



Zambia: Insights into the Data Protection Act 2021

May 2021

Introduction

The Zambian Constitution under article 17 provides for the right to privacy including the right not to be searched (person, home or property); not to have possessions seized; not to have information relating to family, health status and private affairs unlawfully required or revealed; and not to have communications infringed.

Due to the evolving nature of information and communication technology and the need to protect privacy of the individual, Zambia recently enacted the Data Protection Act, 2021 to provide for the use and protection of personal data and to regulate the collection, use, transmission, storage and processing of personal data.¹ The Act also establishes the Data Protection Commissioner and spells out its functions, provides for regulation of data collectors, processors, and controllers and provides for the rights of data subjects.

Below we highlight the key provisions of the Data Protection Act, 2021, particularly the pros and cons.

The Pros

The Data Protection Act is a sign of commitment by the government to implement **article 17** of the Constitution which provides for the right to privacy. Enacting the law places Zambia among the few but growing number of African countries with a specific law on protecting individual data privacy. The scope of application of the Act is exhaustive and, per **section 3(1)**, the Act applies to the processing of personal data performed wholly or partly by automated means and to any processing otherwise than by electronic means.

The principles and rules related to processing personal data laid down in **section 12** highly reflect the internationally acceptable data protection standards as encapsulated in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,² and Europe's General Data Protection Regulation (GDPR).³ If rightly employed, these principles will enhance individuals' data protection and promote the right to privacy.


Section 13 introduces a fundamental principle in regard to processing of personal data by the data controller. **Section 13(b)(v)** provides that a data controller may process data "for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." This provision limits processing of data when such processing will fundamentally affect other rights and freedoms.

¹ *The Data Protection Act, No. 3 of 2021,*

https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%203%20The%20Data%20Protection%20Act%202021_0.pdf

² <https://www.oecd.org/sti/economy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm>

³ <https://gdpr-info.eu/>

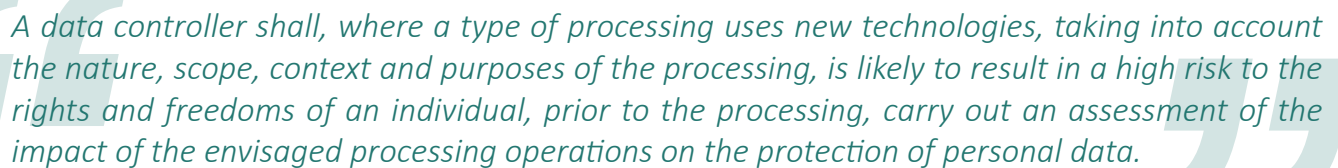


Specifically, **section 17** bars the processing of data of children or vulnerable persons unless consent is given by their parent or guardian. Data controllers are also required to take all reasonable efforts, including through technology, to ascertain whether consent has been obtained.

Part V (section 19-28) and **Part VI (sections 29-38)** offer guidelines to regulate data controllers, processors and auditors, including their functions and obligations. In prescribing the requirements for licensing, obligation to adhere to licensing requirements, and the punitive fines for violating the Act, these provisions emphasise compliance with the law so as to strongly protect personal data.

Freedom of expression stands to be promoted as **section 43** exempts journalistic works from limitations specified in section 12 on the principles of relevancy (section 12 (1) (c)), accuracy (section 12 (1) (d)), purpose (section 12 (1) (e)) and appropriate security (section 12 (1) (g)). In a number of African countries, journalistic works are not similarly exempt, which potentially has a chilling effect on freedom of expression and access to information.

Section 46 requires a data controller to carry out a data protection impact assessment to determine whether there are high risks to the rights and freedoms of an individual before data processing. The section provides:




A data controller shall, where a type of processing uses new technologies, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of an individual, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The data protection impact assessment is important as it serves to ensure that only specific kinds of data are collected, to specified limits and with minimised negative impact on individual privacy and other rights and freedoms.

The heavy penalties imposed on data controllers and individuals for contravention of the law under **section 55** will compel data controllers' compliance in fear of the huge fines. On conviction, a body corporate is liable to pay two percent of annual turnover of the preceding financial year or 600,000 Kwacha (USD 26,658), whichever is higher, and for a natural person, a fine not exceeding 300,000 Kwacha (USD 13, 329), or imprisonment for a term not exceeding 10 years, or both.

Part IX (sections 58-69) provides for the rights of data subjects. The rights include access and notification (section 58), rectification (section 59), erasure (section 60), objection (section 61), decision on automated data processing (section 62), restriction of processing (section 63), right to be informed by a data controller of the reasons for data collection (section 64), portability (section 65), notification obligation (section 66), lodging complaints (section 68) as well as the right to appeal (section 69). This specification of the data subject's rights means individuals could easily identify violated rights and pursue remedial measures.

The rules and principles of data protection and the rights of the data subject laid down in the Act promote individual autonomy of the data subject over their data. This thus provides data subjects with commendable levels of control over personal data. This is further buttressed by **section 15** on consent justification and objection to data processing, which includes giving consent in a prescribed manner, withdrawal of such consent, destruction of all data collected following withdrawal of consent, objection to processing, and termination of the process of collection of data upon objection.



Part X (sections 70 and 71) regulates the transfer of personal data outside Zambia. Under section 70, all personal data must be stored on a server or data centre located in Zambia. However, under section 70(2), data may be stored outside Zambia if prescribed by the communications minister, but under **section 70(3)** sensitive data can only be stored in Zambia. This section could, to some extent, guarantee storage of personal data in countries with data protection and processing laws that are, at a minimum, as strong as Zambia's. Even where cross-border transfers may be effected, section 71 lays down conditions to be fulfilled before transfer, including the data subject's consent and approval of the Data Protection Commissioner. The minister may prescribe the procedure for cross-border transfers.

The Code of Conduct provided by **section 78** and prepared by the Data Protection Commissioner further buttresses individuals' privacy. The Code of Conduct aims to bind data controllers, data processors and data auditors while dealing with personal data. The Code relates to issues such as provision of information to data subjects regarding confidentiality; advertising or representation of services; fair, accessible format and transparent processing of personal data for all data subjects.

The Cons

Processing Data for Personal Use

While **section 3(1)** encompasses all aspects that involve use of personal data, it potentially raises privacy issues. **Subsection 3(2)** provides that, "This Act does not apply to the processing of personal data by an individual for personal use." However, it does not define what individual or personal use is. Hence, the provision underlooks the possibility that individuals could process personal data in the guise of "personal use" yet put it to other uses that undermine other individuals' privacy.

Establishment of the Office of the Data Protection Commissioner

Section 4 establishes the Office of the Data Protection Commissioner whose functions include registration of data controllers and processors; licensing data auditors; providing information to stakeholders; giving advice to, and representing government on data protection; and maintaining a data register of data controllers, data processors and data auditors.

Although the provisions on its functioning appear to cast it as an independent data protection commission, the office has been placed under the ministry responsible for communications. Since personal data issues are very sensitive, common practices in data protection regimes require the establishment of independent data protection commissions. Placing the Office of the Data Protection Commissioner under an already existing institution could potentially make it prone to external influence such as political influence from the ministry and other government authorities that can interfere with the right to privacy.

Collection of Personal Data

Section 16 provides for collection of personal data by a data controller directly from a data subject and the circumstances under which personal data may be collected from a source other than the data subject. Exemptions apply "for the purposes of national security" (section 16(2)(d)(iv)), and where it is "necessary to prevent a reasonable threat to national security, defence or public order" (section 16(2)(g)(iii)). In many countries, "national security", "defence" and "public order" have been widely used as excuses to infringe individuals' rights, including privacy. While collecting data in circumstances described in section 16(2) is often justified, it should be done under appropriate safeguards that detail data controllers, the affected categories of data, the restrictions to be imposed, and storage period of the data as a way of assessing risks to rights and freedoms of individuals. Moreover, laws need to define concepts such as "national security".

Data Retention

Section 51 is emphatic on storage of data by controllers and processors for as long as that information is used for the specific purpose for which it was collected and for as long as the information is relevant for that purpose. The section, however, specifies the minimum storage period as one year and thereafter, for an undetermined period that may be prescribed.⁴ The section is clear on the purpose principle but one year may be too long to store some data. Moreover, the provision for storage for an undetermined period that may be prescribed provides room for abuse of the principle of purpose of data collection.

Cross-Border Data Transfers

Part X (sections 70 and 71) seek to regulate cross-border data transfers. These sections guarantee some level of data protection in Zambia as cross-border transfers are subjected to consent and approval of the Data Protection Commissioner. Yet it is possible that using these sections, state agencies could easily access personal data without the consent of data subjects, thereby undermining their privacy rights and potentially subjecting them to unauthorised surveillance.

Lack of Regulations

Currently, the Act cannot be enforced due to lack of implementing regulations. The Minister should therefore, in accordance with **section 82**, swiftly issue the relevant regulations to not only elaborate but prescribe the mode of implementation of the Act in respect to, among others, rights of data subjects and the arising duties, obligations and limitations, notification of security breaches, licensing of data auditors, processing of genetic, biometric and health data, processing of unique patient identifier, personal data of children, data retention, and registration of data controllers and data processors.

Conclusion

Zambia's Data Protection Act is a fairly drafted law that attempts to address key principles of data protection and individuals' privacy rights. It also makes major strides in addressing the needs of the data subject including through a unique provision for a data protection impact assessment and placement of restriction on processing of data of vulnerable persons. If implemented, it will enhance data protection and privacy of the individual. However, the problematic provisions as highlighted in this brief should be ironed out if the law is to comprehensively achieve its intended purpose.

⁴ The person to make the prescription is not mentioned, but could most probably be the Data Commissioner since their office is charged with the regulation of data protection and privacy in Zambia.



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Tel: +256 414 289 502

Email: programmes@cipesa.org

Twitter: [@cipesaug](https://twitter.com/cipesaug)

Facebook: facebook.com/cipesaug

www.cipesa.org