published in a form likely to reveal the identity of the data subject."

JUSTIFICATION

1. For consistency.

2. Enforcement of a law which imposes a pecuniary penalty is already covered under sub-Clause (2)(e)(i).
3. To guard the Act against abuse.

11. Amendment to Clause 8

Amend Clause 8 by replacing the words "person or public body" with "data collector or data controller".

JUSTIFICATION

To maintain consistency in the use of phrases in the Act.

12. Amendment to Clause 9

Amend Clause 9 as follows;

1). In paragraph (a) of sub-Clause (1) by rephrasing as follows;

(a) the nature and category of data being collected.

2). Split sub-Clause (1)(b) into two separate paragraphs as follows;

"(b) the name and address of the person responsible for the collection of data.

"(c) the purpose for which the data is required"

3). Delete paragraph (g) of sub-Clause (1).

2). Delete sub-Clause (3) (b).

3). In sub-Clause 3 (d) interchange the word "revenue" with the word "public".

JUSTIFICATION

1. For clarity.
2. For consistency.

13.Amendment to Clause 11

Amend Clause 11 by replacing Clause 11 with the following;

(1) "A data collector or data processor or data controller shall ensure that the data is complete, accurate, up-to-date and not misleading having regard to the purpose for its collection or processing.

(2) A data subject shall ensure that the personal data given to the data collector or data processor or data controller is complete, accurate, up to date and not misleading.

JUSTIFICATION

1. To oblige the data subject to provide accurate personal data which further enhances the principle of accuracy of data.
2. To also obligate the data controller, data processor or data collector to collect, hold and process accurate data.

14. Amendment to Clause 12

Amend Clause 12 as follows;

1). In sub-Clause (2), delete the words "or provide the data subject with evidence in support of the data"

2). Replace sub-Clause (3) with the following;

> "Where the data controller is not able to comply with the request under subsection (1), the data controller shall inform the data subject of the rejection, and the reasons for the rejection in writing."

3). Delete sub-Clause (4)

JUSTIFICATION

1. For clarity.

15. Amendment to Clause 13

Amend Clause 13 as follows;

1). In sub-Clause (1) interchange the word "only" with the word "be";

2). Delete Sub-Clause (3) (b);

3). Delete sub-Clause (3) (c) (ii)

4). In sub-Clause (3) (c) (iii) insert the word "public" between the word "of" and "revenue";

5). In sub-Clause (3)(c) (iv) delete the words "or are reasonably contemplated";

6). Delete sub-Clause (3)(c)(v);

7). Insert a new sub-paragraph immediately after (iv) to provide as follows;

"(v) Where the processing is carried out in the public interest and such processing does not override the legitimate interests, rights and freedoms of the data subjects.

8). In sub-Clause (3) (d) delete the words "the further processing of data is necessary" and rearrange the remaining part to be a subparagraph of (c) as (c) (vi);

10).Delete Sub-Clause (3)(f).

JUSTIFICATION

1. For clarity.
2. To guard against abuse.
3. For consistency.

16. Amendment to Clause 14

Amend Clause 14 as follows;

1). In Sub-Clause (2) delete paragraphs (b) and(c).

JUSTIFICATION

1. For clarity.
2. For consistency

17. Amendment to Clause 15

Amend Clause 15 by redrafting it as follows;

"Where a data processor or data controller processes or stores personal data outside Uganda, the data processor or data controller shall ensure that-

(a) the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by this Act;

(b) the data subject has consented; or

(c) such processing or storage is for the benefit of the data subject."

JUSTIFICATION

To enhance the conditions for processing or storing personal data outside Uganda.

18. Amendment to Clause 16

Amend Clause 16 as follows;

1). In sub-Clause (1), inserting the words "data collector or data processor" immediately after the word "data controller".

2). Substitute the word "person" with words "data controller or data processor".

JUSTIFICATION

For clarity and consistency.

19. Amendment to Clause 17

Amend Clause 17 as follows;

1). In sub-Clause (1), replacing the word "operator" with "data processor".

2). In sub-Clause (2) replacing the word "ensure" with "protect".

JUSTIFICATION

For clarity and consistency.

20. Amendment to Clause 18

Amend Clause 18 by;

1). Substituting the headnote with the following;

"Data processing"

2). Redraft sub-Clause (1) to read as follows;

> "A data processor shall process personal data only with the prior knowledge and authorization of the data controller and shall treat such personal data as confidential."

JUSTIFICATION

1. The words "operator" or "authorised person" are foreign to the bill. According to the definition Clause it is only the data processor who processes personal data on behalf of the data controller.
2. For clarity.

21. Amendment to Clause 19

Amend Clause 19 as follows;

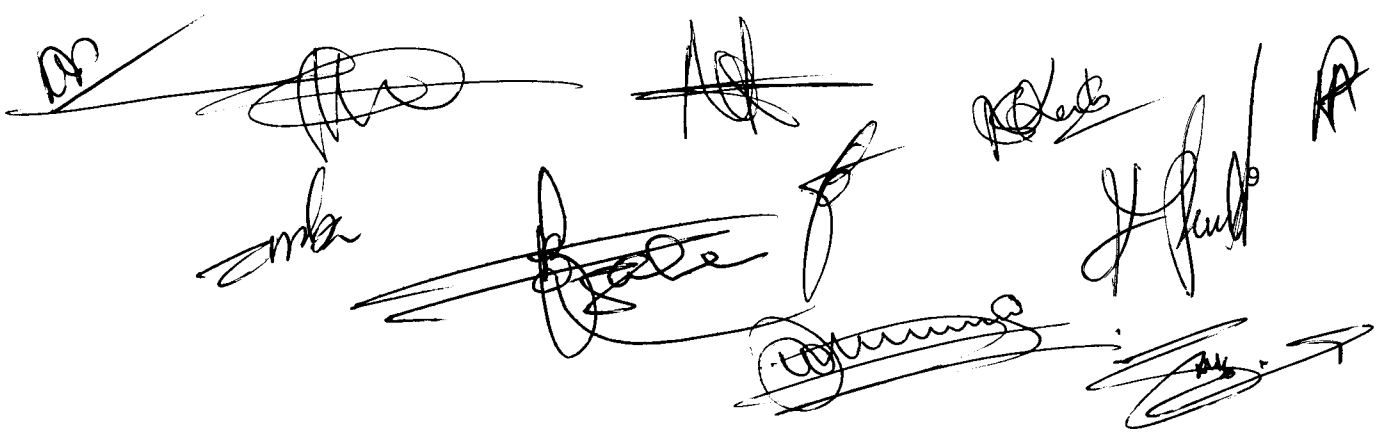
1). In sub-Clause (2), insert the words "data collector or data processor" immediately after the word "controller" wherever it appears in the Clause.

2). In sub-Clause (4) insert the words "referred to in sub section (3) between the words "notification" and "shall".

3).In sub-Clause (4) insert the words "relating to the breach" immediately after the word "information".

4).Delete-sub Clause (5).

5). In sub-Clause (6) the word "may" should be deleted and replaced with shall.



JUSTIFICATION

1. For clarity since there is sufficient belief by the Authority that the data subject would be protected by the publicity of the notification of data breaches.
2. For consistency in the use of words in the Act.

22. Amendment to Clause 20

Amend Clause 20 as follows;

1). Split sub-Clause (1)(b) as follows;

"(b) give a description of the personal data which is held by the data controller;

"(c) provide the identity of a third party or a category of a third party who has or has had access to information."

2). In sub-Clause (4) insert another paragraph (c) immediately after paragraph (b) to provide as follows;

"(c) court orders."

3). In sub-Clause (5)(a), correct the word **"indentifies"** to read "identifies".

4). In sub-Clause (5)(b) delete the words "from that data and" between "or" and "any".

JUSTIFICATION

1. For clarity and consistency.

23. Amendment to Clause 21

Amend Clause 21 as follows;

1). In sub-Clause (1), replace the word "individual" at the end of the sub-Clause with "Data Subject".

2). In sub-Clause (2) replace the words "person concerned" with the words "data subject".

3). Redraft sub-Clause (3) as follows;

"Where the data controller gives reasons for non-compliance, a copy of the notice required by subsection (2) shall be given to the Authority within fourteen days;

4). Redraft sub-Clause (4) as follows;

"(4) Where the Authority is satisfied that the data subject is justified, the Authority shall direct the data controller to comply within seven days".

JUSTIFICATION

1. For clarity.
2. For consistency

24. Amendment to Clause 22.

Amend Clause 22 as follows;

1). Redraft sub-Clause (1) as follows;

> "A data subject may by notice in writing to a data controller, require the data controller to stop processing his or her personal data for purposes of direct marketing."

2). In sub-Clause (2), substitute the words "person concerned" with the words "data subject";

3). Insert a new sub-Clause immediately after sub-Clause (2) to provide as follows;

"(3) Subject to sub-section (1) a data subject may enter into agreement with a data controller for purposes of using or processing his or her personal data for pecuniary benefits."

3). Delete sub-Clauses (3) and (4)

JUSTIFICATION

1. For clarity and consistency.
2. The data subject should retain the authority over the sale of his or her data and not to be at the mercy of the data controller, data processor or Data collector.
3. There is already satisfaction that the data subjects request is valid by the Authority hence the use of "shall".

25. Amendment to Clause 23

Amend Clause 23 as follows;

1). In sub-Clause (3) replace the word "intends" with the words "has taken"

2). delete paragraph (e) of sub-Clause (4)

3). Insert another sub-Clause immediately after sub-Clause (4) to provide as below;

> (5) "Where the data subject is not satisfied with the decision of the data controller in sub Clause (3), the data subject shall complain in writing to the Authority within fourteen days."

4). Redraft sub-Clause (5) as follows;

"(5) Where the Authority is satisfied on a complaint by a data subject that the data controller has failed to comply, the Authority shall order the data controller to comply within seven days."

4). Delete Sub Clause (6).

JUSTIFICATION

1. For clarity and consistency.

26. NEW CLAUSE

Insert a new Clause immediately after Clause 23 to provide as follows;

"24. Right to transfer Personal Data.

A data subject may request a data collector, data processor or data controller to transfer his or her personal data to another data collector, data processor or data controller."

JUSTIFICATION

To provide for a right of data subjects to transfer personal data to other data controllers or data processors if they so wish.

27. NEW CLAUSE

Insert a new Clause immediately after Clause 23 to provide as follows;

"25. Right to share personal data.

A data collector, data processor or data controller with the consent or at the request of the data subject may share personal data with another data collector, data processor or data controller for a lawful purpose."

JUSTIFICATION

To require the data controller, data processor and data controller to only share personal data with the consent of a data subject.

28. Amendment to Clause 27

Amend Clause 27 as follows;

1. In sub-Clause (1) insert the word "the" between the words "with" and "Act" in the headnote to read as follows;

"Complaints against breach and non-compliance with the Act"

JUSTIFICATION

1. For clarity.

29. Amendment to Clause 29

Amend Clause 29 (1) by;

1. Inserting the following words "apply to a Court of competent jurisdiction for " between "to" and "compensation" to read as;

"Where a data subject suffers damage or distress through the contravention by a data controller, data processor data controller of the requirements of this Act, that data subject is entitled to apply to a Court of competent jurisdiction for compensation from the data collector, data processor or data controller for the damage or distress"

JUSTIFICATION

1. To specify that the right to compensation shall be enforced by a court of competent jurisdiction.
2. The provision in its current form is subject to abuse because it allows a person to infringe on the provisions of the Act as long as they can prove reasonable care.
3. For clarity

30. Amendment to Clause 30

Amend Clause 30 as follows;

1. In sub-Clause (1), substitute for the word Minister with the word "High Court".
2. Delete sub Clause (3).

JUSTIFICATION

Article 42 guarantees the right of an aggrieved party to apply to a court of law in respect of an administrative decision taken against him or her. This promotes the rule of law and the doctrine of separation of powers.

31. Amendment to Clause 31

Amend Clause 31 as follows;

Redraft Clause 31 to read as follows;

"31. Unlawful obtaining or disclosing of personal data.

(1) A person shall not unlawfully-

(a) obtain, disclose or procure the disclosure to another person of personal data held or processed by a data collector, data controller or data processor.

(2) A person who contravenes this section commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment for ten years or both."

JUSTIFICATION

1. For consistency and clarity
2. To provide for stringent sanctions for unlawful disclosure and obtaining of personal data.

32. NEW CLAUSE

Insert a new Clause immediately after Clause 31 to read as follows;

"32. Unlawful destruction, deletion, concealment or alteration of personal data.

(1) A person shall not unlawfully destroy, delete, mislead, conceal or alter personal data.

(2) a person who contravenes this section commits an offence and is liable on conviction to a fine not less than two hundred and forty currency points or imprisonment not exceeding ten years or both."

JUSTIFICATION

To provide sanctions against unlawful destruction, deletion, concealment or alteration of personal data.

33. Amendment to Clause 33

Amend Clause 33 by redrafting the Clause to read as follows;

"Offences committed by a body corporate.

(1). Where an offence prescribed under this Act is committed by a body corporate, a director, manager, secretary, or other similar officer, may be held liable for the offence committed.

(2). In addition to any penalty stipulated by the relevant provisions of this Act, the Court may-

(a) impose a penalty not exceeding 4% of the corporation's annual gross turnover; or

(b) order the withdrawal of any license, permit or any other right held by the body corporate under any law."

JUSTIFICATION

1. To enhance the penalties for breaches by corporations under the Act so as to discourage breach.
2. To prescribe the liable persons in case offences committed by bodies corporate.

34. Amendment to Clause 34

Amend Clause 34 by inserting the words "after consultation with the Authority" immediately after the word "May".

JUSTIFICATION

To encourage the involvement of the Authority in coming up with regulations.

35. NEW CLAUSE

Insert a new Clause immediately after Clause 35 to provide as follows;

"36. Transitional

All processing or collection of personal data must within one year after the commencement of this Act be made to conform to the Act."

JUSTIFICATION

To cater for the transitional period after the commencement of the Act.