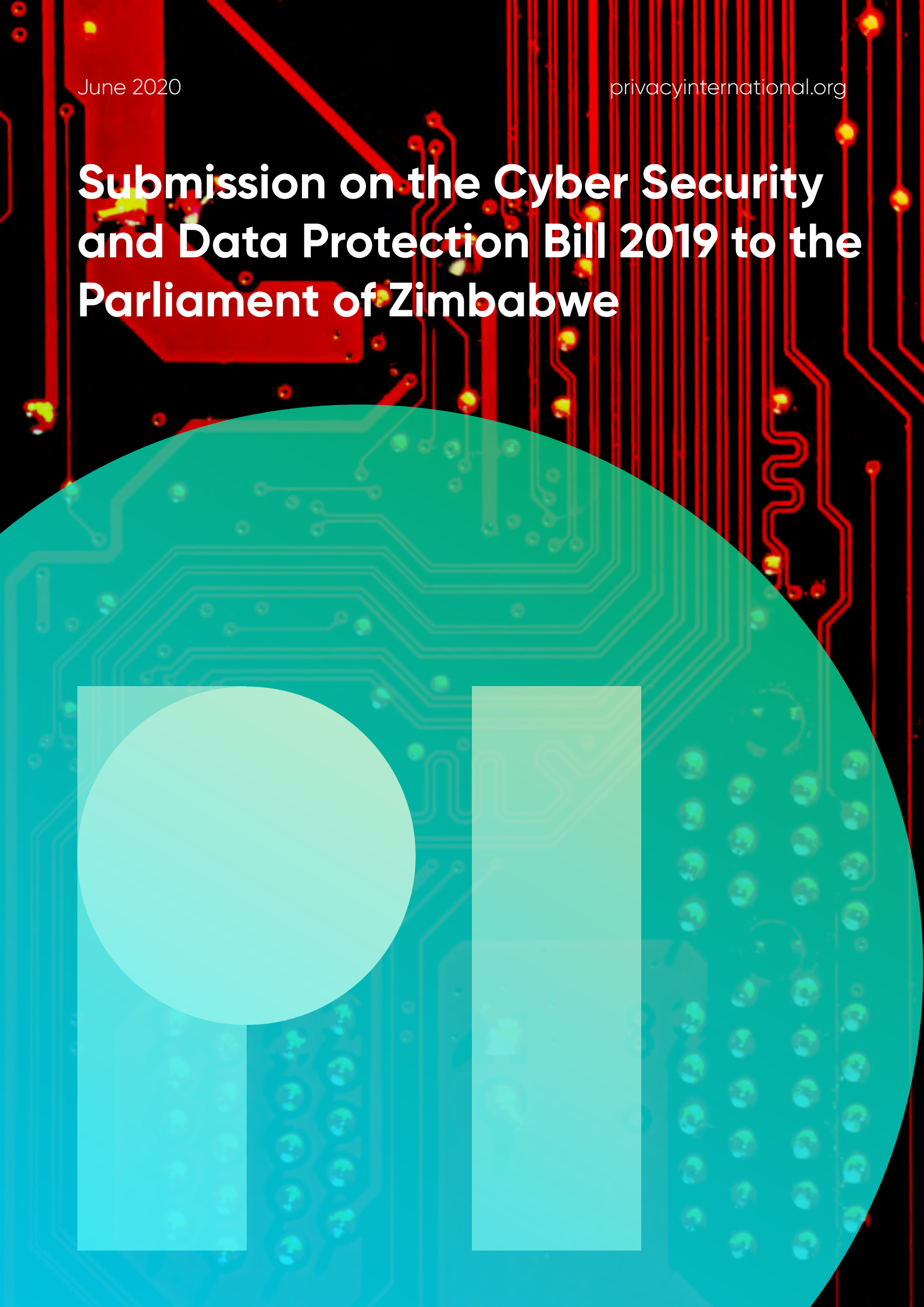
June 2020

privacyinternational.org

Submission on the Cyber Security and Data Protection Bill 2019 to the Parliament of Zimbabwe



About us

Privacy International (PI) is a non-governmental organization, which is dedicated to protecting the right to privacy around the world. PI is committed to ensuring that government surveillance complies with the rule of law and the international human rights framework. As part of this commitment, PI researches and investigates government surveillance to raise public awareness about technologies and laws that place privacy at risk. In this context the organization has been working on issues relating to identification systems, the collection, use and sharing of biometric data since its foundation.

PI takes this opportunity to congratulate Zimbabwe for taking a positive step towards the regulation of Data Protection and privacy by gazetting the Cyber Security and Data Protection Bill (House Bill 18 of 2019). PI welcomes this opportunity to provide input on this important Bill which deals with matters that fall squarely within PI's areas of interest and scope of work.

PI understands that the data protection aspects of this Bill will replace the privacy provisions currently contained in the outgoing Access to Information and Protection of Privacy Act of 2001. While the cyber security aspects of the Bill will amend the sections of the country's Criminal Law (Codification and Reform) Act that apply to computer crimes.

This brief provides a summary overview of the Bill and points out some of its positive and negative aspects. The brief concludes by giving recommendations on how to bring the Bill more fully in line with Zimbabwe's Constitution and internationally recognised data protection standards.

Whist the Bill provides for most of data principles, obligations and rights of data subjects, the Bill proposed has a number of significant shortcomings which means the law does not meet international standards in protecting personal data and risks undermining the purpose and scope of the law. We recommend that full consideration be given to the areas of concern and improvements outlined below under each Part of the Bill, and be rectified to bring the law into alignment with Zimbabwe's national and international obligations.

Contact

Kuda Hove
Policy Officer, Privacy International
kudah@privacyinternational.org

Alexandrine Pirlot de Corbion
Director of Strategy, Privacy International
alex@privacyinternational.org

Part I Preliminary

Object

The object of the law presented **in Section 2** is weak and has a long way to go in fulfilling the objective of data protection - to protect people. It is good practice that this section of the law would make direct reference to fundamental rights and international human rights obligations, and the State's responsibilities under national and international law, and explicitly confirm that this law would comply with these in its scope and application.

Interpretation

The following definitions listed under **Section 3** of the Bill are inadequate:
- "*Data controller*" - It should not be restricted to "licensable by the Authority" - it should be any "natural or legal person, public or private, that, by itself or in association with others, decides the purposes and means of the processing of personal data."
- *"Personal data"* - the definition here should emphasise that it is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier."
- *"Critical data"* - this term is used in the Bill but it is not defined.

Application

Section 4 attempts to define the scope of application of the law but it remains vague. Section 4(2)(a) refers to "effective and actual activities of any data controller" but does not define what these are. Section 4(2)(b) refers to states the Act applies to *"a controller who is not permanently established in Zimbabwe"* but does not define what that means.

Part III Data Protection Authority

Designation of Postal and Telecommunications Regulatory Authority as Data Protection Authority.

Section 7 of the Bill proposes the establishment of the Data Protection Authority (DPA)., and while we welcome the recognition of the government of the need to establish a DPA in Zimbabwe, the choice to assign DPA functions to the national telecommunications regulator is troublesome. The Data Protection Authority is an additional function that will be assigned to the existing Postal and Telecommunications and Regulatory Authority of Zimbabwe.

We are concerned that POTRAZ has been assigned with this mandate given that it is not an independent authority. In the past, POTRAZ has failed to make any firm rulings on alleged price fixing by the three Mobile Network Operators with a presence in Zimbabwe.
Mobile Network Operators and Internet Service Providers contribute a portion of their annual incomes to POTRAZ. This gives POTRAZ a vested interest in the profitability of these entities,

raising doubts about how motivated POTRAZ would be in making positive data protection and privacy rulings that ultimately affect the MNOs and ISPs profitability.

The overall effect of these assignments will lead an unnecessary concentration of power in a single entity that is wholly controlled by government, and therefore the law would fail to establish an independent authority to oversee the implementation of the law.

Furthermore, Part III of the Bill provides very little information on how the Authority would be set-up and operate in terms of its composition and structure, i.e. will a separate office be set-up in the POTRAZ, and the resources to be allocated to the mandate and functions of the authority.

While we welcome the inclusion of the role of the Authority to advise on matters relating to privacy and freedom of information as well as to conduct research on policy and legal matters, we strongly encourage that this role not be limited to the Authority working together with the responsible Minister but to a wider set of stakeholders including other relevant government bodies as well as public bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regards to the processing of persons' personal data.

This reaffirms the importance of the independence and autonomy of the Authority, which would not currently be the case as per this Bill, to ensure that it is in a position to effectively and independently undertake this advisory role.

Functions of Data Protection Authority

Whilst we welcome the power of the Authority to process complaints from data subjects as well as to conduct inquiries or investigations on its own accord, **Section 8** fails to outline the power of the Authority to impose sanctions. The independent Authority must have the power to impose appropriate penalties, including fines, enforcement notices, undertakings, and prosecution.

This process of sanction should not depend on submission of the complaint by a data subject but can be imposed pro-actively by the independent data protection authority as well as in response to complaints by civil society organisations. There is need for collective redress for damages arising from the violation of the misuse of data. Furthermore, the Bill in its current state is silent on the issue of data subjects getting compensation for material and non-material damage arising from the misuse of their data.

The access to an effective and independent Authority is an important component of the right of data subjects to effective remedy against a data controller and/or data processor, where they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law. The inclusion of this power under this Section is coherent and would align itself with the various provision sunder Section 33 "Offences and Penalties".

Part IV Quality of data and Part V General Rules on the Processing of data

Across Part IV Quality of data and Part V General Rules on the Processing of data under Sections 9 to 11, and 24, the Bill uphold international recognised principles of data protection.

Non-sensitive personal data

Section 12(2) is widely worded to insinuate that in some instances the data subject's consent to have their personal information processed may be implied and not expressly stated by the data subject. This sets a dangerous precedent that has no place in a data protection law. As noted in the definition of 'consent' provided for in Section 3 consent must be an "unequivocal, freely given, informed expression of will".

Similarly, **Section 12(3)** outlines that the processing of non-sensitive personal is permitted, without the consent of the data subject, when necessary for a variety of listed purposes. These exemptions are overly broad. In the way it is currently worded it would allow the processing of non-sensitive personal data for a broad range of purposes without consent. This provision fails to ensure consideration of the rights of data principals and is open to abuse.

In particular, we are concerned by the following:
- **Subsection (12)(3)(d):** It is unclear what is meant by *"public interest"*. The term is not defined in the Bill and the Bill does not refer to the definition of "public interest" which could be provided for in other laws in Zimbabwe. The current wording is open to abuse. Also, "public interest" needs to be assessed in relations to the interests, rights or freedoms of the individual.
- **Subsection (12)(3)(e):** It is unclear what is meant by *"legitimate interest"* of the controller or a third party. The term is not defined in the Bill and the Bill does not refer to the definition of *"legitimate interest"* which could be provided for in other laws in Zimbabwe. The current wording is open to abuse.
- **Subsection (12)(4):** The Data Protection Authority should have the discretion to define the circumstances in which the condition stipulated under subsection (3)(e) are considered as having been met. This is especially concerning given the lack of independence of the appointed Authority from the Executive arm of government.

Sensitive information

Section 13 states that sensitive information may only be processed with the relevant data subject's written consent. This consent may be withdrawn at any time, the data subject does not have to provide any reasons when doing so.

The Authority's discretion under **Section 13(1)(c)** to lift the prohibition of processing sensitive personal data without the data subject's consent is concerning, and must be reviewed.

Various provision sunder **Sections 13(2)** need to be revised to minimise the use of overly broad language and terminology which may be used to unjustifiably process personal information without express consent including under **Section 13(2)(d)** relating to national

security, under **Section 13(2)(f)** relating to data made public by data subject, under **Section 13(2)(g)** relating to data processed for scientific research **and Section 13(2)(h)** by a law or any regulation for any other reason constituting substantial public interest. The processing of sensitive personal data without the consent of a data subject must be restricted and should not cause any prejudice.

Genetic data, biometric sensitive data and health data

According to **Section 14**, the data subject's written consent is also required to process that individual's genetic data, biometric sensitive data and health data.

Health-related data may only be processed under the responsibility of a health-care professional, except if the data subject has given his or her written consent or if the processing is necessary for the prevention of imminent danger or for the mitigation of a specific criminal offence. Health related data may only be collected from other sources where the data subject is incapable of providing the data.
Section 14(2), like Section 13(2) uses overly broad language and terminology which is not defined in the law and their use restricted including in the name of national security, for scientific research, and public interest. Furthermore, Section 14(2)(g) allows for the processing of genetic, biometric and health data without the consent of a data subject if the information "has apparently made been made public." The use of the word 'apparently' is not acceptable and fails to provide clarity. This leads to excessive exceptions for the need for consent for the processing of genetic, biometric and health data which should be subject to higher safeguards.

Part VI Duties of the data controller and data processor

The Bill provides that the data controller and data processor must disclose information to the data subject relating to the processing of the data subject's data. Such information includes the data controller's name and contact address, the purpose of the processing, existence of the data subject's right to object to the processing and the intended recipients of the processed data. These disclosures must be made even when the information being processed is not collected directly from the data subject to which it relates.

However, in addition to the concerns outlined below in relations to existing provisions under this part of the Bill, there are two other obligations which must be imposed on data controllers and processors:

1) Adopting data protection by design and by default
Data protection should be embedded into systems, projects and services from the beginning to ensure that by design and default they implement the data protection principles and safeguard individual rights. 'Data protection by design' which requires implementing appropriate technical and organisational measures which are designed to effectively implement data protection principles. 'Data protection by default' which requires implementing appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

2) Impact assessments

Data controllers and the data processors should undertake an impact assessment to be conducted prior to processing personal data. An impact assessment requires at minimum assessment of:

- the necessity and proportionality of the processing,
- the risks to individuals and,
- how these are to be addressed

Disclosures when processing data directly from the data subject

We welcome the inclusion of the right to information of data subject provided for in **Section 15.** However, some additional elements should be included including:

- the name and contact address of the data processor
- the legal basis for processing
- the period for which the data will be stored
- the source of the data
- the right to lodge a complaint with the data protection authority
- the existence of profiling, including legal basis, the significance and envisaged consequences of such processing on the data subject
- the existence of automated-decision making, and the very least a meaningful explanation of the logic involved, the significance and envisaged consequences of such processing on the data subject. This is particularly important to reinforce the right provided for in Section 25.

Authority to process

Section 17 is brief and remains vague. The Bill should clearly articulate the obligations of the data processor.

Security breach notification

Data controllers have an obligation under **Section 19** of the Bill to notify the DPA of any data breaches without undue delay. The Bill is silent on the specific timelines within which this breach notification must be made and the format in which the breach must be submitted to the DPA.

This Section is not complete and fails to provide sufficient guidance on what must occur should there be a security breach. This Section should outline more clearly the obligations of the data controllers and data processors to notify the supervisory authority and the data subject in case of a data breach within a reasonable time period to be defined by the law. For example, information provided for under Section 21 should be outlined here too.

It is recommended that there be clear timeline within which the data breach notifications must be given. A number of other jurisdictions have indicated that such notification must usually be given within a period of 72 hours.

Obligation of notification to Authority

Various of the exemptions provided for in **Section 20** are too broad. For example, subsection 20(3) fails to provide what sort of registry should be exempt from the obligation to notify an Authority that they are processing personal data of data subjects. Furthermore, exemptions of "public interest" are too vague and are subject to abuse if left undefined. We are also concerned by the discretion awarded to the Authority exempt certain categories from notification under this section given its lack of independence from the executive.

Part VII Data subject

A central component of any data protection law is the provision of the rights of *data subjects*. These rights should appear early in the law, as they should be seen as applying throughout, underpinning all provisions in the law. These rights impose positive obligations on data controllers and should be enforceable before an independent data protection authority and courts.

We welcome the reference to various rights under section 15 and 16 as well as other parts of the Bill. However, there are several rights missing for the current Bill which we would urge be added including:

The right to rectify, block or erasure: A data subject has the right to rectify and block (restrict) data processed about themselves to ensure the data is accurate, complete and kept up-to-date and that it is not used to make decisions about them when the accuracy is contested. An individual should have the right to demand that the data controller correct, update, or modify the data if it is inaccurate, erroneous, misleading, or incomplete. Individuals also have the right to 'block' or suppress processing of personal data in particular circumstances. Personal data can then be stored but not further processed until the issue is resolved

The right to data portability: Data subjects should have the right to request that personal data about themselves that is processed by the data controller be made available to them in a universally machine-readable format, and to have it transmitted to another service with the specific consent of that individual. This right is a step towards ensuring that the data subject is placed in a central position and has a full power over their personal data.

The right to an effective remedy: The law must include the right of an individual to an effective remedy against a data controller and/or data processor, where they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law. Whilst Section 8 of the Bill notes the function of the data protection authority to receive complaints from a data subject the law does explicitly provide for the right to an effective remedy. This reaffirms the need for the independent supervisory authority to have the power not only to receive complaints from data subjects, but it must be able to investigate them, and sanction the violator within their own scope of powers - or refer the case to a court. The law should also provide for the data subject to take action against a supervisory authority where they have failed to deal with their complaint. As well as the right to complain to a supervisory authority, individuals should also have access to an effective

judicial remedy via the courts. Individuals should be empowered to take action themselves, as well as instructing others (including NGOs) to take action on their behalf.

Right to compensation and liability: A person whose rights are found to have been violated should have a right to compensation for the damage suffered – material or non-material (e.g. distress). This underlines the need for robust enforcement models to be in place to ensure that any violation can be investigated and acted upon by a relevant authority. But as noted elsewhere in our submission, the Bill fails to provide **Section 8** fails to outline the power of the Authority to impose sanctions. The independent Authority must have the power to impose appropriate penalties, including fines, enforcement notices, undertakings, and prosecution.

Furthermore, whilst there are provided elsewhere in the law in particular Section 15 and Section 16, the following rights must also be listed under Part VII of the Bill:

- **The right to information:** Whilst this right is provided for in Section 15(1) and Section 16(1), it must also be provided under Part VII
- **The right to access** Whilst this right is provided for in Section 15(1)(e)(iii) and Section 16(1)(e)(iii), it must also be provided under Part VII
- **The right to object:** Whilst this right is provided for in Section 15 (1) (c)and Section 16(1)(c), it must also be provided under Part VII
- **The right to rectify:** Whilst this right is provided for in Section 15(1)(e)(iii) and Section 16(1)(e)(iii), it must also be provided under Part VII

Decision taken on basis of Automatic Data Processing

The potential harms from the automatic processing of information that enable for example, profiling are addressed in **Section 25** of the Bill even though the Bill does not define what profiling is. This Section states that a data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. The data subject may give consent to adhere to the decisions reached solely by the automatic processing of the data subject's information.

For profiling, it is important that a clear definition be provided in the Bill. Individuals must be aware when profiling will reveal sensitive personal data and that there are safeguards in place. Individuals' rights should also apply to the data that is inferred, predicted and derived as a result of profiling. Section 25 falls short of providing the necessary safeguards.

Part VIII Transborder flow

Sections 28 and 29 of the Bill relate to the transborder transfer of data to countries with an adequate level of data protection and countries without an adequate level of data protection respectively.

Transfer to a country outside the Republic of Zimbabwe which does not assure an adequate level of protection

We are concerned by the inclusion of **Section 29** in this law. This is because it permits the transfer of data to a country outside the Republic of Zimbabwe which does not assure an adequate level of protection. Personal data should not be transferred to a country which does not assure an adequate level of protection. This provision is particularly concerning given the reference to terms which are not defined in the law such as *"public interest"* and *"vital interest"*.

There are various reasons for data transfers to occur, which may be seen as being exempt from compliance with data protection as provided by law but irrespective of the exceptions deployed, these transfers need to be highly regulated and will require further guidance to ensure that they are not broadly interpreted or open to abuse, and are compliant with human rights standards. These exceptions must be narrowly framed and interpreted to ensure that such agreements do not result in the weakening of the data protection offered in the law.

Part IX General Provisions

Regulations

The discretionary powers awarded to the Minister in **Section 32** are too broad and vague. This section must be reviewed to ensure that the powers granted to the Ministry do not permit it to bypass the function and powers of the Authority nor effective parliamentary scrutiny. Clarity is necessary to explain the role and powers of the Authority in relations to this section which awards the Ministry.

Part XII Consequential Amendments

Amendment of Cap. 9:23.

The inclusion of **Section 164E** which seeks to criminalise the transmission of intimate images without consent is a positive step.

The major cause for concern under Part XII is the inclusion of the definition of *"remote forensic tool"* which may include keystroke logging hardware or software. A keystroke logger is software or hardware which records the keystrokes as they are inputted into a computer via the keyboard. Keystroke loggers are a serious threat to users because they enable the easy interception of data they input on their devices. This interception of information as it is entered through the keyboard makes it possible to intercept passwords, and other forms of confidential information.

The first issue with this is that there is no prescribed procedure in the Bill about the circumstances under which such privacy breaching tools may be deployed. Second, there is also no oversight, for example from the judiciary on how these intrusive technologies are

used. Less intrusive methods of gathering evidence must be used as a way to avoid the use of excessive investigative methods such as key stroke loggers.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org