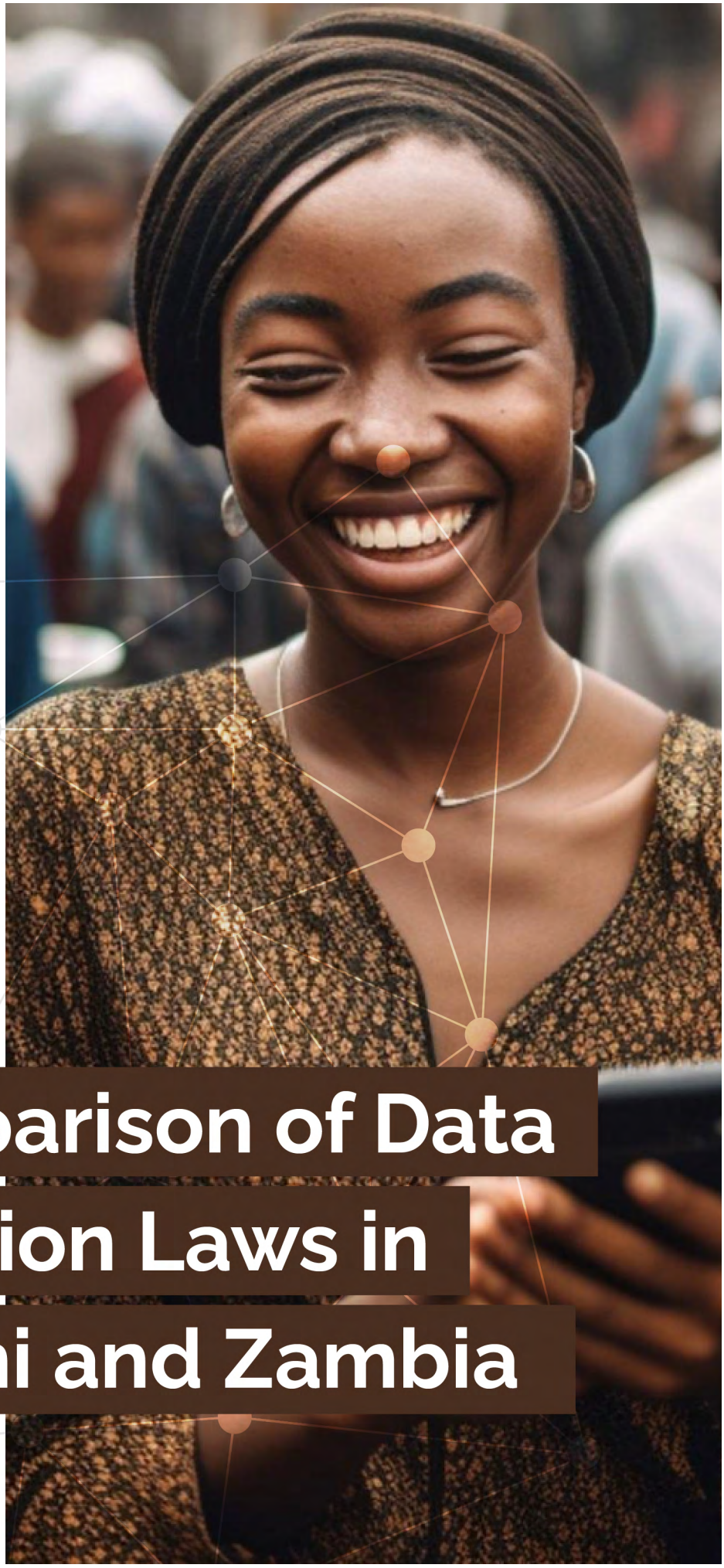
PARADIGM INITIATIVE

Digital Policy Digest

No. 1 of 2023



A Comparison of Data Protection Laws in Eswatini and Zambia

PARADIGM INITIATIVE

Digital Policy Digest

This Digital Policy Digest (DPD) documents digital rights policies and laws and presents guidance on areas needing reform. This edition features a legal analysis of data protection laws in two Southern Africa countries.

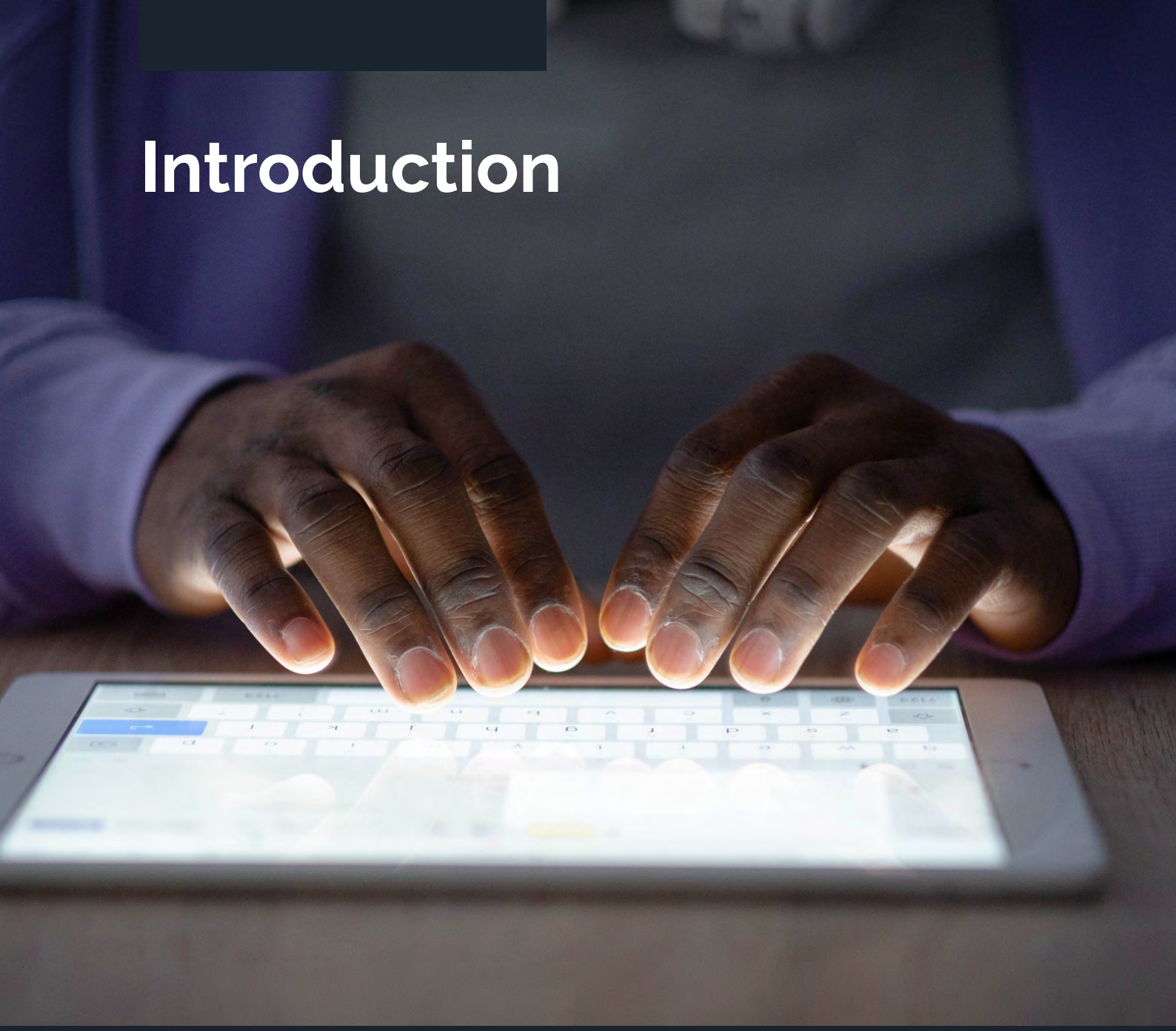
Published by:
Paradigm Initiative.

Researcher:
Thobekile Matimbe

Edited by:
Nnenna Paul-Ugochukwu.

Design & Layout by:
David Chima

Introduction



Personal data is a precious mineral that must be extracted with human rights safeguards to avert adverse impacts on fundamental rights. In 2022, Eswatini enacted a data protection law following closely behind its Southern African counterparts, Zambia and Zimbabwe, which enacted their laws on 23 March 2021 and 3 December 2021, respectively. On the other hand, Malawi and Namibia are yet to enact data protection legislation. An assessment of the Eswatini and Zambia data protection enactments presents some significant differences. While the assessment of the laws below is not exhaustive, it highlights what other countries yet to enact data protection laws can emulate or avoid.

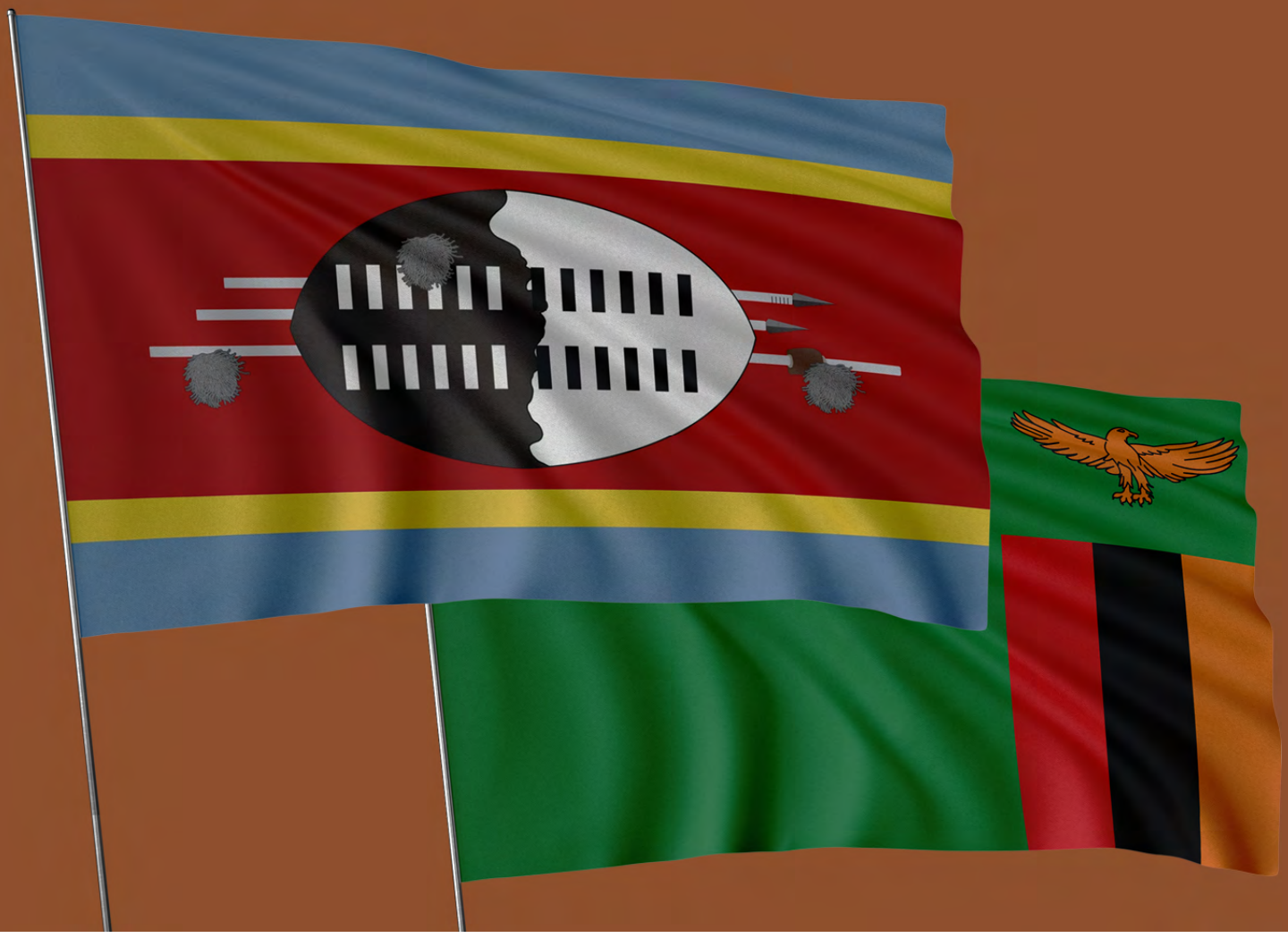
Introduction

Observing regional developments, the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) took effect in June 2023, after Mauritania ratified as the 15th signatory. African states have had low traction to ratify the regional treaty, considering its adoption on 27 June 2014. The significance of the Malabo Convention regarding data protection is the expectation that it can instil the conscience to preserve privacy in the African States through its laws. If complied with, it creates, to a large extent, an instinct to preserve personal data in a way that advances human rights. Article 8 of the Malabo Convention stipulates that each State party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of data.

The African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa adopted in 2019, provides in Principle 42(1) that in adoption of laws for the protection of personal information of individuals should do so according to human rights standards. The yardstick for data protection is clearly set.

The Malabo Convention defines a data subject as a natural person that is the subject of personal data protection, and the Declaration refers to personal information of an individual. For purposes of this analysis, a data subject is any individual or natural person whose data is processed. The data controller is a natural or legal person controlling the personal information of an individual.

Eswatini versus Zambia



Eswatini passed the Data Protection Act, 2022 on 4 March 2022 (the Eswatini Act) with the objective of providing for the collection, processing, disclosure and protection of personal data, balancing competing values of personal information privacy and sector-specific laws and other related matters. Its purpose is to provide for the collection. In terms of section 3, the Eswatini DPA applies to data controllers and processors, whether or not they are domiciled, or their principal place of business is in Eswatini who use automated or

non-automated means in Eswatini for forwarding personal data. The Eswatini Act also concerns the processing of personal data wholly or partly by automated means. Where the data controller fails to comply with the Act, section 6 provides for the penalties, including a warning, formal notice or a fine where the formal notice is not complied with.

On the other hand, Zambia passed its Data Protection Act, 2021 (the Zambian Act) on 24 March 2021 to 'provide an effective system for the use and protection of personal data; regulate the collection, use, transmission, storage and otherwise processing of personal data; establish the Office of the Data Protection Commissioner and provide for its functions; the registration of data controllers and licencing of data auditors; provide for the duties of data controllers and data processors; provide for the rights of data subjects; and provide for matters connected with, or incidental to, the foregoing.' In Zambia, the Act applies to the processing of personal data performed wholly or partly by automated means and to any processing other than by electronic means, as provided in Section 3.

> The objectives of the Eswatini and Zambia Acts differ in that the object of the Zambian Act is data protection entirely while the Eswatini Act seeks to balance competing interests of privacy with other sector-specific laws. The objective of the Eswatini Act does not centre data protection law in line with human rights. An amendment to the objective would strengthen the Eswatini Act, according due regard to data protection in compliance with human rights standards of privacy. Balancing privacy with sector-specific laws which in themselves may be contrary to human rights standards falls short of adequate safeguards. This human rights-based approach ensures a more robust approach to data protection.

Processing of Personal Information

In terms of section 9(2) of the Eswatini Act, personal information must be processed if the data subject consents, the processing is necessary in terms of contractual obligations to which the data subject is a party, the processing ensures compliance with a legal obligation to which the data controller is a subject, processing is necessary to protect legitimate interests of the data subject, it is necessary for the proper performance of public law duty by a public body or processing is necessary for pursuing the legitimate interests of third party to whom the information is required. Section 9(4) provides that personal information may only be processed, if given the purpose for which it is collected, it is adequate, relevant and not excessive.

A data controller in Zambia shall process personal information by consent of the data subject in terms of section 15(1) of the Zambia Act while section 12(1) of the Zambia DPA stipulates how

data controllers should handle data to safeguard the rights of data subjects. It provides for data rectification, use limited to purpose and fair, transparent, and lawful processing. Section 13(a) and (c) of the Zambia Act provides that a data controller may process personal data where the data subject has given consent to the processing of that data subject's personal data or the processing relates to personal data which is manifestly made public by the data subject, the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or for compliance with a legal obligation to which the data controller is subject or where the processing relates to personal data which is manifestly made public by the data subject. Section 13(b) states that data may processed where the processing is necessary '(i) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (ii) for compliance with a legal obligation to which the data controller is subject; (iii) in order to protect the vital interests of the data subject or of another natural person; (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; (v) 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;'

> To varied degrees, both acts give data subjects agency over their data providing consent as a starting point to the processing of personal information. With regards to the processing of personal information, the Eswatini Act does not particularly mention human rights as part of its text as in the Zambian Act under section 13(b)(v). The Zambian Act refers to data protection with a human rights lens, particularising this importance where children are concerned. Ultimately, human rights safeguards must be the yardstick in processing data for everyone.

Data Protection Authorities and Breaches

The Eswatini Act vests the authority to implement the Act in the already existing Eswatini Communications Commission (Commission) and does not create a new entity. In the event of a data breach, a data controller must notify the Commission and the data subject as soon as reasonably possible of any unauthorised access to personal data in terms of Section 17(1) and 17(2) of the Eswatini Act. There is no specific timeline within which data breaches should be disclosed.

The Zambia Act implies a separate data protection commission must be established, yet the government of Zambia vested the role of implementing the law

in the Zambia Information Communications and Technology Authority (ZICTA) established by the Information Communications and Technologies Act of 2009. While this move closed the gap that could have arisen from enacting the law and setting up a data protection authority instantly deploying the wheels of the law to turn, the concern is that ZICTA may fail to discharge its data protection functions due to competing interests fully. The Zambian DPA vests in the Ministry responsible for communications, the Office of the Data Protection Commissioner responsible for regulating data protection and privacy. Regarding data breaches, section 49(1) obligates a data controller to notify the Data Protection Commissioner within twenty-four hours of any security breach affecting personal data processed, and section 49(3) provides that the data controller should also notify the data subject as soon as practicable.

> In practice, both Eswatini and Zambia adopted a similar approach of relying on existing authorities to implement their data protection laws. Data Protection Authorities are mandated to ensure the implementation of data protection legislation, a key function best executed by an independent and efficient body. Some African countries have not established new entities as data protection authorities but have leveraged existing authorities regulating postal and telecommunications or information, communications, and technology, as in the case of Eswatini and Zambia. The concern with this approach is that already existing authorities may fail to fully commit to implementing data protection due to other competing functions. A benefit of this approach is the prompt commencement of implementation of a datza protection law, avoiding a lengthy waiting period to establish a fresh entity. Irrespective of the approach, a data protection authority must be able to ensure functions are fully discharged without suspension of other functions based on conflicting interests by an entity with other principal roles.
>
> Regarding data breaches, the Eswatini Act gives unfettered discretion to data controllers to determine when it is reasonable to disclose any unauthorised access to personal data, a potential threat to privacy. Discretion can be abused without a timeline indicating the urgency with which data breaches must be addressed. On the other hand, the Zambia Act stipulates a 24-hour timeline within which data controllers should notify the Data Protection Commission of data breaches while data subjects are notified as soon as practicable. The approach in the Zambia Act accords the relevant urgency in data protection cases.

Automated Decision-Making

The use of artificial intelligence and emerging technologies necessitates data protection responses that ensure safety, trust and fairness in handling personal data. Section 45(1) of the Eswatini Act provides that a person can-

not be subjected to a decision which has a legal effect on them based on an automated processing of personal information with the relevant exceptions provided.

The Zambia Act progressively addresses the processing of personal data collected through emerging technologies. Its section 46(1) guides data controllers to consider the nature, scope, context and purposes of the processing and the likelihood of resulting in a high risk to the rights and freedoms of an individual. The same calls data controllers to conduct impact assessments before processing the data to understand the impact on personal data.

> While section 45(1) of the Eswatini Act protects data subjects from automated decision-making with legal effect on the data subject, this provision is limited in the scope of protections. Protection should rather be directed at avoiding human rights violations as opposed to legal effects. The Zambia Act has more consideration for human rights and provides for impact assessments to be conducted by data controllers, a key element ensuring the responsibility to prevent harm to data subjects. In the absence of comprehensive artificial intelligence strategies in both countries, these provisions afford a level of protection and are a basis of trust building for data subject.

Operationalisation

In Eswatini, section 54(1) provides that the Minister may enact regulations to give effect to the Act. This provision is not mandatory. The failure of section 54(1) to make it mandatory for the Minister to enact regulations within a stipulated time frame leaves room for operationalisation of provisions of the Act, such as section 51(1) of the Eswatini Act, which makes it mandatory for the Eswatini Communications Commission to enact rules guiding whistleblowing. Section 82(1) of the Zambia Act states that the Minister may enact regulations to better carry out the provisions of the Zambia Act.

> Enactment of data protection regulations is a key aspect of data protection in both countries that needs to be done to fully operationalise the Acts.

Cross-Border Transfer of Personal Data

In Eswatini, personal information shall only be transferred to recipients in a Member State that has transposed the Southern African Development Community (SADC) data protection requirements as provided under section 32 of the Eswatini Act referring to sub-regional requirements. SADC has a Model Law on Data Protection on data protection in Southern Africa which presents the SADC requirements in a bid to harmonise data protection laws in Southern Africa. However, section 33(1) provides that personal information may be transferred to other countries outside of Eswatini or SADC Member States if there is adequate protection and the transfer itself is solely to allow the processing that is otherwise authorised to be done by the controller.

The Zambia Act provides in section 70(1) that a data controller shall process and store personal data on a server or data centre in Zambia. Still, the Minister may prescribe categories of personal data that may be stored outside the country, as stated in section 70(2). However, sensitive personal data shall be processed and stored in a server or data centre located in Zambia under section 70(3) of the Zambia Act.

> The Eswatini Act is more direct in its reference to SADC requirements. The Zambia Act does not refer to SADC requirements specifically but allows the Minister to stipulate exceptions through regulations of personal data categories that can be processed outside of Zambia. For legitimate cross-border flows of personal data, a trusted environment needs to be fostered through best data governance practices. It is key to development through the use of emerging technologies.

Conclusion

Attendant rights-respecting practices of data protection are key in order for protections to be guaranteed and implemented. Countries yet to enact data protection laws need to develop laws that give effect to human rights. As such, they must avoid a copy-and-paste approach but enact laws carefully, adopting best practices. Compliance and commitment to international standards are essential for data protection, ensuring privacy and signifying positive State willpower. Zambia is commended for its progressive data protection law, while Eswatini can consider drawing lessons to strengthen its approach. Eswatini is urged to ratify the Malabo Convention, a progressive step taken by Zambia on 24 March 2021.

MORE ABOUT US

Paradigm Initiative has worked in communities across Nigeria since 2007 and across Africa since 2017, building experience, community trust, and an organisational culture that positions us as a leading non-governmental organisation in ICT for Development and Digital Rights on the continent. Across our regional offices in Kenya, Nigeria, Senegal, Zambia, Zimbabwe, Cameroon, the Democratic Republic of Congo (DRC), and beyond, we have impacted youth with improved livelihoods through our digital inclusion and digital rights programs. The organisation's programs include Life Skills. ICTs. Financial Readiness. Entrepreneurship (LIFE) Training Program, a digital readiness workshop for girls, and Life@School Club Program. PIN has also built online platforms that educate and serve as safe spaces for reporting digital rights violations. These mediums, in the form of reports, short films, and educational online platforms, include Ayeta, Londa, and Ripoti. The organisation is also the convener of the annual Digital Rights and Inclusion Forum (DRIF), a pan-African platform where conversations on digital policy in Africa are shaped, policy directions debated, and partnerships forged for action. The forum has been held since 2013.

PARADIGM INITIATIVE

374 Borno Way, Yaba 101245, Lagos, NIgeria

www.paradigmhq.org

@paradigmHQ