

**MISA-Zimbabwe Commentary**

**Cybersecurity and Data Protection Bill HB 18 of 2019**

Contents

[INTRODUCTION 2](#_Toc43374603)

[DECLARATION OF RIGHTS 3](#_Toc43374604)

[SUMMARY STRUCTURE OF THE BILL 4](#_Toc43374605)

[ANALYSIS OF SECTIONS 4](#_Toc43374606)

[Part I 4](#_Toc43374607)

[Part II 6](#_Toc43374608)

[Part III 7](#_Toc43374609)

[Part IV and Part V 9](#_Toc43374610)

[Part VI 12](#_Toc43374611)

[Part VII 16](#_Toc43374612)

[Part IX 17](#_Toc43374613)

[Part X 18](#_Toc43374614)

[Part XII 19](#_Toc43374615)

[CONCLUDING RECOMMENDATIONS 20](#_Toc43374616)

# Preface

MISA Zimbabwe produced a summary statement on the Bill immediately after its gazetting. This commentary reflects expanded reflections and recommendations to improve the current Bill.

# INTRODUCTION

After several attempts, Zimbabwe gazetted the Cyber security and Data Protection Bill 2019 (hereinafter the “Bill”) on Friday 15 May 2020. The Bill responds to the growing technological dictates. Zimbabwe, like many jurisdictions suffer “law-lag” as the enactment of laws is slower than the technological developments. Laws regulating cyber security, criminal laws, and data protection are archaic. Criminal provisions in the Criminal Law (Codification and Reform) Act (Criminal Code), were not exhaustive. The Access to Information and Protection of Privacy Act (AIPPA) on data and personal information protection remains inadequate, and myriad with controversial provisions.[[1]](#footnote-1)

This paper is an in-depth analysis of the proposed Bill and incorporates global and regional developments in respect of cyber security and data protection laws. The Constitution and other international human rights standards anchor the commentary and recommendations. The commentary makes recommendations for Parliamentarians to consider for purposes of revising the Bill. Relevant recommendations from zero drafts have also been incorporated and reiterated.

# DECLARATION OF RIGHTS

The Bill is measured and reviewed against the Constitution which is the supreme law of the land. Of relevance are the following sections

* Section 51 on the right to dignity;
* Section 52 on right to personal security;
* Section 57 on right to privacy;
* Section 61 and 62 on freedom of expression, freedom of the media
* Section 68 on the right to administrative justice;
* Section 69 on right to a fair hearing;
* Section 70 on the rights of accused persons
* Section 81 on rights of children protection from sexual exploitation.

These rights while clearly framed in the Constitution, are not the only ‘rights’. The term ‘right’ should not be limited to rights that are only provided for under the Constitutions’ Declaration of Rights. The Constitution in section 47 provides that the entrenchment of the Declaration of Rights “does not preclude the existence of other rights and freedoms that may be recognised or conferred by law, to the extent that they are consistent with this Constitution”. Mavedzenge (2017) observed that “the term ‘any right’ includes those rights conferred upon the citizens by any legislation, common law, customary law or international law that is applicable in Zimbabwe”.[[2]](#footnote-2)

Zimbabwe ratified the African Charter on Human and Peoples Rights, the International Covenant on Civil and Political Rights. Other international instruments include the United Nations Convention Against Transnational Organized Crime, and its Protocol to Prevent, Punish and Suppress Trafficking in Persons, Especially Women and Children. All these instruments have rights that are not inconsistent with the Constitution.

Section 326 of the Constitution provides that customary international law is part of the law of Zimbabwe, unless it is inconsistent with this Constitution or an Act of Parliament, and “when interpreting legislation, every court and tribunal must adopt any reasonable interpretation of the legislation that is consistent with customary international law applicable in Zimbabwe, in preference to an alternative interpretation inconsistent with that law”. This provision is progressive. The rights might not be incorporated in domestic law, but they are not inconsistent either. The state is encouraged to not interpret rights contrary to international law. Section 327 provides for ratification of international treaties and conventions, and their subsequent domestication.

# SUMMARY STRUCTURE OF THE BILL

* Part I of the Bill covers objects, definitions and scope of application Bill.
* Part II sets out the Cyber Security Centre under Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). In addition to setting up the Cyber Security Centre, this part provides for its functions.
* Part III designates POTRAZ as Data Protection Authority (DPA/Authority) and its functions.
* Part IV and V provides on minimum standards and general rules for a data controller processing of data.
* Part VI provides for principles guiding data controllers, which include security, integrity and confidentiality. This part also covers notification procedures for data breaches.
* Part VII provides protection for data subjects on automated data processing decisions, and the recourse for violation of rights. Data subjects with legal incapacitation are also covered.
* Part VIII focuses on cross border transfer of data, and permissibility, and authorization of the same.
* Part IX provides for codes of conduct and ethics that data controller should observe.
* Part X enables the establishment and management of a whistle blower system.
* Part XI provides for making of regulations by the relevant Minister in consultation with the POTRAZ. This part sets out the offences and penalties.
* Part XII deals with amendments to the Criminal Law (Codification and reform) by repealing section 163 to 166.

# ANALYSIS OF SECTIONS

## Part I

1. ***Code of Conduct***

***Issue***: The code of conduct will have to be approved by POTRAZ as the Data Protection Authority. The code of conduct is meant to “institute the rightful use of IT resources, the Internet, and the electronic communications of the structure concerned”

***Discussion****:* Codes of conduct are provided under s30 of the Bill. The Codes of conduct appear to be mandatory hence their approval by the Authority. This is largely common practice for codes of conduct of this nature. It will be appropriate for industry and associations to come up with codes of conduct as per s 30 (2).

The definition however seems to extend to **IT resources**, and **Internet** for the data controller. IT resources is extremely wide as a definition and it might include equipment, networks, hardware, software, technical knowledge, expertise, information and computer systems in the controller’s control or possession. This definition does not address the fact that data processing is manual, and electronic automated or electronic.

***Recommendations*:** The lawmakers should consider removing the IT resources and Internet on the definition of codes of conduct. In the alternative the definition should confine itself to IT processes which means any processes related to the data controller or processor for purposes of gathering or collecting data and processing data.

1. ***Consent***

***Issue***: Consent is essential to processing of personal and sensitive data.

***Discussion***: This definition is critical as it enables and establishes whether data is being processed lawfully or otherwise. The current definition of consent is not sufficient. The definition must be expanded in regulations or codes of conduct. Consent must be clear and unequivocal. It shows agreement, acceptance, concurrence or granting of authority to a processor to process data. Reference can be made to Kenya and South Africa definitions.[[3]](#footnote-3) The Kenyan Bill uses *“manifestation and unequivocal”.*

Some of the issues to consider in defining consent in regulations or codes of conduct include that:

* It must be in written statement signed by the data subject or by their guardian (if legally incapacitated that includes minor or individuals unable to attest).
* If associated with forms, or end user level agreements (EULA), it must clearly spell out and explained
* If electronic this may include ticking a box when visiting an internet website. The ticking of a box should not be silent activated.
* If consent request is through or by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided
* If granted, consent should cover all processing activities carried out for the same purpose or purposes, and if processing is for multiple purposes all purposes should be consented.

***Recommendations***: Sections on consent are spread throughout the Bill’s provisions on processing of data. However, through regulations, the Bill can be strengthened on how to specify the various nature and forms of consent considered sufficient. Further, the burden of proof that consent was given should be on the data controller. At the very minimum the definition must encapsulate the following attributes to constitute lawful consent: freely given in that the person must not be pressured into giving consent or suffer any detriment if they refuse; Specific, in that the person must be asked to consent to individual types of data processing. Informed; the person must be told what they're consenting to. Unambiguous - language must be clear and simple. Clear affirmative action; the person must expressly consent by doing or saying something or doing something.[[4]](#footnote-4)

1. **Personal information and sensitive data**

***Issue***: Personal information and sensitive data definitions

***Discussion***: Personal information definition can be expanded to include other identifiable elements which are currently not included in the Bill. The definition of personal information can include objective and subjective elements. The Bill includes traffic data in definition of data. This means that a cellphone number or an Internet Protocol (IP) address, e-mail address, location data constitute personal information.

Online identifiers such as IP address, cookie identifiers, or even radio frequency identifications (RFID) tags must be considered as personal information. A customer number or customer account is covered under an identifying number (d). Subjective elements include written answers in a test for education purposes, or responses during job interviews, or performance evaluation report at a workplace, and creditworthiness scores by a bank or credit institution.

Personal health information and status are sensitive and should be accorded the utmost protection that enforces one’s privacy and dignity as per the constitution. Insurance or medical institutions are vulnerable to unlawful disclosures people’s medical history and status. The Bill provides for unique patient identifier, as used for purposes of identifying genetic data. A definition of unique identifier might be necessary for avoidance doubt.

***Recommendation:*** The interpretation of personal information can include other subjective and objective elements of personal information as discussed above.The definition of personal information on health is expansive. This interpretation must be carried forward for defining sensitive data. Further the definition of health personal information can be expanded to include the provision of health care services, which reveal information about one’s health status.

Unique identifier should mean any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party. The responsible party would be in genetics be, the hospital or medical laboratory. This use of unique patient identifiers in processing of health data contributes to safeguards. Medical data is easily transferred across borders. These approaches will safeguard sensitive data.

## Part II

1. **Cyber Security Centre**

***Issue***: Section 5-6 establishes the Cyber Security Centre and its mandate respectively.

***Discussion:*** POTRAZ is established by the Postal Telecommunications Act (PTA). Under the Bill, POTRAZ will advise government on cybersecurity and policy, on cybercrime and establish a computer emergence response team (CERT) or national contact point among other functions of coordination among stakeholders, development of whistle blower protection system, policy advice to the Minister including on legal framework governing cyber security matters and oversee the enforcement of the Act with due regard to fundamental human rights and freedoms.

The mandate and responsibilities of POTRAZ are already wide under the original enabling Act, the PTA. These added powers will make this a super-executive institution, with limited independent oversight. POTRAZ under the PTA reports to the Minister, and no one else. Additional mandate will report to the Minister as well.

***Recommendation:*** the setting up of Cyber Security Centre and public designation of an institution is commendable.[[5]](#footnote-5) The recommendation will be a separate institution to be set up for Cyber Security Centre. However, if the Bill retains POTRAZ in this role then POTRAZ must now report and be accountable to Parliament. Its mandate and enforcement of human rights requires independent oversight and not the executive.

## Part III

1. **Data Protection Authority**

***Issue***: Appointment of DPA/Authority

***Discussion***: The Bill designates POTRAZ as the DPA/Authority under s7, with the powers to perform wider ranging functions under s8. The Bill provides wide ranging powers to POTRAZ, an institution that already controls significant data, processed and or controlled by mobile network operators (MNOs), internet service providers (ISPs), and mobile money operators.[[6]](#footnote-6)

The powers under s 8 are very expansive and what will result is that POTRAZ will be a super-administrative body, and reporting to the executive, through the Minister. The functions of the DPA includes providing policy advice to the Minister on constitutional rights issues on privacy and access to information. The DPA functions are the crux of data protection. A comparative analysis on the appointment process, competencies and removal will enable consideration of alternative framing of this provision.

Section 8(2) grants functional autonomy to the Authority. In the lawful exercise of its functions, the Authority is not subject to the direction or control of any person or authority. This is noteworthy, but not sufficient. The composition of the Authority is determined by the executive.[[7]](#footnote-7) A quick review of the PTA establishing POTRAZ evidences an executive driven authority. This undermines functional and operational independence. Section 4(3) of the PTA is verbatim s 8 (2) of the Bill. Despite this intent there are several provisions in the PTA that gives the minister powers to interfere; s 25 (1), minister issues policy directions on national interest, which the Board shall take all necessary measures to comply with, s 25 (3); s 26 (1)-(2), minister may direct Board to reverse, suspend or rescind its decisions or actions, after the minister consultations with President, that Board decision was not in the “national or public interest or the interests of consumers or licensees.” The PTA establishing POTRAZ as the Authority is littered with provisions obliterating functional and operational independence.

For regional experiences, Kenya and South Africa’s data laws are persuasive on how to appoint a DPA. Comparative jurisdictions have separate data commissioner (Kenya) or information regulator (South Africa). The appointments involve Parliament, through nomination and interviews, and or ratification of the final candidate submitted for executive nomination. These are public processes building data subjects’ confidence.

In Kenya, the data commissioner is appointed after a public process, that includes open and transparent interviews led by the Public Service Commission (s 6(1)-(3)). A list of the final three are sent to the President in order of merit. Section 6(4) the President shall nominate from the list and, with approval of the National Assembly, appoint the Data Commissioner. The appointment will be for a 6-year non-renewable term and the qualifications are clearly listed.[[8]](#footnote-8) The data commissioner is an independent office, and reports to the National Assembly annually through the relevant ministry (s70 (1)-(3)). Procedure for removal from office is clearly stipulated including failure to abide by requirements of leadership integrity[[9]](#footnote-9) and is an independent office under the constitution.[[10]](#footnote-10)

South Africa has an information regulator established under s39 of the Protection of Personal Information Act (POPI Act). The information regulator is an independent office, subject to the constitution and reports to the National Assembly. Section 41 details the appointment, qualifications and removal of the information regulator. The information regulator consists of a chairperson and four other members. At least one member must be a practising advocate or attorney or a professor of law at a university; and the remainder of possess any other “qualifications, expertise and experience relating to the objects of the Regulator”. The term of office is five years with reappointment eligibility. Removal for misconduct, incompetence or incapacity is the President acting upon successful motions moved in National Assembly.

***Recommendation***: POTRAZ is accumulating unfettered powers with no oversight mechanisms. The DPA functions should be resident in a new and independent institution, and a statutory commission. The Bill should provide for an independent DPA, accountable to Parliament. The appointment processes must be publicly conducted to instill confidence and legitimacy. It is possible that arguments on the availability of resources for such an initiative might be raised. However additional institutions are being created such as the Public Protector under Constitution Amendment Bill number 2 whose functions can easily include data protection and handling of complaints from public.

The Authority will be providing advice on constitutional matters, that is matters relating to the right to privacy and access to information. In its current composition POTRAZ is not suited for any of these purposes. The POTRAZ Board has diverse but not appropriate skills set for conducting policy advise and oversight on issues such as right to privacy and access to information. The technical staff working on data protection should also be recruited in open public processes.

## Part IV and Part V

1. **Data Quality and Principle of Data Protection and Privacy**

***Issue***: quality of data, principles of data protection

***Discussion***: Part IV, section 9 (1)(a)-(c), summarizes the data protection principles applicable to a data controller. Unfortunately, to make this short and precise, the Bill leaves out critical aspects or has them scattered in other sections, including Part V, sections 10 and 11, making the Bill a complicated read. Kenya, Uganda, and South Africa incorporate principles of processing of data clearly in their laws borrowing from the European Union General Data Protection Regulation (GDPR).

Article 5 of GDPR lays out the principles as follows

* lawfulness, fairness and transparency;
* purpose limitation;
* data minimisation;
* accuracy;
* storage limitation;
* integrity and confidentiality;
* accountability.

Lawfulness, fairness and transparency require data processing to be for lawful purposes, and just and equitable. Section 10 of the Bill addresses lawful processing. Lawfulness is satisfied if consent for processing is granted and considered legitimate. Consent is freely given, in clear terms, and can be withdrawn, see analysis Part I of the Bill. Transparency requires that data subjects (natural persons) be consulted on data to be collected or used including when it is collected through means such as webcrawling.

Data controllers or processors should provide information to data subjects in easily understood language. The language must be plain and simple. The records must be in accessible formats. Purpose limitation should be clear, meaning that it should be "specified, explicit and legitimate purposes”. The Bill in Part V section 11 addresses purpose limitation. The purpose limitation is agreed before data is collected and is enforced throughout data lifecycle.

Data minimization means the personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[[11]](#footnote-11) Data should be kept "accurate and, where necessary, kept up to date" as under section 9 (1)(b) of the Bill. Storage limitation is under s 9(1)(c), retained in a form that allows for the identification of data subjects, for no longer than necessary[[12]](#footnote-12) with a view to the purposes for which the data is collected or further processed. Integrity and confidentiality of data is paramount, including guarding against unauthorized, unlawful processing, accidental loss, destruction using appropriate standards.[[13]](#footnote-13)

Accountability as a principle is covered under Part VI s 24 (1)(a)-(b) of the Bill. Basically, this provision, though further in the Bill is essential to placing the burden of compliance with data protection principles on the controller. The data subject is therefore not required to prove that data protection rights, privacy have been infringed, the data controller must prove that they have been respected and enforced.

Kenya and Uganda Acts under sections 25 (a)-(h), and sections 3(1)(a)-(g)[[14]](#footnote-14), respectively, incorporates the GDPR principles with a few modifications and additions. Kenya adds (h) that the data should not be “transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject”.

***Recommendation***: Part IV should clearly spell out the principles of data protection, and that these are applicable to the data controller, and any other person in their control or authority including data processor. These principles can be further expanded in the Bill as it relates to aspects of processing data for instance, on issues of consent, processing of sensitive data and automated processing of data. These principles can be placed before the functions or designation of the DPA/Authority as they constitute the foundation of DPA/Authority’s function and mandate. The current drafting makes data subject rights afterthoughts and hidden in the Bill’s text.

1. **Processing of non-sensitive data**
2. ***Issue***: processing of non-sensitive data

***Discussion***: Section 12 (3) allows for processing of non-sensitive data without the consent of the data subject in certain circumstances. Section 12(3)(d) indicates such sensitive data can processed without consent, for purposes of “performing a task carried out in the public interest…” and (e) “promoting the legitimate interests of the controller or a third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject claiming protection under this Act”.

A few issues to consider with s 12(3)(d) and (e) as currently framed. First, public interest has attracted a wide definition and application. Absence of a definition of public interest removes clarity and lends itself to broad interpretation, if not abuse. Authorities should not be given this wide latitude to process non-sensitive data without sufficient guard rails.

***Recommendation***: Section 12 (3)(d) should list the specific issues that constitute or qualify as public interest. For s 12(3)(e), the drafters should provide guidance on interpretation and application to remove any prejudice or harm being suffered by the data subject if there is doubt in balancing interests. Section 12(4) stipulates that conditions indicating satisfaction with subsection (3) may be outlined. This is not enough. The data controller and processor have onus of proving that their actions are for the protection of personal data and privacy. The conditions must be outlined in the regulations and codes of conduct to avoid abuse and inconsistent interpretation.

1. ***Issue***: Sensitive data under s 13 (1)(a)-(b) should be processed under conditions of consent in writing which can be withdrawn, at any time.

***Discussion***: Section 13 (2) has several exceptions to consent which presents difficulties as discussed below. Of note is s 13 (2) (b), (d), and (f) which focus on vital interests of the data subject or another person, national security and data in public domain respectively. Section 13 (2)(a) speaks of specific rights of the controller in the field of unemployment law”, this is potentially misleading. Vital interests of data subject or another person is considerably a wide framing and can be abused, especially in the absence of guidelines.

The use of wide exemptions that cover “national security” or “public order” is problematic, hence not recommended. History has shown that such framing lends itself to abuse. When the exemptions are applied they must be justifiable and necessary. The Bill suggests that since data is already in the public domain it is subject to processing without the data subjects’ consent. This has grave implications. First, the data subject might have placed it in the public domain for a specific purpose that it had been processed for. Now that the data is a public record or in the public domain even with the consent of the data subject does not extend to further processing of any kind. A data controller in the employment field or law does not have rights as they relate to the data, they have duties and legal obligations. Rights are for the natural person whose data is being processed. The section might be intending to address the legal obligations of the data controller in the employment law, this should be stated as such.

1. ***Issue***: processing of genetic data, biometric sensitive data and health data under s14

***Discussion***: Section 14 (3) has exemptions to consent on processing of genetic, biometric sensitive and health data similar to s 13 above. Section 14 (3) (a) exempts consent in writing if processing is in compliance with national security laws or (d) processing is required by or by virtue of law or any equivalent legislative act for reasons of substantial public interest or (e), processing is necessary to protect vital interests of the data subject, or another person (g) data relates to data made public by the data subject.

***Recommendation***: To constitute a legitimate and justifiable exemption this provision must be expanded to indicate that the exemption is clearly defined and prescribed by law; they should be legitimate as they advance or respect individual rights and freedoms under the constitution and the Bill and necessary, proportionate in a democratic state. Equally substantial public interest should be considered as such if lawful if processing is proportionate and there are sufficient safeguards for data protection and privacy.

The data that is publicly available due to the data subject’s act must be protected from further processing of any other purposes other than the intended purposes it had been collected or made public for. Public availability should not be assumed as consent, neither does this constitute legal grounds for additional processing of the data. The processing of data subject’s data to protect interests of another person should be clearly framed to indicate that “another person” is a natural identifiable person and not juristic persons. This will eliminate or mitigate against abuse. Vital interests of another person should be clearly defined as those that constitute existential needs and interests. If also there is knowledge that the data subject even if the vital interests existed would not have consent to the processing of the data, then such processing should be deemed unlawful.

## Part VI

Part VI of this Bill covers sections 15, which focuses on disclosures when collecting data directly from data subject, 16 on disclosures when not collecting data directly from data subject, 17 on authority to process, 18 security; 19 on security breach notification; 20 Obligation of notification to Authority; 21 content of notification; 22 authorization, 23, openness of processing and 24 accountability.

1. **Disclosures, Notification, Openness of Processing and Accountability**
2. **Indirect Data collection**

***Issue***: disclosures when collecting data directly from data subject[[15]](#footnote-15)

***Discussion***: Section 15 (e)(i) and section 16 (e) (ii) provides for the data to be disclosed to “recipients or categories of recipients of the data”. It presupposes some level of sharing of personal data with other recipients, and categories not stated. Further, the provision does not specify if the recipients have safeguards or are cross border recipients. Section 15 (1)(c), (e)(iii) and s 16 (e)(iii) provides for data subject right to access and rectify data. This is commendable and necessary but not sufficient as will be discussed under section on data subject rights.

***Recommendations***: These provisions must consider inclusion of section on sharing of data and if the data will be shared or legitimately disclosed to another recipient, the section should provide for the data subject to be informed when personal data are first disclosed to the recipient.

1. **Security of Data**

***Issues***: security of data, section 18 provides for security, integrity and confidentiality of data by the controller, or data processor representative

***Discussion***: The controller’s duties include the obligation to safeguard the security, integrity and confidentiality of data from unauthorized access, negligent loss, alternative or any unauthorized processing. This provision is commendable. Data controllers should put in place mechanisms to reduce the risk of violation of data integrity, confidentiality and security. The risks to the data subject are quite wide and the controller needs to prepare or anticipate some of these risks. These include economic or social risks, such as fraud, financial loss, or reputational damage due to disclosure of personal data

***Recommendations***: The Bill should consider including these duties as part of principles on data protection, and then expanding them in the Bill.

1. **Notifications to Authority**

***Issue*:** Notifications to Authority under section 19 provides that “the data controller shall notify the Authority, without any undue delay of any”

***Discussion*:** The section is short. There is no specification of when notification should be conducted other than undue delay. Undue delay, meaning within what period, after discovery of the breach, this is not clear from the Bill.

***Recommendation*:** The Bill must expand on the notification requirements by the data controller to the Authority, including the nature of notification, the time allowed after breach is discovered to notify the Authority. This cannot be more than 72 hours, unless reasons for further delay are provided. If the drafters are concerned with a voluminous Bill, these clarifications must be included in regulations. Otherwise as currently framed s19 is insufficient to allow the Authority to exercise oversight on data controllers, and or processors. Notification guidelines or regulations should specify a) nature of the personal data breach, number of data subjects affected, categories of data breached; b) include contact persons or details for data protection officer; c) likely impact of the data breach; and d) measures taken by controller.[[16]](#footnote-16)

1. **Notification of Data Subject**

***Issue***: Notification to Data Subject

***Discussion***: The Bill is silent on notification of breach to data subjects.[[17]](#footnote-17)

***Recommendation*:** A reading of the Bill there is no provision allowing for communicating to the data subject of the developments or breach. A data subject should be notified of data breach and it shall be in plain and clear language. Lack of notification of data subjects means that they are not able to seek redress or mitigate harm. Even if the information was encrypted or under storage capability that limits exposure, notification to the data subject is right, and not a privilege. South Africa’s POPI Act, s22 provides that notification shall be in writing and communicated through mail, sent by email, or placed in prominent position on the website of responsible party, or published in the news. Uganda has similar provisions.[[18]](#footnote-18) Notification can only be waived if the identity of such data subject cannot be established or if the notification constitutes a disproportionate effort[[19]](#footnote-19) as defined under the Bill.

1. **Obligation of notification, data protection officer appointment**

***Issue***: obligation of notification to authority, focusing on automated operation or set of operations, appointment of data protection officer (DPOs)

***Discussion***: the section introduces a new term: automated operation in addition to automated processing. The section is convoluted, and easily creates confusion of its intended objective. Notification for processing of data is also exempted if “there is no apparent risk of infringement of the data subject’s rights and freedoms” or the data controller has appointed a data protection officer. This is the first time a data protection officer is introduced in the Bill, in the middle of notification issue, which is the responsibility of a data controller, and or processor. Even though the DPO under the Bill is charged by the controller “with ensuring, in an independent manner, compliance with the obligations provided for in this Act” there are no detailed provisions of her or his responsibilities other than leaving that for guidelines to expand.

***Recommendation***: The Bill should use consistent terms throughout unless if automated operation or set of operations is defined to mean something different from automated processing which the Bill uses on several instances. The DPO appointments and functions require development as much as is possible in the Bill, or immediately after enactment but before commencement to allow institutions to comply if they need to appoint DPOs. There is no clarity on when a DPO is required or not.

1. **Content of notification and authorization**

***Issue***: content notification requirements and impact assessment, authorization

***Discussion***: this section provides for how the notification under s 20 should be conducted. The section is elaborate and exhaustive. A few issues to note: s 21(k) provides for a preliminary assessment of whether security measures are provided for and are adequate for automated processing of data. Section 21(3) provides that inspection should be conducted if data controller “is of the opinion that there are risks to the privacy rights of data subjects”. The inspection should be prior to the commencement of the processing or transfer. Section 20 also briefly mentions data retention.

The Bill does not outline the criteria to be used to decide to conduct an inspection and assessment of security systems other than it being the opinion that specific risks to privacy rights exists.[[20]](#footnote-20) The fact that s 22 allows the Authority to establish categories of data which requires specific processing based on risks to fundamental rights of data subjects is not sufficient. Categories of data do not address the discretion to conduct or not to conduct an assessment and inspection. The significantly wide discretion to the data controller leaves this to a reasonable person test on whether in that person’s opinion risks existed or not. Section 22, allows the Authority to establish categories of data which requires specific processing based on risks to data subjects’ fundamental rights.

***Recommendation***: An inspection and assessment[[21]](#footnote-21) should ideally be conducted before processing. The Bill should make specific provisions for data impact assessments/inspections, including requirements of notification to data subject which must be concise, and in clear, simple language. The Bill must provide for guidelines for data processors on what would result in data protection assessments and inspection. The criteria should include possible profiling, large volumes of data, merging of different data gathered by different processes, use of newer technologies or possible data transfer to countries.

Data retention periods are not clearly stipulated in the Bill.[[22]](#footnote-22) There are other laws which allow retention of data for instance in the telecommunications field in respect of traffic data, or subscriber information. This data is regulated under a different regulation and instrument. The application of the Bill in such matters must be clarified.[[23]](#footnote-23)

1. ***Openness of processing and accountability***

***Issue***: openness of processing by Authority and, accountability of data controller

***Discussion***: Section 23 provides for openness of processing of data. This provision is commendable as it advances openness and transparency of the Authority’s data processing activities. Section 24 provides for accountability of data controller in complying with the principles in the Bill.

***Recommendation***: the maintenance of register ideally should be included in the data protection principles and the functions of the Authority. The register should not be left to the last sections of the Bill. The level of openness must be manifest throughout the Bill. All registered data controllers should be kept in a register open for public inspection. Accountability must be listed as one of the duties that data controllers are required to comply with. An accountability principle should be included in the Bill, for the Authority and data controllers.

## Part VII

Section 25 covers data subject rights on automated data processing, s 26 on representation of data subject who is a child, and s 27 on legally incapacitated data subjects.

1. ***Data subjects***

***Issue***: rights of data subjects are contained in various sections of the Bill

***Discussion***: The Bill provides for various rights for data subjects in different parts of the Bill. This is commendable but not sufficient. Sections with data subject rights include ss9(1)(b), 15(1)(c), 15 (e)(iii), and 16(1)(d) providing for right to object, right to access and rectify.

The Bill will benefit from listing all the data subject rights separately and then reinforcing them with specific sections on their application. These rights, based on international practices[[24]](#footnote-24) and standards include the following:

* The data subject’s right of access
* The data subject’s right to rectification.
* The right to erasure or right to be forgotten
* The right to data portability.[[25]](#footnote-25)
* The data subject right not to be subject to a decision based solely on automated processing,

The data subject rights include the right to be notified when there is a breach, or the personal information and data is compromised, or accessed by unauthorized means. The Bill does not provide for this right as discussed above. The data subject has a right to know at no cost and even to access the record or copy of the information held. Data subjects have the right to object to the processing of data and not to be subjected to direct marketing. These are not absolute rights, and the Bill should clearly outline the limitations as justifiable, necessary, and proportionate.

## Part IX

1. ***Codes of Conduct***

The Bill needs to expand on the duties of the data controller and data processors which are appear in different sections of the Bill. Compliance with the Bill becomes complicated for data controllers and processors who might have limited capacities and skills. If Bill is enacted in its current state, the Authority should develop very user-friendly guidelines to allow compliance for data processors and controllers who have a duty to meet obligations that advance data subject’s rights.

Codes of conduct are useful in providing guidelines on how the controller and processors can regulate their behavior. Codes of conduct are necessary accountability tools. Ordinarily, codes if adopted through and by certain trade associations are mandatory in guiding the practice of a profession. The Authority should use these tools for accountability and provide operational application to complicated Bill provisions.

Codes will contain what is legally and ethically permissible. From the Bill, some of the code of conduct issues must include: fair and transparent processing; legitimate interests or purpose (s11); collection of personal data (s12); technical and organizational measures (s18(1)); breach notification and notification to data subject (s19); data transfers (s28-29) among others. Sectoral codes of conduct reduce compliance costs for controllers.

1. ***Transfer of Data across borders***

The connectedness of the world makes it impossible to ignore prospects of cross border transfers of data, from public and private sector. Organizations that use IT services, such as cloud storage services, for instance Econet-owned Liquid Telecom signed an agreement to invest $50 million to develop data centers and cloud services in Egypt [[26]](#footnote-26) or recruitment companies with remote access and global human resources databases will require to implement lawful data transfer mechanisms.

Section 28-29 provide for data transfer across borders. For transfers to occur, several requirements must be satisfied under s28, while s29 provides for exemptions which will be discussed below. Section 29(1)(d) allows for transfers without satisfaction or assurance of adequate level of protection in another place if “necessary or legally required on important public interest grounds”. Again, public interest grounds remain undefined in the Bill, making this susceptible to abuse.

Further s 29(1)(e), allows for transfer without adequate protection if this is necessary in order to protect the vital interests of the data subject. This drafting is also considerably wide on vital interests and the guidelines must outline this.

## Part X

1. ***Whistleblowing***

Section 31(1) of the Bill gives power to the Authority to establish rules giving the authorization and governing of the whistleblowing system. The rest of Section 31 sets out other considerations that must be taken into account in handling information received from a whistleblower and in conducting the subsequent investigation. Despite the length of the provision, this Section is thin on any protections guaranteed to whistleblowers – it actually does not offer any protections.

This pales in comparison to efforts in neighbouring South Africa to protect whistleblowers through the Protected Disclosures Act.[[27]](#footnote-27) It is unlikely that Regulations will be comprehensive enough to cover an area that countries such as South Africa, the United Kingdom[[28]](#footnote-28) and the United States of America[[29]](#footnote-29) have dedicated entire Acts to. This lack of actionable legislation to regulate whistleblowing is a cause for concern in a country such as Zimbabwe that is struggling with deep-rooted corruption in both the private and public sectors.

The recommendation here is that this Section be revised to set out guarantees of protection for whistleblowers as well as other concrete steps in the handling of investigations that result from whistleblower revelations.

## Part XII

1. ***Cybercrime provisions***

Cyber security and computer crime in Zimbabwe is currently regulated in terms of Chapter VIII of the Criminal Law Code. Part XII of the Bill seeks to amend the acts that are criminalized under this part of the Criminal Law Code.

Part XII is divided into three categories; the first contains a list of definitions relating to the use of computers, the information on them and other related terms, the second category contains a list of criminal activities relating to computer systems and the third category relates to offences relating to electronic communications.

The list of definitions contained under Part XII is fairly easy to understand however, there is a worrisome inclusion of the term “**remote forensic tool**.” In this Bill, the remote forensic tool is defined as “*an investigative tool including, software or hardware, installed on or in relation to a computer system or part of a computer system and used to perform tasks that include keystroke logging or transmission of an IP-address.”*

This is problematic for several reasons; the use of the word “forensic” gives the impression that this is an investigative tool used to investigate events after the commission of an offence. The definition shows that the tool is actually used before the commission of a crime; it is a data collection tool that collects which includes keystroke logs through software or hardware that is remotely installed on a target’s electronic device.

Keystroke loggers are in actual fact privacy breaching tools that collect all the information inputted into a device such as a computer by recording every key typed in, the sequence the keys are typed in as well as recording every mouse click. When these key strokes and mouse clicks are matched to websites visited, it becomes easy to collect sensitive information such as log in details, passwords, banking information and other forms of sensitive information that is not related to the investigation or crime.

Furthermore, neither the Bill nor the Criminal Law Code that it seeks to amend contain any judicial oversight on the use of such far-reaching technologies. There is no procedure at all relating to how this technology may be used and which state security agents may use it. The lack of any boundary setting provisions within which this technology may be used is shocking and reckless. The term remote forensic tool is derived from the SADC Model Law on Cyber Crime and Computer Crime.

Sections 163 to 163F contain definitions and set out computer related crimes such as hacking, the use of viruses and malware to unlawfully interrupt with computer data and the proper functioning of computer systems. It is important to note that Section 163 of the Bill decriminalizes ethical or white hat hacking, that is, the authorized hacking of an information or computer system for finding any security vulnerabilities. Unauthorized hacking of information or computer system is criminalized.

Section 164E of the Bill seeks to criminalize the transmission of intimate images without consent. Revenge porn remains a challenge in Zimbabwe where it is commonplace. The offence now carries a fine and or custodial sentence of up to 5 years.

The amendments contained in the Bill that are a major cause for concern for freedom of expression advocates relate to the offences relating to electronic communications and materials. Zimbabwe has long been plagued by laws that unjustifiably seek to limit free expression and this Bill reemphasizes some of those problematic laws.

Section 164 criminalizes the sending of messages that incite violence or damage to property. In the past, this charge has been used to prosecute organizers of peaceful protests and other forms of public disobedience. The same goes for sections 164A and 164B that criminalize the sending of threatening messages and cyber-bullying and harassment respectively.

This is not to say that these are useless or unnecessary provisions however, the way these Sections are widely worded makes it easy for the State and any of its security agencies to target and persecute individuals in the name of investigating crime in terms of this cyber law. The same criticism applies to Section 164C which relates to the transmission of false data messages. This provision is similar to the scandalous provisions found in the outgoing AIPPA as well as the Criminal Law Code which were specifically aimed at silencing the Zimbabwean media and any other dissenting voices that dared criticize government.

It is strongly recommended that these Sections relating to electronic communications be thoroughly revised to bring them into line with the constitutional provisions relating to free speech, media freedom as well as case law that criticized and in some instances struck down[[30]](#footnote-30) similarly worded provisions in AIPPA and the Criminal Law Code.

# CONCLUDING RECOMMENDATIONS

***Definitions***

Critical definitions and terms that are required for enhanced privacy and data protection are missing. These include anonymization or pseudonymization. Anonymization is modification of personal data resulting in no connection of data with an individual.[[31]](#footnote-31) Admittedly, the bar for implementation is high, for anonymization but necessary that it is included in the Bill.

Article 4(5) of the GDPR defines pseudonymization as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.” Once the data is pseudonymous, it is possible to use that data for other purposes. The data should not be capable of re-identification which is a risk for users.[[32]](#footnote-32) This might be necessary for research purposes, provision of public services or other public goods without breaching data subject rights. The use of anonymization and pseudonymization enables stronger privacy protection and safeguards. These standards can be used for data not necessary to be retained, and if a breach occurs, reduced harm will be suffered.[[33]](#footnote-33)

Kenya Data Protection Act defines "anonymization" as the removal of personal identifiers from personal data so that the data subject is no longer identifiable. South Africa uses ‘‘de-identification’’ and “re-identification” as concepts for removal personal identification information and the ability to reintroduce them again making it possible to identify the data subject. South Africa uses de-identification as deleting any information that—(a) identifies the data subject; can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

***Other Data Related Laws***

The Bill has implications for other laws and policies that relates to different industries or areas that have in the past processed or continue to process data. Parliament must conduct a legal analysis of some of the laws that will be impacted by this Bill. For example, National Registry laws that relate to national identity management, registration or in the financial instruments such as the Banking Act or credit bureau policies are relevant or Health related laws for medical and insurance sectors. The proposed Bill has significant implications for public and private actors. Compliance costs and processes will be considerably expensive, for human resources, technical capacities. Public and private institutions will require significant time to comply with this Bill.

***General Presentation***

The Bill is drafted in a very complicated manner. Several sections could benefit from simplification and clearer drafting and language. The law is supposed to be accessible, readable and easily understood, especially if it contains fundamental rights and freedoms. Unfortunately, this Bill read against comparative laws in the region, and beyond is drafted in a confusing and tortuous manner. The drafters’ intention will evade the legislators. For example the Bill’s application under s 4 (2) is drafted in a complicated manner. It will benefit from redrafting, and simplification. It could read “a data controller who (i) is established or ordinarily resident in Zimbabwe and processes personal data while in Zimbabwe; or (ii) not established or ordinarily resident in Zimbabwe, but processing personal data of data subjects located in Zimbabwe”. Clear provisions make compliance easier.

***Transition and Commencement***

The Bill should clearly state the transition period and not leave the commencement date being set through gazetting. A longer transition period will enable compliance to be achieved. Arguments are that there will be a vacuum again if there are delays. This is not necessarily the case. If the Bill continues as an omnibus, then sections on cybercrimes can come into effect immediately upon gazetting, as they are amending an existing law. The newer provisions of data protection should be accorded an additional 6-12 months before commencement. This will allow the Authority to be established, rules and regulations developed, and public and private institutions to regularize their affairs. The relevant ministry working with stakeholders must conduct a regulatory impact assessment and appreciate the actual cost for compliance.

1. In February 2019 Cabinet approved the repeal of AIPPA and its replacement with [↑](#footnote-ref-1)
2. Justice A Mavedzenge, Accessing the National Voters’ roll through the Right of access to information in Zimbabwe, Zimbabwe Rule of Law Journal Volume 1, Issue 1 February 2017 [↑](#footnote-ref-2)
3. Kenya Data Protection Act (2019) "consent" means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject. South Africa Protection of Personal Information Act (2013) ‘‘consent’’ means any voluntary, specific and informed expression of will

   in terms of which permission is given for the processing of personal information [↑](#footnote-ref-3)
4. Commentary on Consent under the General Data Protection Regulation [↑](#footnote-ref-4)
5. Similar institutions locations are not known for instance the Monitoring and Interception Communications Centre under the Interception of Communications Act (ICA). [↑](#footnote-ref-5)
6. Oversight of money transmission providers and mobile banking providers now obtain recognition of their payment system in terms of section 3(1) of the National Payment Systems Act [Chapter 24:23], in addition to the licensing provided under Postal and Telecommunications Act of the mobile network [↑](#footnote-ref-6)
7. Sections 6-7 of Postal and Telecommunications Act, POTRAZ is presided over by 5-7 members appointed by the President after consultation with the Minister. The Board in consultation with the Minister appoints a Director General, who is responsible for the day to day operations of the Authority. [↑](#footnote-ref-7)
8. Kenya Data Protection Act, Section 7 [↑](#footnote-ref-8)
9. Constitution of Kenya (2010) Chapter 6 on leadership integrity, [↑](#footnote-ref-9)
10. Constitution of Kenya (2010) section 260 of which Chapter Fifteen on Commissions and Independent Offices [↑](#footnote-ref-10)
11. Uganda Data Protection and Privacy Act section 14. Minimality. (1) A data controller or data processer shall only process the necessary or relevant personal data. (2) For the avoidance of doubt a data controller or data processer shall not process personal data which is in excess of the data which is authorised by law or required for a specific purpose. [↑](#footnote-ref-11)
12. Longer than necessary is also subjective, some Zimbabwe laws give time period for data retention [↑](#footnote-ref-12)
13. See section 18 under Part VI [↑](#footnote-ref-13)
14. Uganda Data Protection and Privacy Act section 3 (a) be accountable to the data subject for data collected, processed held or used; (b) collect and process data fairly and lawfully; (c) collect, process, use or hold adequate, relevant and not excessive or unnecessary personal data; (d) retain personal data for the period authorized by law or for which the data is required; (e) ensure quality of information collected, processed , used or held; (f) ensure transparency and participation of the data subject in the collection, processing, use and holding of the personal data; and (g) observe security safeguards in respect of the data. [↑](#footnote-ref-14)
15. This is similar to provisions of Article 13 of the GDPR though there are several aspects not included such as when information is likely to be shared across borders [↑](#footnote-ref-15)
16. See Article 33 of the GDPR [↑](#footnote-ref-16)
17. Section 21 (h) provides for data subject notification processing of automated data. [↑](#footnote-ref-17)
18. Uganda Data Protection and Privacy Act, section 23 (3) Where the Authority determines that the data collector, data processor or data controller should notify the data subject, the notification shall be made by- ( a) registered mail to the data subject's last known residential or postal address; (b) electronic mail to the data subject's last known electronic mail address; (c) placement in a prominent position on the website of the responsible party; or (d) publication in the mass media. [↑](#footnote-ref-18)
19. Disproportionate effort means effort that is so labour intensive as to consume a lot of time, money and manpower resources; [↑](#footnote-ref-19)
20. The DPA under s 8 on functions is empowered to conduct inquiries or investigations of its own accord or at the request of data subject [↑](#footnote-ref-20)
21. Statutory Instrument 142 of 2013, Postal and Telecommunications (Subscriber Registration) Regulations provide for "privacy impact form" means a form which evaluates an entire project from a privacy perspective and identifies risks and mitigation strategies throughout; [↑](#footnote-ref-21)
22. SI 142 of 2013, for example section 7(6) on Service Providers indicates that “service providers shall maintain subscriber information of customers with numbers or identities potted to other service providers for a period of 5 years”. [↑](#footnote-ref-22)
23. Laws which regulates the retention of electronic records or mobile subscribers’ details, or traffic data [↑](#footnote-ref-23)
24. See GDPR Article 15-22 [↑](#footnote-ref-24)
25. Kenya Data Protection Act section 38 (1) A data subject has the right to receive personal data concerning them in a structured, commonly used and machine-readable format. [↑](#footnote-ref-25)
26. <https://techcabal.com/2020/05/29/africas-cloud-computing-industry-is-set-to-grow-as-data-adoption-rises/> [↑](#footnote-ref-26)
27. Act no. 26 of 2000 [↑](#footnote-ref-27)
28. Public Interest Disclosure Act [↑](#footnote-ref-28)
29. Whistleblower Protection Act [↑](#footnote-ref-29)
30. CCZ 02-15 - Madanhire and Another V Attorney-General [↑](#footnote-ref-30)
31. This is done through randomization which is altering the accuracy of data in order to remove the strong link between the data and the individual. Generalization is also used to dilute the attributes of the data subjects by modifying the scale or order of the data, like region or town) [↑](#footnote-ref-31)
32. South Africa Protection of Personal Information Act defines ‘‘re-identify’’, in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that— (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject. [↑](#footnote-ref-32)
33. Kenya Data Protection Act, section 39 (2) “A data controller or data processor shall delete, erase, anonymize or pseudonymize personal data not necessary to be retained under sub-section (1) in a manner as may be specified at the expiry of the retention period” [↑](#footnote-ref-33)