REPUBLIC OF ZAMBIA

REPORT

OF THE

COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES

ON THE

DATA PROTECTION BILL, N.A.B. NO. 28 OF 2020

FOR THE

FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

Published by the National Assembly of Zambia

REPORT

OF THE

COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES

ON THE

DATA PROTECTION BILL, N.A.B. NO. 28 OF 2020

FOR THE

FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

Table of Contents

REPORT OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES ON THE DATA PROTECTION BILL, N.A.B. NO. 28 OF 2020, FOR THE FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

1.0 MEMBERSHIP OF THE COMMITTEE

The Committee consisted of Mr G M Imbuwa, MP (Chairperson); Ms P Kucheka, MP (Vice Chairperson); Mr D M Kundoti, MP; Mr M Mukumbuta, MP; Dr E I Chibanda, MP; Mr M K Tembo, MP; Dr F Ng'ambi, MP; Mr D Mumba, MP; Mr C D Miyanda, MP and Mr G K Chisanga, MP.

The Honourable Mr Speaker
National Assembly
Parliament Buildings
LUSAKA

Sir,

The Committee has the honour to present its Report on the Data Protection Bill, N.A.B. No. 28 of 2020, for the Fifth Session of the Twelfth National Assembly referred to it by the House on Wednesday, 27th January, 2021.

2.0 FUNCTIONS OF THE COMMITTEE

The functions of the Committee are as set out under Standing Order 157 (2) and among other functions, the Committee is mandated to consider Bills that may be referred to it by the House.

3.0 MEETINGS OF THE COMMITTEE

The Committee held nine meetings to consider the Data Protection Bill, N.A.B. No. 28 of 2020.

4.0 PROCEDURE ADOPTED BY THE COMMITTEE

In order to acquaint itself with the ramifications of the Bill, the Committee sought both written and oral submissions from the stakeholders listed at Appendix II.

5.0 BACKGROUND TO THE BILL

The African Union Convention on Cyber Security and Protection of Personal Data was adopted by the Assembly of Heads of State and Government of the African Union in June, 2014. On 29th January, 2016, the President of the Republic of Zambia signed the African Union (AU) Convention on Cyber Security and Protection of Personal Data during the 26th Ordinary Session of the Assembly of Heads of State and Government of the AU. The AU Convention addressed four main areas, namely:

i) electronic transactions;
ii) personal data protection;
iii) electronic Commerce; and
iv) cyber security and cybercrime

The Convention provided a guideline for Member States to formulate appropriate legal frameworks that would empower their citizens and ensure their respective online environment was trusted, safe, beneficial and empowering to all individuals.

In 2017, the Government, through the Ministry of Transport and Communications commenced the process of reviewing the *Electronic Communications and Transactions Act, No 21 of 2009,* in line with the AU Convention on Cyber Security and Data Protection and in harmonisation with the proposed SADC model laws.

In 2018, Government approved the repeal of the *Electronic Communications and Transactions Act, No 21 of 2009*, and the replacement of the Act with three standalone laws that would be in line with regional and international best practice and would be responsive to the needs of the Zambian people. Therefore, the *Electronic Communications and Transactions Act, No 21 of 2009,* was to be repealed and replaced with the following laws:

(a) Electronic Communications and Transactions Bill;
(b) Data Protection Bill; and
(c) Cyber security and Cybercrimes Bill.

In the fourth quarter of 2019, Cabinet approved the Ratification of the Convention on Cyber Security and Data Protection (Malabo Convention) and approved for presentation before Parliament the two bills, namely: Data Protection and Electronic Communications and Transactions. Further, Parliament in November 2020 also approved the ratification of the Convention by Zambia.

In view of this, the Government introduced the Data Protection Bill N.A.B No. 28 of 2020.

6.0 OBJECTIVES OF THE BILL

The objectives of the bill were to:

(a) provide for an effective system for the use and protection of personal data;

(b) regulate collection, use, transmission, storage and otherwise processing of personal data;

(c) establish the Office of the Data Protection Commissioner and provide for its functions;

(d) provide for the registration of data controllers and licensing of data auditors;

(e) provide for the duties of data controllers and data processors;

(f) provide for the rights of data subjects; and

(g) provide for matters connected with, or incidental to, the foregoing.

7.0 SALIENT PROVISION OF THE BILL

The salient provisions of the Data Protection Bill, N.A.B. No. 28 of 2020, were as set out below.

PART I – PRELIMINARY PROVISIONS

Clause 1 – Short title and commencement

Clause 1 Provided for the short title and the date of commencement of the Bill.

Clause 2 – Interpretation

This clause sought to provide for interpretation of certain selected words and phrases for ease of understanding of the Bill.

Clause 3 – Application

This clause sought to set out the boundaries of the application of the Bill. It excluded the processing of personal data by individuals for personal use.

PART II – OFFICE OF THE DATA PROTECTION COMMISSIONER

Clause 4 – Establishment of the Office of the Data Protection Commissioner

This clause provided for the establishment of the Office of the Data Protection Commissioner which would be housed in the ministry responsible for communication. The clause also provided for the functions of the Office of the Data Protection Commissioner which included registering data controllers and data processors.

Clause 5 Data Protection Commissioner

This clause provided for the appointment, qualifications and functions of the Data Protection Commissioner.

Clause 6 - Appointment of Deputy Data Protection Commissioners and Other Staff

The clause provided for the appointment, by the Civil Service Commission, of the two Deputy Data Protection Commissioners and other staff that were necessary for the performance of the functions of the Office of the Data Protection Commissioner.

PART III – INSPECTORATE

Clause 7 – Inspectors

The clause provided for the appointment of suitably qualified inspectors by the Civil Service Commission.

Clause 8 – Powers of Inspector

The clause provided for the powers of inspectors appointed under clause 7. It empowered an inspector to, with a warrant and at reasonable times, enter and inspect any business premises of a data processor or data controller, remove from the premises equipment, commodities or product used in contravention of the Act, inspect equipment and supplies in or about the licensed premises, among other things.

Clause 9 – Arrest without warrant

This clause empowered an inspector to arrest a person without a warrant if an inspector had reasonable grounds to believe that, the person had committed an offence, was about to commit an offence or was willfully obstructing an inspector in the execution of the inspectors duties.

Clause 10 – Seizure of property

The clause sought to empower a law enforcement officer to seize and detain property that the inspector had reasonable ground to believe that it was or was being used to commit an offence under the Act.

Clause 11 – Restoration of property

This clause provided for the restoration of property by the courts where the owner of the property had been found not guilty or the proceedings have been withdrawn. It also provided for the forfeiture of the property where the owner could not be found.

PART IV – PRINCIPLES AND RULES RELATING TO PROCESSING OF PERSONAL DATA

Clause 12 – Principles relating to processing of personal data

Clause 12 provided seven principles of data processing that every data processor and data controller must ensure were applied in the processing of personal data.

Clause 13 – Processing of personal data

Clause 13 provided circumstances when personal data may be processed, one of which was where the processing was necessary and the data subject had given consent to the processing of that data.

Clause 14– processing of sensitive personal data

Clause 14 prohibited the processing of sensitive personal data and set out the conditions under which such data may be processed.

Clause 15- consent, justification and objection

Clause 15 provided conditions and circumstances under which personal data may be processed. It mandated a data processor and data controller to obtain written consent before processing of personal and also to inform the data subject of that data subject's right to withdraw that consent at any time.

Clause 16- Collection of personal data

This clause sought to mandate a data controller to collect personal data directly from a data subject. The clause further provided for instances when this requirement may be dispensed with.

Clause 17 – Processing of child and vulnerable person's personal data

The clause sought to provide for conditions that a data controller must meet in order to process personal data of a child or a vulnerable person. It provided for safeguards in the processing of personal data where the data subject was a child or a vulnerable person as defined in the Bill.

Clause 18 – Offence and penalty for contravention of personal data obligation

The clause sought to provide for a penalty for contravention of personal data obligations for both corporate bodies and natural persons.

PART V – REGULATION OF DATA CONTROLLERS, DATA PROCESSORS AND DATA AUDITORS

Clause 19- Prohibition from controlling or processing personal data without registration

Clause 19 aimed at providing for a prohibition for any person to control or process personal data without registering as a data controller or a data processor in accordance with the law.

Clause 20 – Application for registration as data processor or data controller

The clause aimed at providing for the procedure of registration of any person who intended to process personal data. It provided for an application to be made to the Data Protection Commissioner in a prescribed manner and on payment of a prescribed fee.

Clause 21 – Registration of data controllers and data processors

The clause sought to provide for the registration of data controllers and data processors by the Data Protection Commissioner within fourteen days on receipt of an application were an applicant met the prescribed requirements.

Clause 22 – Renewal of certificate of registration

The clause provided for the renewal of the certificate of registration by the data processor and the data controller.

Clause 23 - Change in details of data controller or data processor

The clause mandated a data controller and data processor to notify the Data Protection Commission of any change in details of the particulars relating to the registration within seven days of the change.

Clause 24 – Suspension or cancellation of registration

This clause sought to provide for instances when a Data Protection Commissioner may suspend or cancel the certificate of registration.

Clause 25 – Re-registration

The clause sought to provide for an opportunity by the data processor or data controller to apply for re-registration where a certificate of registration was cancelled or suspended.

Clause 26 – Surrender of certificate of registration

The clause sought to provide for the surrender of the certificate of registration by a registered data controller and a data processor where that data controller or data processor intended not to continue providing the services of data processor or data controller.

Clause 27 – Exemption of specific organisations from registration

This clause empowered the Data Protection Commissioner by declaration, to exempt a person for a limited or unlimited period time from the requirements of the Bill.

Clause 28 – Power to forebear

Clause 28 empowered the Data Protection Commissioner to forebear from applying to a data controller any provision of the Bill where the Data Protection Commissioner considered that forbearance was consistent with the objects of the Bill. It further mandated the Data Protection Commissioner to publish in the Gazette a notice of any forbearance granted.

PART VI – DATA AUDITORS

Clause 29 - Data Auditors

This clause empowered the Data Protection Commissioner, on application, to license data auditors in a prescribed manner and form.

Clause 30 – Application for license

This clause sought to provide for the procedure for application for a license for any person who intended to provide data auditing services under this Bill.

Clause 31- Issue of license

The clause provided for the issuance of a license by the Data Protection Commissioner to an applicant where the applicant met the prescribed requirements.

Clause 32 – Condition of license

The clause sought to lay down the conditions upon which a license may be issued and provided for the validity of a license.

Clause 33 – Variation of license

This clause sought to provide for the variation of a license on application by a licensee at any time during the validity of the license.

Clause 34 – Surrender of license

The clause sought to provide for a procedure of surrender of a license where a licensee decided not to continue providing the services under that license.

Clause 35 – Transfer of license

The clause sought to provide for an application to the Data Protection Commissioner for approval by a licensee, where a licensee intended to transfer or assign a license. It further mandated the Data Protection Commissioner to determine an application for approval, within thirty days of such receipt.

Clause 36 – Suspension and Cancellation

This clause provided the grounds under which the Data Protection Commissioner may suspend or cancel a license. The clause further mandated the Data Protection Commissioner to accord a licensee an opportunity to be heard before suspension or cancellation of the license.

Clause 37 – Renewal of license

This clause sought to provide for the procedure for renewal where a licence expired and a licensee intended to renew it. It further provided for the period within which an application for renewal may be made and set out the requirements to be fulfilled for renewal to be granted.

Clause 38 – Functions of data auditor

The clause sought to provide for the functions of a data auditor and among them was the duty to promote adherence to principles of data protection by controllers and processors of data.

PART VII – EXEMPTIONS FROM PRINCIPLES AND RULES OF PROCESSING OF DATA

Clauses 39 to 44

The clauses collectively sought to provide for exemptions from the application of the Part IV in the processing of personal data if processing was for any of the following reasons:

(a) national security, defence or public order;

(b) prevention, detection, investigation and prosecution of contraventions of law;

(c) processing for purpose of legal proceedings;
(d) research, archiving or statistical purposes; or

(e) journalistic purposes.

The Part further provided that the requirement for processing of data under this Part shall be for lawful and legitimate purposes.

PART VIII – DUTIES OF DATA CONTROLLERS AND DATA PROCESSORS

Clauses 45 to 57

The clauses provided for the duties of both the data controllers and data processors. The duties included:

(a) keeping and maintaining a record of all processing activities;

(b) prior to processing, carrying out an assessment of the impact of the envisaged processing operations on the protection of personal data;

(c) providing guarantees regarding the technical and organisational security measures employed to protect personal data;

(d) appointing data protection officers;

(e) notifying the Data Protection Commissioner within twenty four hours of any security breach affecting personal data being processed;

(f) taking necessary measures to comply with the principles and obligations specified in the Bill;

(g) not to engage another data processor without prior authorisation by the Data Protection Commissioner;

(h) obtaining consent from a data subject for any disclosure of that data subject's data;

(i) making available to the data subject any agreement entered into with another data controller with regards to data of that data subject; and

(j) notifying the Data Protection Commissioner of any third party agreement that allowed a third party to trade on the profile of a data subject.

The Part further sought to prohibit a person from processing personal data in legal proceedings except under the circumstances highlighted under clause 56 and also the Part sought to provide for a penalty for any person that contravened the provisions of this Part.

PART IX – RIGHTS OF A DATA SUBJECT

Clauses 58 to 68

These clauses sought to provide for the rights of a data subject. The following were the rights of a data subject set out in this Part:

(a) right of access to data of that data subject's personal data and notification;

(b) right to rectification of any inaccurate personal data concerning the subject's data;

(c) right to erasure of personal data of that data subject's data;

(d) right to object to processing of a data subject's personal data;

(e) right not to be subjected to a decision based solely on automated processing, including profiling;

(f) right to restriction of processing in circumstances laid down in clause 63;

(g) right to be provided with certain prescribed information where data was obtained from another person other than a data subject;

(h) right to data portability;

(i) right to be kept informed by the data controller or processor, of any rectification or restriction in the processing of personal data; and

(j) right to lodge a complaint and an appeal in an event that the data subject was aggrieved by the decision of the Data Protection Commissioner and the Minister respectively.

PART X – TRANSFER OF PERSONAL DATA

Clause 70 – Cross-border transfer of personal data

Clause 70 mandated data controllers and processors to process and store data in the Republic. It further empowered the Minister to prescribe categories of personal data that could be stored outside the Republic.

Clause 71 – Conditions for cross border transfer of personal data

This clause provided for conditions under which personal data, other than that categorised by the Minister, may be transferred outside the Republic.

PART XI – GENERAL PROVISIONS

Clause 72 – Right to compensation

The clause provided for the right of a data subject to receive compensation from a data controller as the court may determine for any damages suffered by that data subject.

Clause 73 – offences

Clause 73 criminalised unlawful disclosure of sensitive personal data to another person.

Clause 74 – Power of the Data Protection Commissioner to compound certain offences

Clause 74 aimed at empowering the Data Protection Commissioner to compound certain offences where a person admitted that that person had committed an offence under this Bill.

Clause 75 – Forfeiture

This clause provided for the forfeiture by the court of any medium that was used to commit an offence or which contained data that related to an offence in issue.

Clause 76 – Offences by principal officer shareholder or partner of body corporate or un incorporate body

This clause provided for a penalty where an offence was committed by principal officer, shareholder or partner of a body corporate or unincorporated body.

Clause 77 – General Penalty

The clause sought to provide for a general penalty for any offence were a penalty had not been provided for.

Clause 78- Code of Conduct

The clause empowered the Data Protection Commissioner to prepare a code of conduct for data controllers, data auditors and data processors.

Clause 79- Guidelines

The clause sought to empower the Data Protection Commissioner to issue guidelines that were necessary for the better carrying out of the provisions of in the proposed law.

Clause 80 – Register

This clause mandated the Data Protection Commissioner to maintain a register which contained information as may be prescribed.

Clause 81 – Auditing of data controllers

The clause sought to empower the Data Protection Commissioner and data auditors to audit data controllers annually.

Clause 82 – Regulations

This clause empowered the Minister to issue such regulations as for the better carrying out of the provisions of the Bill.

8.0 CONCERNS RAISED BY STAKEHOLDERS

In supporting the *Data Protection Bill, National Assembly Bill, No. 28 of 2020*, stakeholders raised the following concerns and expressed the view that these needed to be addressed before the Bill could be enacted in order to improve the law.

Clause 2 – Interpretation

Stakeholders noted that under the term 'automated', the last sentence had a typographical error 'Person=s'. They were of the view that this should be replaced with the word "person's".

They also noted that under the term "child abuse data", there was a typographical error "the subject". This should be corrected to read 'the subject'.

The "**A**" before the definition of "data processor" should be deleted.

The Committee was informed that under genetic data there was also a typographical error which needed to be corrected "2009particular". Stakeholders proposed that it should read as "2009 particular".

Data Protection Officer

Stakeholders also noted that there was no definition for The Data Protection Officer in the Preliminary. They proposed that since a data protection officer was an appointed person by the data collector or data processor to ensure that the relevant organisation processes personal data are in compliance with the provisions of the Act, there was need for the position to be defined in the Bill.

The definition of legal practitioner was proposed to read as follows: "Legal practitioner" has the meaning assigned to the words in the *Legal Practitioners Act Chapter 30 of the Laws of Zambia*'

It was also proposed that the word "to" between the words "or" and "one" in the definition of "personal data" in line 4 of the definition be deleted; and that a coma after the word "identifier" be added.

In the definition of "processing", it was suggested that the word "of" should be inserted between the words "out" and "any" in line 4 of the definition.

Definition of "vulnerable person" should come after the definition of "third party" so as to follow the alphabet.

Clause 4 – Establishment of Office of Data Protection Commissioner

Most stakeholders who appeared before the Committee raised concerns regarding Clause 4 which provided that the Office of the Data Protection Commissioner be housed under the Ministry of Transport and Communications. They were of the view that the Office of the Data Protection Commissioner could be a body corporate under the Ministry. They noted that the current provision left it open to interpretation as to whether the Office would be a directorate under the Ministry or an autonomous body corporate under the Ministry. In the view of the stakeholders as a body corporate, the Office of the Data Protection Commissioner could be an innovative institution and, hence attract international collaborators. Once established, the corporate body could be governed through a board to be provided for in the Bill. Stakeholders argued that the Office would not be independent in its operations if placed under the Ministry as a directorate. While acknowledging that it was difficult to have a Data Protection Commissioner that was autonomous of the Government, it was critical to consider the best possible place for the Office to ensure professional independence.

Clause 5 – Data Protection Commissioner

Some stakeholders were of the opinion that the inclusion of qualifications for the Data Protection Commissioner in the Bill may render the qualifications inflexible. They proposed that the Civil Service Commission should determine the qualifications from time to time especially that the area of ICT was ever evolving. Furthermore, the list of stipulated qualifications in the regulations should broadly include related disciplines such as Statistics and Data Science. Further, the structure of the Office of Data Protection Commissioner should not be provided for in the Act as it may lead to rigidity in responding to developments in the area of data management. This was because any changes to the structure under the proposed set up would need an amendment to the Act, which may be a lengthy process.

Clause 6 – Appointment of Deputy Data Protection Commissioners and other staff

Some stakeholders observed that clause 6 provided for the appointment of Deputy Data Protection Commissioners and other staff. In their view, the position of Deputy Data Protection Commissioner was a senior position which required a person appointed in that position to be responsible for the formulation of policies and planning. As a result, stakeholders were of the view that the law should provide a means of identifying a person to be appointed Deputy Data Protection Commissioner. They, therefore, proposed that qualifications for a Deputy Data Protection Commissioner needed to be expressly provided for under clause 6.

Other stakeholders submitted that the appointment of Deputy Data Protection Commissioners and other staff should be on merit by the Civil Service Commission and not on the recommendation of the Data Protection Commissioner to avoid patronage.

Clause 8 - Powers of Inspectors

Stakeholders proposed that in clause 8(5)(b), the word "document" in the second line be replaced with the word "thing" for consistency and avoidance of duplication of the word.

Clause 9 – Arrest without warrant

Most stakeholders raised concern regarding the provision which mandated the Inspector to arrest without a warrant where there was reasonable grounds to believe that the person committed an offence under the Act. While noting that this provision would be subject to abuse, they were of the view that the clause could remain as provided in the Bill because such an action would depend on the gravity and urgency of the matter.

Clause 11- Restoration of property

Some stakeholders proposed that in clause 11(1) (b) the words "enforcement authority" should be replaced with the words "enforcement officer" because the use of the word authority appeared misplaced.

Clause 15 – Consent, justification and objection

Some stakeholders noted that clause 15(1) of the Bill provided that a data controller would not process data unless the data subject consented to the processing in writing. They were of the view that processing data only with the express consent of the data subject would be impracticable for some stakeholders with numerous and widespread membership or clients, covering both the public and private sectors, who may not be easily reachable. Further, they argued that information at times was demanded through a court order which compelled an organisation to disclose information without a written consent from the data subject. Stakeholders, therefore, were of the view that certain categories of organisations with huge client base should be exempted from seeking their clients' consent.

Clause 17 – Processing of child and vulnerable persons personal data

It was proposed that in clause 17, the words "or vulnerable person's" be added after the word "child's" wherever it appeared for inclusion and consistency with the other clauses.

Clause 19 – Prohibition from controlling of processing personal data without registration

Stakeholders also noted that Part V, clause 19(1) provided that a person shall not control or process personal data without registering as a data controller or data processor, clause 20 provided for application for registration as data processor or data controller; clause 21 provided for registration of data controllers and data processors and clause 22 provided for the renewal of certificate of registration as being functions of the Data Protection Commissioner in the Bill. These functions were already a mandate of the Information and Communications Technology Association of Zambia (ICTAZ). Therefore, the functions of the Data Protection Commissioner as proposed in the Bill would be a replication of some of the functions of the ICTAZ.

Clause 22 – Renewal of certificate of registration

Stakeholders noted that clause 22(1) provided that a registered data controller or data processor may apply to the Authority for renewal of a certificate of registration as provided in the Bill. However, they noted that the Authority, in Part I, of the Bill, referred to the Zambia Information and Communications Technology Authority (ZICTA) which was established by the *Information Communications and Technology Act, No. 15 of 2009*. They proposed that the renewal should be done through the Office of the Data Protection Commissioner whose functions would be, among others, registering, licencing, and keeping and maintaining the register of controllers and data processors as provided in clause 4(2)(a) of the Bill.

Clause 24 – Suspension or cancellation of registration

In clause 24(1) (c), stakeholders proposed that the word "and" should be replaced with the word "or" after the word 'registration' because suspension or cancellation can be based on any of the items in (a) to (d) and not upon satisfaction of all. In clause 24(4), they suggested the replacement of the word "will" with the word "shall" between the words "commissioner" and "prescribe" so as to use a mandatory word to create an obligation.

Clause 27 – Exemption of specific organization from registration

Stakeholders were of the view that the marginal note in clause 27, should be amended to read as "Exemption from registration" so as to reflect the essence of the substantive provision which was wider than the current marginal note.

Clause 30 – Application for licence

Stakeholders observed that clause 30(4) provided that where an application for a licence was rejected, the Data Protection Commissioner would inform the applicant in writing stating the reasons. However, the reasons for rejecting an application have not been provided in the Bill. Stakeholders were of the view that the reasons for rejecting an application should be stated the same way clause 36 provided for reasons that may lead to the suspension or cancellation of a licence.

Clause 33 – Variation of licence

Some stakeholders proposed that in clause 33(3) (a), the word "or" should be added after the words "public interest" because public interest can be based on any of the items and not all.

Clause 35 - Transfer of Licence

Stakeholders submitted that in clause 35(3), the word "Protection" should be added between the words "Data" and "Commissioner" for completeness.

Clause 37 – Renewal of Licence

In clause 37, it was suggested that subsection (5) should be numbered as subsection (3).

Clause 38 – Function of data auditor

Stakeholders noted that the provision for functions of data auditor was misplaced. They were of the view that clause 38 be placed after clause 29 for ease of reading, understanding and reference.

Clause 39 – National Security, Defence and Public Order

Stakeholders were of the view that clause 39 should be amended to read: ''A data controller that processes personal data in the interests of national security, defence and public order is exempt from the provisions of part IV, except; as provided in clause 12(1)(c), (d), (e) and (g); and clause 47'' to make it complete.

Clause 40 – Prevention, Detection, Investigation and Prosecution of Contraventions of Law

Stakeholders proposed that clause 40(2) be amended to read as follows: "Processing authorised by law under clause 40(1) shall be exempt from the provisions of part IV, except; as provided in clause 12(1)(c), (d), (e) and (g); and clause 47''. The inclusion was seemingly omitted.

Clause 42 – Research, Archiving or Statistical Purposes

Stakeholders proposed that new clause 42(2) and (3) be inserted in clause 42 to read as follows:

> *(2) - Despite clause (1), where sensitive personal data is being processed for scientific or historical research purposes by a person other than a public body, that person shall not process such sensitive personal data without the authorisation of the Data Protection Commissioner and*

(3) - where personal data is being processed for scientific research purposes by a person other than a public body, that person shall ensure that the personal data is anonymised.

The inclusion is meant to enhance the necessary restrictions on the processing of sensitive personal data to ensure that the data could be protected.

Clause 46 – Data Protection Impact Assessment

Stakeholders proposed that clause 46(2) (a) should be amended to read: "personal data is processed using an automated processing system, including profiling, which produces legal effects concerning the natural person or similarly significantly affects that natural person". They contend that the current provision does not read well and may not convey what was intended.

Clause 49 – Notification of security breach

Stakeholders noted that clause 49 provided that the data controller notified the Authority within twenty-four hours of any security breach affecting personal data processed. However, the Authority in clause 2, referred to ZICTA. The stakeholders were of the view that notification of security breach should be directed to the Data Protection Commissioner who was responsible for data protection. They also proposed that the words "Data Protection Commissioner and" be added before the words "the Authority" and that the words "twenty" and "four" in clause 49(1) in the second line be separated.

Clause 52 – Duties of Data Processors

In clause 52(3), the spelling of the word "matter" should be corrected in the last line.

Clause 55 – Offence by Data Controller

Stakeholders suggested that the words "or two million penalty units" be inserted between the words "year" and "whichever" in clause 55(1) as the penalty appears to have been left out.

Clause 65 – Right to Data Portability

It was proposed that clause 65(1) be amended to read: "A data subject shall have the right to receive that data subject's personal data in a structured, commonly used, machine readable or otherwise legible format and may transmit that data to another data controller". The proposed amendment was intended to ensure for clarity and the rights of the data subject.

Clause 67 – Derogation from Rights

Stakeholders were of the view that clause 67(d) should be amended to read as "subject to clause 42 for historical or scientific research purposes". This was meant to reconcile the provision within clause 42 so that they were not contradictory.

Clause 70 – Cross-border transfer of personal data

Some stakeholders noted that clause 70(2) allowed the Minister to specify which personal data could be stored outside Zambia. . However, stakeholders were of the view that there was need to qualify the statement so that personal data on critical databases or information important for national security or the economic and social well-being of the Republic could not be stored outside Zambia.

Other stakeholders argued that although this clause allowed a data controller to store data on "a server or data centre located outside the Republic", it would be prudent for the Bill to provide a clause that stipulated that "all data in the Republic shall be stored on local servers". This would ensure that the existing data infrastructure being put in place by Infratel was fully utilised. This was because the absence of such a clause could lead to bodies corporate, especially foreign entities, opting to store their data outside the country. This storage of data outside the county may not be a good idea, particularly, that most of the data related to local persons.

Further, stakeholders noted that while clause 70 permitted the Data Controller to store personal data on server or data centre located in Zambia. This could result in additional costs to doing business where existing data controllers currently stored their data in other jurisdictions beyond Zambia. They were of the view that an impact assessment should be conducted. The results of a regulatory impact assessment should be used to ascertain whether a necessary requirement for businesses as the attendant benefits outweigh the anticipated additional cost to businesses.

Clause 75 – Forfeiture

Stakeholders noted that the Bill provided for forfeiture of medium containing personal data to courts of law where there had been a conviction. However, they were of the view that the nature of electronic medium would be that it may contain other sensitive information relating to data subjects not involved in the investigation. Additionally, the media may also contain other information that may be critical to the operations of the data controller or processor. They proposed that the Bill needed to consider extracting specific information from the medium or the duplication of medium for purposes of fulfilling court proceedings. This was because if that was not done, it could have major business disruption for entities concerned and systemic implications.

9.0 GENERAL CONCERNS

Stakeholders made some general observations regarding the provisions of the Bill as outlined below.

(a) While stakeholders supported the proposal for "anonymisation", "encryption" and "pseudonymisation" of personal data, they were of the view that the implementation of the legislation required proper management for the legislation to be accepted by citizens. They submitted that once the Bill was enacted into law, it would be necessary to sensitise all stakeholders on the operations of the Data Protection Commission and its functions, especially small and medium enterprises (SMEs) who may have to implement the law.

(b) While stakeholders acknowledged that implementing legislation in relation to data protection was important, they were of the view that it would be important to appreciate that the technology being used for data protection was dynamic. Therefore, it would be cardinal for the country to periodically review the legislation so that it could remain in tandem with the technological changes globally. The Committee was also informed that the term Inspector was not defined under Part I, Preliminary. In this regard, they were of the view that the term "Inspector" be clearly defined.

(c) Stakeholders explained that provision for an appeal procedure was very important especially as it related to registration of officers such as data processors and controllers. However, they proposed an inclusion of an intermediate stage such as an arbitrator before the High Court to determine simple cases. They further added that an adhoc tribunal encompassing individuals with suitable legal qualifications similar to those of High Court Judges appointed by the Minister should be established as an intermediary measure between the Data Protection Commission and High Court.

10.0 COMMITTEE'S OBSERVATIONS AND RECOMMENDATIONS

Having interacted with various stakeholders with regard to the Bill, the Committee makes observations and recommendations as outlined below.

(a) Establishment of Office of Data Protection Commissioner

The Committee notes that clause 4(1) proposes to establish the Office of the Data Protection Commissioner under the Ministry of Transport and Communications. However, the provision is silent on whether the Office will be a directorate under the Ministry or an autonomous body corporate. While acknowledging that it is difficult to have a Data Protection Commissioner that is autonomous of the Government, the Committee finds it critical to consider the best possible place for the Office that will assure professional independence. In this regard, the Committee recommends that the Office of the Data Protection Commissioner be an autonomous body under the Ministry in order to inspire confidence among stakeholders and ensure that enforcement of regulations is without bias.

(b) Appointment of the Data Protection Commissioner

The Committee observes with concern the proposal to in clued the qualifications for the Data Protection Commissioner in the Bill as it may not be easy to adjust them accordingly when need arises. The Committee is of the view that the Civil Service Commission should determine the qualifications from time to time considering that the area of ICT is dynamic. Further, the structure of the Office of Data Protection Commissioner should not be enshrined in the Act as it will be difficult to respond timely respond to developments in the area of data management. This is because any changes to the structure will need an amendment to the Act, which may be a lengthy process.

(c) Harmonisation of the functions of the Data Protection Commissioner and the Information Communications Technology Association of Zambia

The Committee notes that the Bill provides in clauses 19 to 22 for the functions of the office of the Data Protection Commissioner which include areas where the Information and Communications Technologies Association is already mandated to perform. The Committee is of the view that the *Information Communication Technologies Association of Zambia Act, No. 7 of 2018*, and the Data Protection Bill, N.A.B. No 28 of 2020, should be harmonised in order to address the potential conflict and duplication of roles that may arise regarding the respective mandates.

(d) Renewal of certificate of registration

The Committee observes that clause 22(1) provides that a registered data controller or data processor may apply to the Authority for a renewal of a certificate of registration as provided in the Bill. However, the Committee notes that the Authority in Part I of the Bill, refers to the Zambia Information and Communications Technology Authority (ZICTA). In this vein, the Committee recommends that renewal of certificate of registration should be carried out by the Office of the Data Protection Commissioner who is mandated to, among others, register, licence, and keep and maintain registers of controllers and data processors as provided under clause 4(2).

(e) Consent to data processing

The Committee notes that clause 15(1) of the Bill provides that a data controller shall not process data unless the data subject consents to the process in writing. The Committee agrees with the stakeholders who argue that processing data only with the express consent of the data subject will be impracticable because some stakeholders have numerous and widespread membership which may not be easily reachable. Additionally, personal data is sometimes demanded by way of court order which makes it difficult for data subjects to consent in writing. In this regard, the Committee recommends that this provision should be revisited to provide an exemption to public bodies processing data in their course of duty.

(f) Review of legislation

The Committee notes that while it is important to implement the data protection legislation, the information technology sector is dynamic which means that even the technology being used for data protection will be dynamic. Therefore, the Committee recommends that it will be prudent for the country to periodically review the legislation so that it remains in tandem with the technological changes that are happening globally.

(g) Data storage outside the country

The Committee is of the view that, while the Bill allows a data controller to store data on a server or data centre located outside the Republic, the national economy or national security could be compromised if certain sensitive data was stored on servers outside the country. This provision will also be against the country's aspiration for job creation and may compromise the sovereignty of the nation. Further, the auditing of the data stored outside the county may be difficult because of unfriendly laws in other countries. In view of the foregoing, the Committee recommends that where cloud computing is allowed, the institutions that store personal data in other jurisdiction should be held accountable locally in case of a breach.

11.0 CONCLUSION

The National Assembly recently ratified the African Union (AU) Convention on Cyber Security and Personal Data Protection. In this regard, it is necessary that the Convention is domesticated for it to have the force of law in Zambia. The Data Protection Bill, if enacted, will result into an effective system for the use and protection of personal data. Its enactment will ensure that there is regulation on the collection, use, transmission and storage of personal data. This Bill is, therefore, progressive.

The Committee wishes to express its gratitude to all stakeholders who appeared before it and tendered both oral and written submissions; and to thank you, Mr Speaker, for affording it an opportunity to scrutinise the Bill. The Committee also appreciates the services rendered by the Office of the Clerk of the National Assembly and the permanent witness from the Ministry of Justice.

We have the Honour to be, Sir, the Committee on Media, Information and Communication Technologies mandated to consider the Data Protection Bill, N.A.B. No. 28 of 2020, for the Fifth Session of the Twelfth National Assembly.

Mr G M Imbuwa, MP,
(Chairperson)

Mrs P C Kucheka, MP
(Vice-Chairperson)

Mr D M Kundoti, MP

(Member)

Mr M Mukumbuta, MP
(Member)

Dr E I Chibanda, MP
(Member)

Mr M K Tembo, MP
(Member)

Dr F Ng'ambi MP
(Member)

Mr D Mumba, MP
(Member)

Mr C D Miyanda, MP
(Member)

Mr G K Chisanga
(Member)

APPENDIX I – National Assembly Officers

Ms C Musonda, Principal Clerk of Committees
Mr F Nabulyato, Deputy Principal Clerk of Committees (SC)
Mr C K Mumba, Senior Committee Clerk
Ms C R Mulenga, Committee Clerk
Mr C Bulaya, Committee Clerk
Mr S Samuwika, Committee Clerk
Mrs R M Kanyumbu, Typist
Mr D Lupiya, Parliamentary Messenger

APPENDIX II – The Witnesses

PERMANENT WITNESSES

MINISTRY OF JUSTICE
Mrs O Sakala, Deputy Chief Parliamentary Counsel
Ms M Siwiwaliondo, Senior Parliamentary Counsel
Mrs N Nchito, Senior Parliamentary Counsel

MINISTRY OF TRANSPORT AND COMMUNICATIONS
Hon. M Kafwaya, MP, Minister of Transport & Communications
Eng. M Lungu, Permanent Secretary –
Mr Y Bwalya, Director -Communications
Mr S Mbewe, Director Planning & Monitoring
Mr A Sichinga, Assistant Director –Technical
Mr N Nkunika, Assistant Director –Policy
Ms S Musonda, Principal Communications Officer –Infrastructure
Ms C Phiri, Principal Communications Officer -M&E
Ms L M Munyama, Senior Planner

MINISTRY OF FINANCE
Mr C Chikuba, Permanent Secretary – Economic Management and Finance
Mr I Akapelwa, Assistant Director – Economic Management Department
Mr E Sakanyi, Principal Planner – Economic Management Department
Mr M Mweemba, Senior Economist - Economic Management Department
Ms I Kafwenba, Senior Economist - Economic Management Department

MINISTRY OF HEALTH
Dr K Malama, Permanent Secretary, Technical Services
Mr E Ngulube, Permanent Secretary - Administration
Dr C Sichone, Director – Health Policy
Mr P Chishimba, Director, Monitoring and Evaluation
Mr A Kashoka, Assistant Director- ICT
Dr A Kabalo, Health Promotion Environment and Social Determinants
Mr E Malikana, Deputy Director Health Policy

ZAMBIA INFORMATION AND COMMUNICATIONS AUTHORITY
Mr P Mutimushi, Director General
Mr T Malama, Director Legal
Mr M Mutale, Director Technology and Engineering
Mr N Samatebele, Manager Cyber Security
Ms M Chisha, Acting Manager Legal
Mr A Mpondela, Legal Officer

INFORMATION COMMUNICATION TECHNOLOGY ASSOCIATION OF ZAMBIA (ICTAZ)

Mr C Lalusha, Vice-President
Mr C Sinyangwe, Member
Ms S Y Mavula, Chief Executive Officer and Registrar

ZAMBIA STATISTICS AGENCY (ZAMSTATS)
Mr M Musepa, Director General
Mr N Bukoka, Chief Statistician
Mr Kafuli, Assistant Director Population and Social Statistics

NATIONAL PENSION SCHEME AUTHORITY (NAPSA)
Mrs L Chilumba, Director
Mr R Kamanya, Director Strategy and Business Performance
Mrs M Kayombo, Legal Manager Regulatory Enforcement
Mr M Mvula, Area Manager ICT Infrastructure
Ms O Chirwa, Legal Officer Regulatory and Enforcement
Mr B Liyanda, Legal Officer Regulatory and Enforcement
Mr M Kangwa, Senior Manager Information Technology Security
Mr D Chibesakunda, Senior Information Technology Security Officer
Mr D Munyame, Manager, ITC Service Delivery
Mr P Sunkutu, Manager Business Applications

ZAMBIA REVENUE AUTHORITY (ZRA)
Mr K Chanda, Commissioner General
Mr E Phiri, Director, Research

INFRATEL
Mr Bwalya, Chief Executive Officer
Mr Z Mbumwae, Chief Information Officer
Mr S Kaonga, Legal Counsel

COPPERBELT UNIVERSITY (CBU)
Mrs F Bwalya, Manager – ICT Operations
Dr J Kalezhi, Dean – School of ICT
Mr P Hampande, Director – CBU – IBIC
Mr G Phiri, Monitoring and Evaluation Officer
Mrs C Mwembeshi, Manager Quality Assurance and Security Center for ICT

ZCAS UNIVERSITY
Dr E S B Jere, Dean – School of ICT

BLOGGERS OF ZAMBIA
Mr R Mulonga, Chief Executive Officer
Ms B Nkowani, Programmes Coordinator
Ms M Dambwa, Programmes Officer

SMART ZAMBIA INSTITUTE (SZI)
Mr M Makuni, Director, eGovernment
Ms N Mwanza, Assistant Director, Standards

Ms G Nkula, Head Quality Assurance and Security
Mr J Chipeta, Principal Policy
Mr S Mbuzi, Senior Security Officer
Ms C Chipango, Senior Policy Officer

UNIVERSITY OF ZAMBIA (UNZA)
Dr O Muyati, Dean School of Natural Science
Dr M Nyirenda, Head of Department Computer Science
Mr D Zulu, Senior Lecture Computer Science,
Mr D Leza, Acting Director Center for ICT
Mrs C Mwembeshi, Manager Quality Assurance and Security Center for ICT

BANK OF ZAMBIA
Dr F Chipimo, Deputy Director – Operations
Mrs R C Mhango, Deputy Governor – Administration
Mr F Hara, Chief of Staff
Ms G Mposha, Director – Bank Supervision Department
Ms F Tamba, Director – Non-Bank Financial Institutions Department
Mrs C Punabantu, Acting Director – Board Services Department
Mr L Kamamga – Director – Banking Currency and Payment Systems
Mrs H Banda, Deputy General Counsel
Ms B Mwanza, Assistant Director – Communications
Dr J Lungu, Assistant – Governor's Office
Mr C Kapembwa, Executive Assistant – Deputy Governor – Operations
Ms P Sinkamba, Executive Assistant – Deputy Governor - Administration

BANKERS ASSOCIATION OF ZAMBIA
Mr H Kasekende, Standard Chartered Bank (CEO) - Bankers Association of Zambia Chairperson
Ms R Kavimba, Standard Chartered Bank, BAZ Legal Committee Vice Chairperson
Mr W Luwabelwa, Stanbic Bank, Chief Compliance Officer/ BAZ Legal Representative
Ms J Mtaja, Zanaco Bank, Regulatory and Advisory Specialist
Ms A Malama, Standard Chartered Bank, Country Technology Manager
Mr C Lalusha, Absa Bank, Chief Information Officer
Mr A Chisha, Zanaco Bank, Head Core Banking & Enterprise Applications
Ms K Kaulungombe, Zanaco Bank, Company Secretary & Acting Chief Legal Officer
Mr L Mwanza, Bankers Association of Zambia, Chief Executive Officer
Ms M Zimba, Bankers Association of Zambia, Public Relations & Administrative Officer

MULTICHOICE
Ms G Zulu, Head Regulatory Affairs, MultiChoice Zambia
Ms Kate Munuka, MultiChoice Southern Africa Compliance Manager
Mr U Nel, Principal CII Governance MultiChoice Africa
Mr L Momba, Head Regulatory Affairs Southern Region

ICT COLLEGE
Mr G Mumba, Acting Executive Director
Mr J Silungwe, Direct5or ICT

AIRTEL ZAMBIA
Mr J Chulu, Legal Counsel