Deloitte.

Zambia Data Protection Act 2021

Quick Guide

November 2023

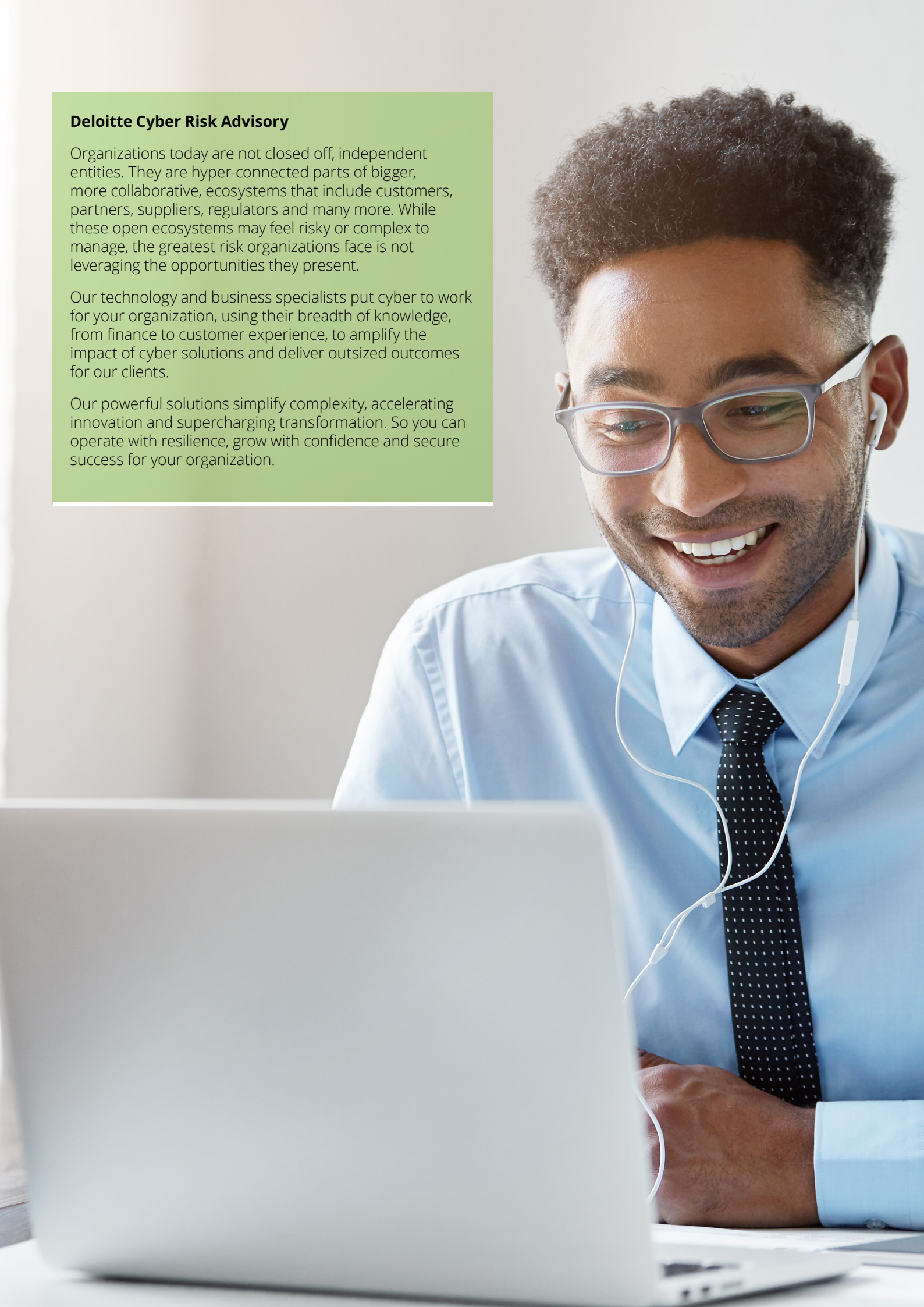
MAKING AN IMPACT THAT MATTERS since 1845

Deloitte Cyber Risk Advisory

Organizations today are not closed off, independent entities. They are hyper-connected parts of bigger, more collaborative, ecosystems that include customers, partners, suppliers, regulators and many more. While these open ecosystems may feel risky or complex to manage, the greatest risk organizations face is not leveraging the opportunities they present.

Our technology and business specialists put cyber to work for your organization, using their breadth of knowledge, from finance to customer experience, to amplify the impact of cyber solutions and deliver outsized outcomes for our clients.

Our powerful solutions simplify complexity, accelerating innovation and supercharging transformation. So you can operate with resilience, grow with confidence and secure success for your organization.



Background

Africa - Data Privacy Legislation

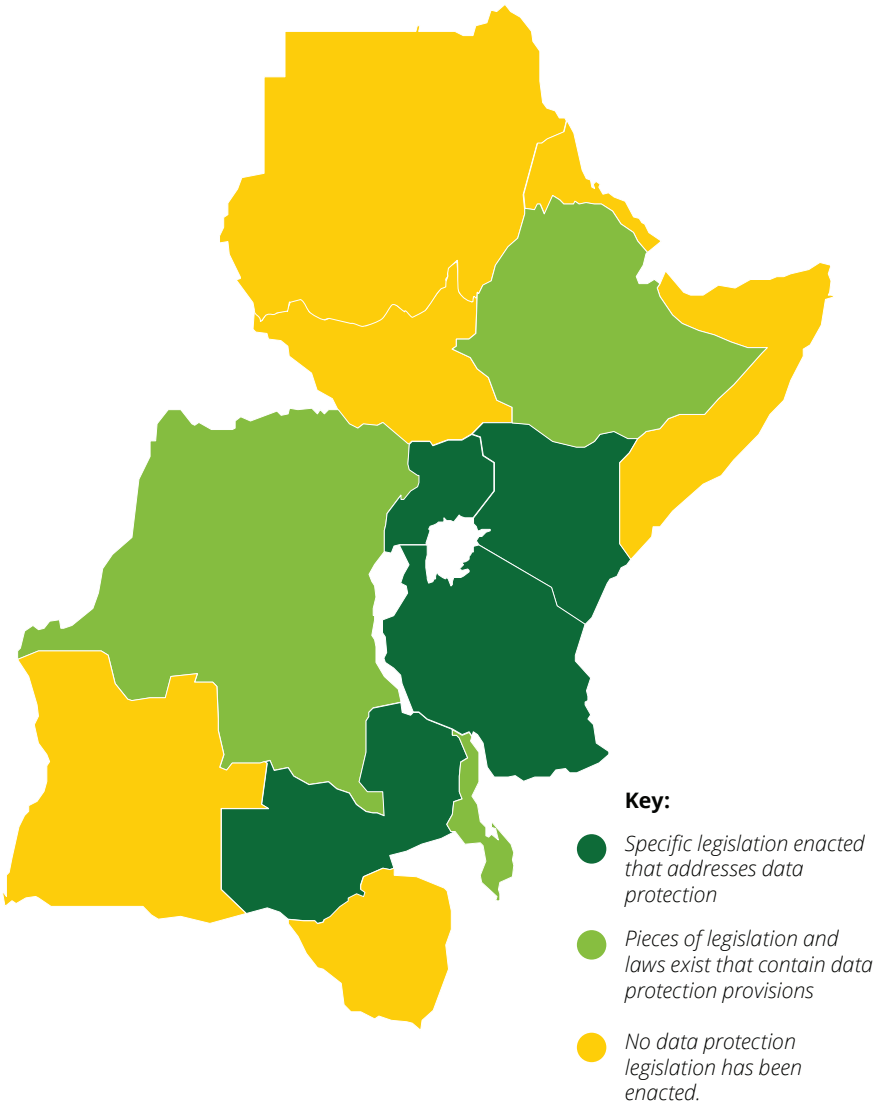
The Kenya Data Protection Bill was enacted and came into effect on 25 November 2019. Registration is required with the ODPC and has been ongoing since July 2022.

Tanzania's Parliament recently passed the Personal Data Protection Bill in 27 November 2022 which establishes a Commission for the Protection of Personal Data.

In 2021, the Ethiopian government prepared a preliminary draft of the Ethiopian Personal Data Protection Proclamation under the auspices of the Ministry of Technology and Innovation.

On 25 February 2019, the Ugandan President Assented to the Data Protection and Privacy Act, 2019 ('the Act').

Rwanda Law gazette'd on 15 October 2021 The passing of this law began a 2-year journey to compliance.



Burundi does not have a law that specifically regulates personal data protection. However, several laws and regulations currently in force contain data protection provisions or impose confidentiality obligations on specific types of personal information.

Zambia Data Protection Law was enacted by Parliament of Zambia on 24th March 2021. The Act is 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.

Introduction

Overview

Zambia has promulgated a Data Protection Act....

The Zambia Data Protection Act, No. 3 of 2021 (Data Act) is the primary legislation that regulates data privacy and protection in Zambia. It came into force on 1st January 2023 and is intended to provide an effective system for the use and protection of personal data, and to regulate the collection, use, transmission, storage, and otherwise processing of personal data.

The Zambia Data Act applies to all persons who process personal data in Zambia, regardless of whether they are based in Zambia or abroad. It also applies to all forms of personal data, including electronic, paper-based, and genetic data.

The Zambia Data Act sets out a number of key principles that data controllers and processors must comply with, including:

Principles of the Zambia Data Protection Act

Transparency: Data controllers and processors must be transparent about how they collect, use, and store personal data.

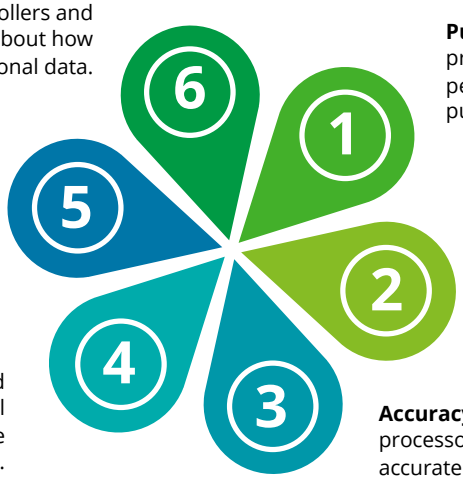
Purpose limitation: Data controllers and processors must only collect and process personal data for specific and lawful purposes.

Integrity and confidentiality: Data controllers and processors must take appropriate measures to protect the integrity and confidentiality of personal data.

Data minimization: Data controllers and processors must only collect and process the minimum amount of personal data necessary for the purposes for which it is being processed.

Storage limitation: Data controllers and processors must only store personal data for as long as is necessary for the purposes for which it is being processed.

Accuracy: Data controllers and processors must keep personal data accurate and up-to-date.



Transfer of Personal Data Outside Zambia

The Zambia Data Protection Act establishes the Office of the Data Protection Commissioner (ODPC), which is responsible for overseeing the implementation of the Act and enforcing its provisions. The ODPC has a number of powers, including

- The power to investigate complaints,
- Issue notices, and
- Impose penalties on data controllers and processors who breach the Data Act.

The Data Protection Act is a significant piece of legislation that will help to protect the privacy of individuals in Zambia. It is important for all data controllers and processors to be familiar with the Act and to comply with its provisions.

Here are some of the key provisions of the Data Protection Act:

01 **Registration of data controllers and processors:** Any person who intends to process personal data must register with the ODPC.

02 **Data processing notification:** Data controllers and processors must notify the ODPC of their data processing activities.

03 **Consent:** Data controllers must obtain consent from data subjects before collecting, using, or disclosing their personal data.

04 **Sensitive personal data:** Data controllers are prohibited from processing sensitive personal data without a lawful basis.

05 **Data protection impact assessment:** Data controllers must carry out a data protection impact assessment (DPIA) before processing personal data in certain circumstances.

06 **Rights of data subjects:** Data subjects have a number of rights, including the right to access their personal data, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, and the right to object to processing.

07 **Appointment of a Data Protection Officer:** Organisations processing personal data are required to appoint a Data Protection Officer in accordance with the guidelines issued by the Data Protection Commissioner.

Zambia Data Protection Act 2021

Pro's of the Zambia Data Protection Act 2021

The Zambia Data Protection Act 2021 comes with good deeds for the Zambia republic and promotes good virtues in line with the global data protection standards such as the General Data Protection Act (GDPR) and other African Legislations. Some of the advantages include;

01 **Enhanced data protection and privacy for individuals:** The Act provides a number of safeguards for individuals' personal data, including the right to access, rectify, erase, restrict processing, data portability, and object to processing.

02 **Increased transparency and accountability for data controllers and processors:** The Act requires data controllers and processors to be transparent about their data processing activities and to be accountable for their compliance with the Act.

03 **Support for innovation and economic growth:** The Act provides a clear and predictable regulatory framework for data processing, which can help to promote innovation and economic growth.

04 **Protection of vulnerable persons:** The Act places specific restrictions on the processing of personal data of vulnerable persons, such as children and people with disabilities.

Cons of the Zambia Data Protection Act 2021

However, there are con's as well to the Zambia Data Protection Act 2021, these are;

01 **Lack of implementing regulations:** The Act has not yet been fully implemented, as there are no implementing regulations in place. This means that some of the provisions of the Act are not yet enforceable.

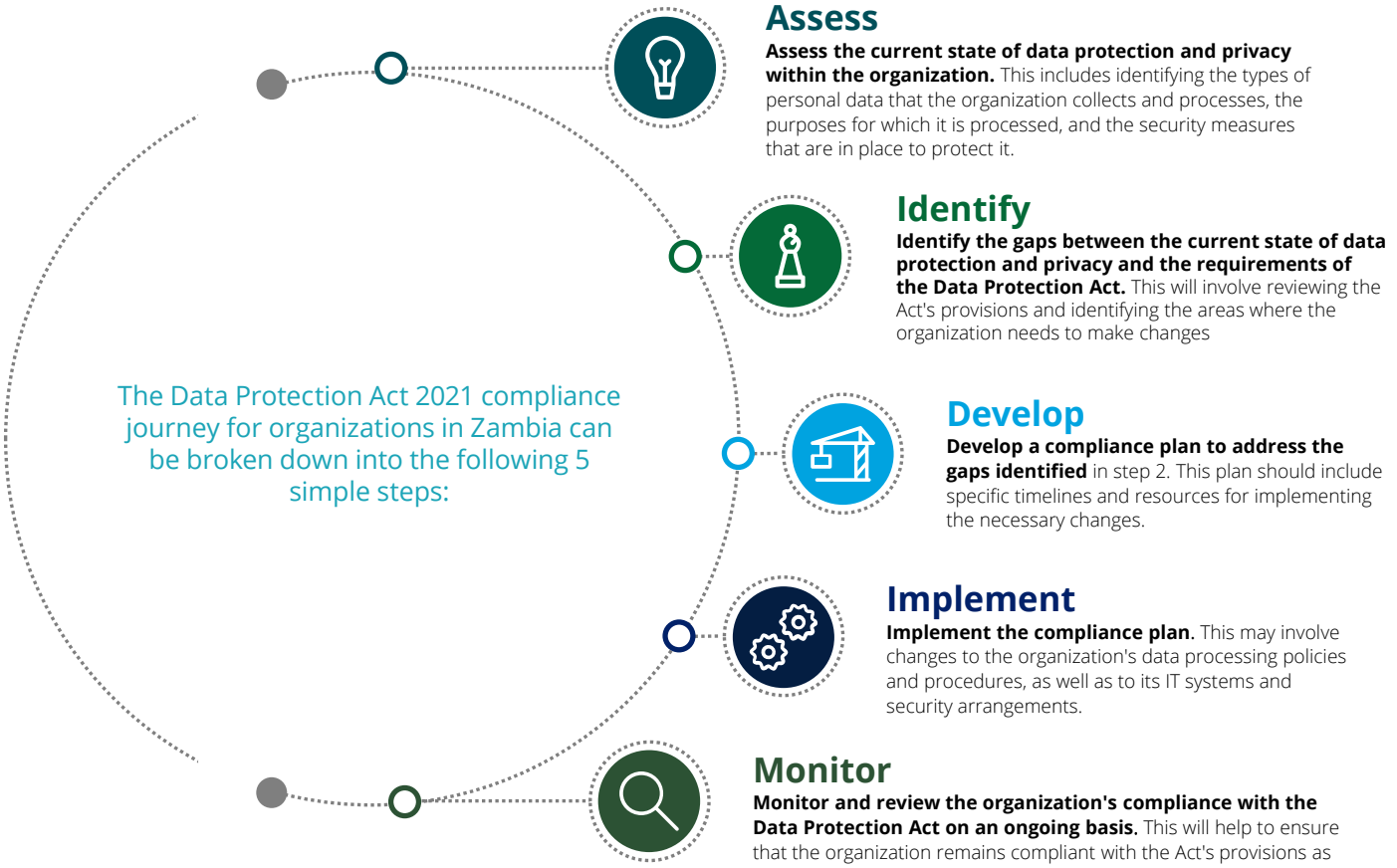
02 **Potential for conflict with other laws:** Some of the provisions of the Act may conflict with other laws in Zambia, such as the Cyber Security and Cyber Crimes Act. This could lead to uncertainty and confusion for data controllers and processors.

03 **Potential for high compliance costs:** The Act places a number of obligations on data controllers and processors, which could lead to high compliance costs.

04 **Limited enforcement powers of the Data Protection Commissioner:** The Data Protection Commissioner has limited powers to enforce the Act, which could make it difficult to deter breaches of the Act.

Compliance Journey for Organizations

Organizations looking towards compliance to the Zambia Data Protection Act 2021 have to follow certain guidelines and meet certain requirements that will allow them to be Data Protection Act 2021 compliant. This steps include;



Assess

Assess the current state of data protection and privacy within the organization. This includes identifying the types of personal data that the organization collects and processes, the purposes for which it is processed, and the security measures that are in place to protect it.

Identify

Identify the gaps between the current state of data protection and privacy and the requirements of the Data Protection Act. This will involve reviewing the Act's provisions and identifying the areas where the organization needs to make changes

Develop

Develop a compliance plan to address the gaps identified in step 2. This plan should include specific timelines and resources for implementing the necessary changes.

Implement

Implement the compliance plan. This may involve changes to the organization's data processing policies and procedures, as well as to its IT systems and security arrangements.

Monitor

Monitor and review the organization's compliance with the Data Protection Act on an ongoing basis. This will help to ensure that the organization remains compliant with the Act's provisions as they evolve.

Here are some specific steps that organizations in Zambia can take to comply with the Data Protection Act 2021:

01 **Register with the Data Protection Commissioner (ODPC).** All organizations that process personal data in Zambia are required to register with the ODPC. This can be done online through the ODPC's website.

02 **Develop a data protection policy and procedure.** The data protection policy should set out the organization's approach to data protection and privacy. It should also include procedures for collecting, using, storing, and disposing of personal data.

03 **Implement data security measures.** Organizations should implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, alteration, loss or destruction.

04 **Obtain consent from data subjects.** Organizations must obtain consent from data subjects before collecting, using, or disclosing their personal data.

05 **Provide data subjects with access to their personal data.** Data subjects have the right to access their personal data and to have it corrected, erased, or restricted. Organizations must have procedures in place to comply with these requests.

06 **Report data breaches to the ODPC.** Organizations are required to report data breaches to the ODPC within 24 hours of becoming aware of them.

The Big Picture

Key Elements of the Zambia Data Protection Act 2021

Penalties for non compliance

Infringement of provisions of the Zambia Data Protection Act 2021 (DPA) will attract a penalty of not more than One hundred million or, in the case of an undertaking, not more than 2% of its annual turnover of the preceding financial year, whichever is higher.

Where the offence is committed by a natural person, that person shall be liable, on conviction to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding five years, or to both.

Additionally,a natural person who commits an offence under the Act for which a specified penalty is not provided, is liable, on conviction, to a fine not exceeding three hundred thousand penalty units or to imprisonment for a term not exceeding three years, or to both.

Increased territorial scope

DPA will apply to all companies processing the personal data of data subjects residing in Zambia, regardless of the company's location.

Explicit and retractable consent from data subjects

Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Data subject rights

Data subjects can request confirmation whether or not their personal data is being processed, where and for what purpose. Additionally, data subjects can request to be forgotten, which entails the removal of all the data related to the data subject.

Breach notification within 24 hours

Notify the Data Commissioner within Twenty-Four (24) hours of becoming aware of a breach and to the data subject in writing within a reasonably practical period.

Privacy by design

Now a legal requirement for the consideration and inclusion of data protection from the onset of the designing of systems, rather than a retrospective addition.

Data inventory

Organizations must maintain a record of processing activities under its responsibility– or, in short, they must keep an inventory of all personal data processed. The inventory must include the multiple types of information, such as the purpose of the processing.

Data protection officers

Depending on the type of personal data and intensity of processing activities, an organisation shall be required to appoint a Data Protection Officer to facilitate the need to demonstrate compliance to the Act.

Zambia Data Protection Act 2021

Organizations should also be aware of the following specific requirements of the Data Protection Act 2021:

Sensitive personal data. The Act places special restrictions on the processing of sensitive personal data, such as data on health, race, and ethnicity. Organizations must obtain explicit consent from data subjects before processing sensitive personal data.

Data protection impact assessments (DPIAs). Organizations must carry out a DPIA before processing personal data in certain circumstances, such as when the processing is likely to result in a high risk to the rights and freedoms of individuals.

Cross-border data transfers. The Act restricts the transfer of personal data outside of Zambia. Organizations must obtain the consent from the data subject as well as the ODPC before transferring personal data outside of Zambia.

The Zambia Data Protection Act 2021 is a complex piece of legislation, and it is important for organizations in Zambia to seek legal advice to ensure that they are complying with its provisions.

Part IV, Section 14 (1) – Processing Sensitive Personal Data

A person shall not process sensitive personal data, unless—

1. *Processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is exercising a judicial function;*
2. *Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services ;or*
3. *Processing is necessary for reasons of public interest.*

Zambia Data Protection Act 2021

Part IV, Section 14 (1) – Processing Sensitive Personal Data

A body corporate that contravenes the provisions of this Part commits an offence and is liable on conviction to—

1. *A fine not exceeding one hundred million penalty units; or*
2. *Two percent of annual turnover of the preceding financial year, whichever is higher*

Zambia Data Protection Act 2021

Data Controllers, Data Processors & Data Auditors

The Zambia Data Protection Act 2021 does not explicitly classify Data Controllers and Data Processors into different categories. However, the Act does impose different requirements on Data Controllers and Processors depending on the nature and scope of their data processing activities.

A Data Controller is defined as a person who, either alone or jointly with other persons,controls and is responsible for keeping and using personal data on a computer, or in structured manual files, and requests, collects, collates, processes or stores personal data from or in respect of a data subject. On the other hand a Data Processor is defined as a person, or a private or public body that processes personal data for and on behalf of and under the instruction of a data controller. A Data Auditor is any person who intends to provide data auditing services under the Act.

Registration as Data Controller and Data Processor is mandatory under the Act and failure to register is termed as an offence and is penalized as per the law. Data Auditors must also be licenced by the Data Protection Commissioner in the prescribed manner and form on payment of the prescribed fee.

The Act mandates the following from Data Processors and Controllers;

Part VIII, Section 47 – Duties of the Data Controller & Processor

A data controller or data processor, shall provide guarantees regarding the technical and organisational security measures employed to protect the personal data associated with the processing undertaken and ensure strict adherence to such measures.

Zambia Data Protection Act 2021

Part V, Section 20 (3)– Data Controller & Processor

The Data Protection Commissioner shall, where it rejects an application under subsection (2), inform the applicant, inwriting and give reasons for the decision..

Zambia Data Protection Act 2021

Part V, Section 20 (2)– Data Controller & Processor

The Data Protection Commissioner may, within fourteen days of receipt of an application under subsection (1), grant or reject the application.

Zambia Data Protection Act 2021

Part V, Section 21 (1) – Data Controller & Processor

The Data Protection Commissioner shall, within

fourteen days of the approval of an application under section 20, issue the applicant with a certificate of registration, if the applicant meets the prescribed requirements.

Zambia Data Protection Act 2021

Part V, Section 21 (1) – Data Controller & Processor

A registered data controller or data processor may three months before the expiration of the validity of the certificate, apply to the Authority for renewal of a certificate of registration in a prescribed manner and form on payment of a prescribed fee.

Zambia Data Protection Act 2021

Part VIII, Section 47 – Duties of the Data Controller & Processor

(45) A data controller shall keep and maintain, in writing, a record of—

Processing activities and meta data under its responsibility in the prescribed manner and form; and

All categories of processing activities carried out in the prescribed manner and form.

A data controller shall make the record available to the Data Protection Commissioner on demand.

Zambia Data Protection Act 2021

Part IV, Section 18 (1) - Offence and penalty for contravention of personal data obligation.

A body corporate that contravenes the provisions of this Part commits an offence and is liable on conviction to—

(a) A fine not exceeding one hundred million penalty units; or

(b) Two percent of annual turnover of the preceding financial year, whichever is higher.

Zambia Data Protection Act 2021

Part VII, Section 47 (3) – Auditing and Review

A data controller and data processor shall undertake a periodic review of security safeguard in accordance with guidelines issued by the Data Protection Commissioner.

Zambia Data Protection Act 2021

The Zambia Data Protection Act 2021 also does add the responsibilities of maintaining the CIA (Confidentiality, Integrity and Availability) on the Data Controller and Processors.

1 Integrity

- Maintaining integrity of personal data using methods including pseudonymisation and encryption.

2 Confidentiality & Availability

- Ensuring ongoing confidentiality, integrity and implementation of measures necessary to protect the integrity of personal data;

3 Measures Implementation

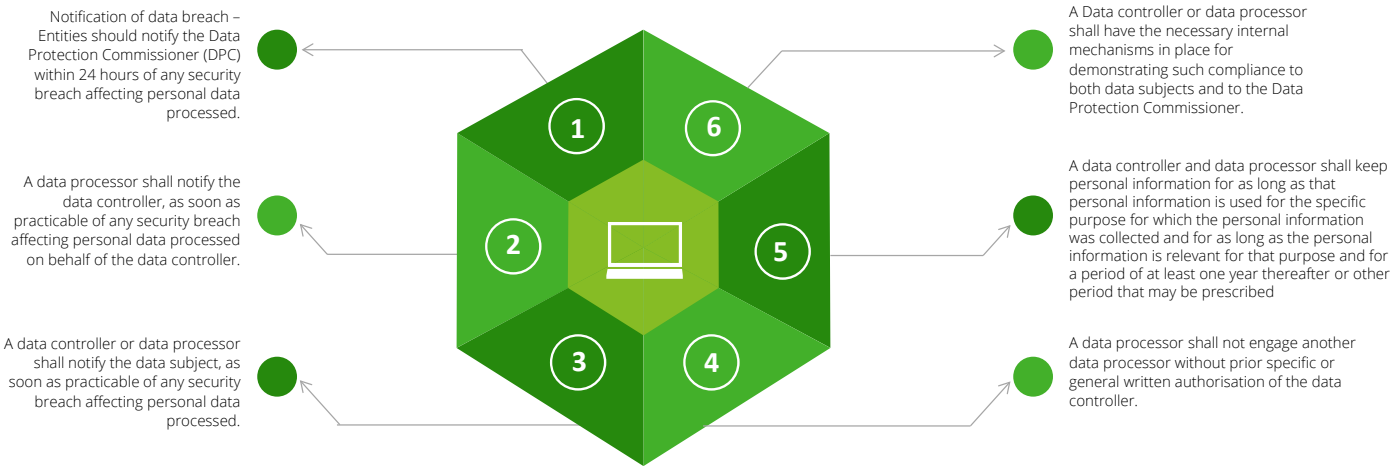
- Implement measures necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

4 Policies

- Implementation of appropriate data protection policies.

Data Processor & Data Controller Obligations

The Zambia Data Protection Act 2021 does add different obligations to the entities. These include:



Data Subject Rights

Data Subject Rights are a crucial part of the Zambia Data Protection Act, granting individuals more autonomy over their personal information and how it's used. These rights allow individuals to have control over and place limits on the collection, use and disclosure of their data. Below is an overview of rights granted to data subjects.

Rights of the Data Subject as prescribed in the Zambia Data Protection Act 2021

- Right to obtain confirmation on whether their data is being processed
- Right to restriction of processing
- Right to know the period of storage of the personal data.
- Right to portability of personal data.
- Right to know the 3rd parties who have access to their data.
- Right to access their data.
- Right to rectification of data.
- Right to erasure.
- Right to Objection.

Part VII, Section 47 (3) – Auditing and Review

A data subject may, where that data subject's personal data is being processed, access in a manner that the data subject understands the following information:

a. The purpose of the processing, the category of data the processing relates to, and the categories of recipients the data is disclosed to;

b. Envisaged period for which the personal data shall be stored, where possible or if not possible, the criteria used to determine that period;

c. Data being processed, as well as the source of that data; and

d. Information about the basic logic involved in any automatic processing of data relating to the data in case of automated decision making.

Zambia Data Protection Act 2021

Cross-Border Transfer of Data

The Zambia Data Protection Act 2021 (Act) imposes restrictions on the cross-border transfer of personal data. Section 70 of the Act states that no person shall transfer personal data outside of Zambia unless:

- The transfer is made to a country that has been designated by the Minister of Communications and Technology as a country with an adequate level of data protection;
- The transfer is made subject to a contract or other instrument that has been approved by the Data Protection Commissioner (ODPC); or
- The transfer is made with the consent of the data subject.
- The Minister of Communications and Technology has not yet designated any countries as having an adequate level of data protection under Section 70 of the Act. This means that, in general, organizations in Zambia cannot transfer personal data outside of Zambia without the approval of the ODPC or the consent of the data subject.

The ODPC may approve the cross-border transfer of personal data if the ODPC is satisfied that the transfer is necessary for the purposes of:

- The performance of a contract between the data subject and the data controller;
- The taking of steps to enter into a contract between the data subject and the data controller;
- The compliance of the data controller with a legal obligation;
- The protection of the vital interests of the data subject or another individual;
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- The purposes of scientific research or historical research or statistical research; or
- The purposes of journalism or artistic expression or literary expression.
- The ODPC may also approve the cross-border transfer of personal data if the ODPC is satisfied that the transfer is subject to appropriate safeguards to protect the privacy and security of the personal data.

The Act also places restrictions on the transfer of sensitive personal data outside of Zambia. Sensitive personal data includes data on race, ethnicity, religion, political affiliation, trade union membership, health, sexual orientation, and criminal convictions. The Act prohibits the transfer of sensitive personal data outside of Zambia without the explicit consent of the data subject.

The Act does not apply to the transfer of personal data outside of Zambia if the transfer is made by an individual for personal or household purposes.

Part X, Section 70 – Data Transfer Outside Zambia

71. (1) Personal data other than personal data categorised in accordance with section 70(2) may be transferred outside the Republic where—

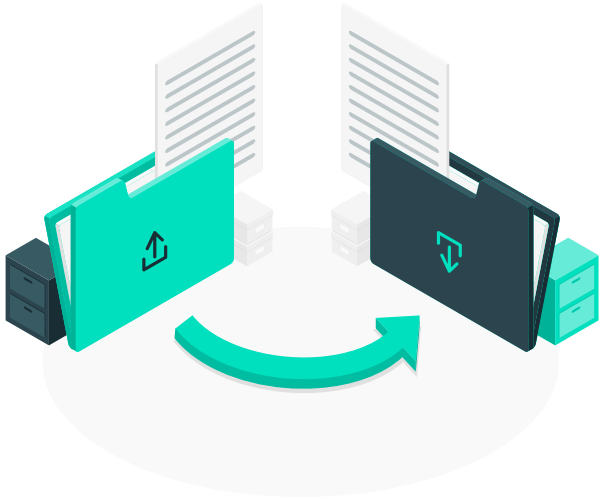
(a) the data subject has consented and

(i) the transfer is made subject to standard contracts or intragroup schemes that have been approved by the Data Protection Commissioner; or

(ii) The Minister, has prescribed that transfers outside the Republic is permissible; or

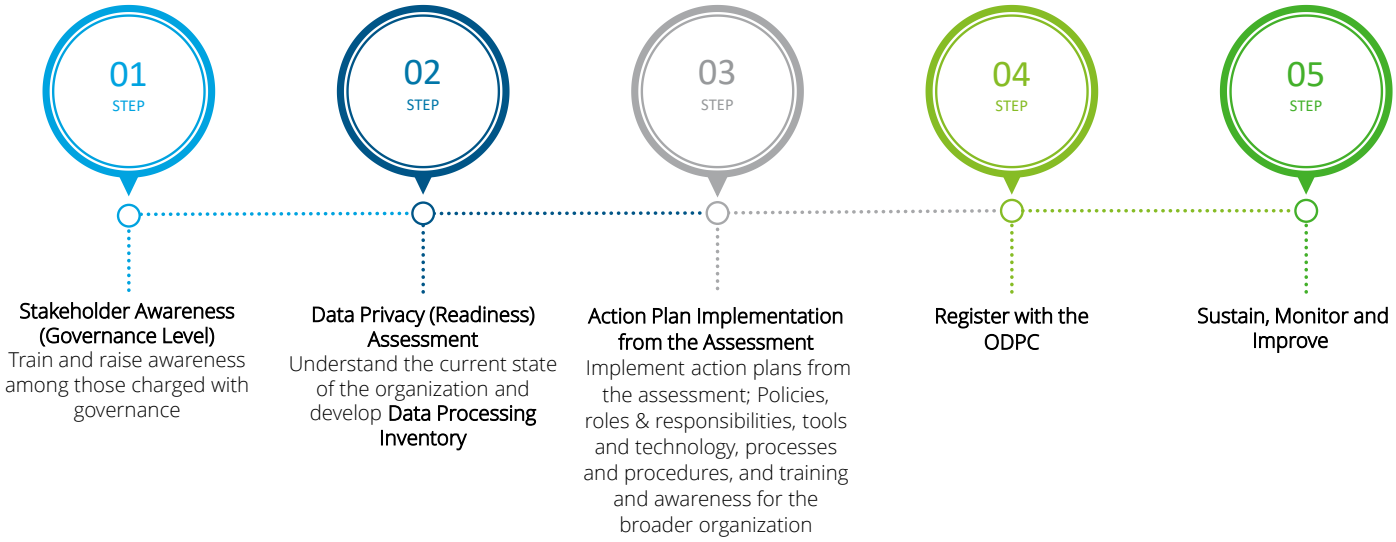
(b) the Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity.

Zambia Data Protection Act 2021



Data protection and privacy

The Journey of Compliance



Here are some additional tips for organizations in Zambia on their journey to Data Protection Act 2021 compliance:

Start early.

The earlier you start your compliance journey, the more time you will have to implement the necessary changes.

Get buy-in from senior management.

It is important to have the support of senior management in order to successfully implement a data protection and privacy program.

Involve all stakeholders.

Data protection and privacy is everyone's responsibility. It is important to involve all stakeholders, including employees, customers, and suppliers, in your compliance journey.

Take a risk-based approach.

The Data Protection Act 2021 requires organizations to take a risk-based approach to data protection. This means that you should focus your resources on the areas where the risks are highest.

Keep up to date with the latest developments.

The Data Protection Act 2021 is a new law, and there are still some areas of uncertainty. It is important to keep up to date with the latest developments in data protection and privacy law in Zambia.

Deloitte's Approach to Data Protection

Approach - Actions to take to prepare for the Data Privacy Regulations

Based on a comprehensive DPA readiness roadmap, a tailored transformation program helps organizations prepare in the optimal way for the Data Protection Regulations

Strategy
A strong starting point determining high level direction and risk appetite, upon which the organisation builds its privacy organisation.

Organisation and Accountability
Enabling effective implementation of the privacy strategy requires a strong and multidisciplinary privacy organisational structure. This covers the structure of the privacy organisation as well as the role and position of key players, such as the Data Protection Officer. This layer also covers accountability; how to prove compliance?

Policy, process & data
Partnering with the Business to ensure data is protected, governed, managed and utilised effectively in line with the organisation's strategy. Also covers technological challenges such as data access requests, data retention, right to be forgotten, breach notification and international and 3rd party data transfers.

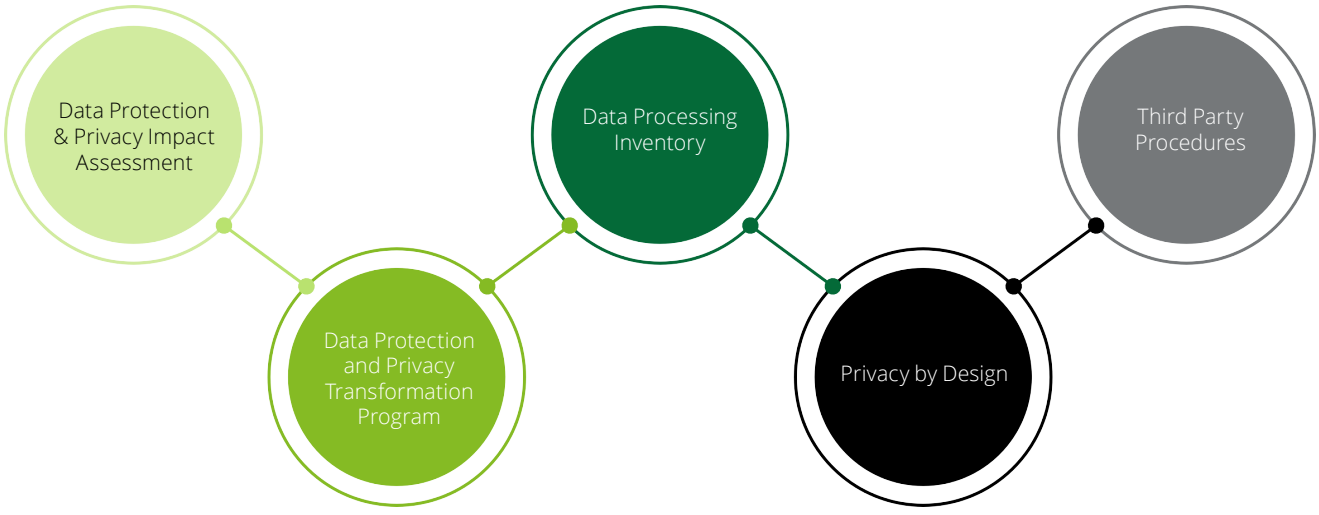
Communication, Training, Awareness
Creating a high level of organisational awareness on privacy ensures that the organisation's employees know and follow the rules.

Privacy Operations
Embedding privacy into the organisations project methodology. This is done by efficient and practical guidance during conception of a new or changed product or service (Privacy by Design) as well as assessing new and existing systems following the established Privacy Impact Assessment method. Also covers audit guidance and readiness for certification programs and adherence to code of practice in data protection and privacy.

Processing Inventory
A processing inventory is a fundamental element of any privacy program and will be a mandatory requirement following the DPA.

Approach – Actions to take

Actions to take to prepare for the Data Protection Act (DPA) and other Data Protection Regulations



Contacts

Anthony Muiyuro
Partner, Risk Advisory
Email: amuiyuro@deloitte.co.ke
Tel: +254 719 039 262

Urvi Patel
Partner, Risk Advisory
Email: upatel@deloitte.co.ke
Tel: +254 711 584 007

Brian Sitamulaho
Associate Director, Risk Advisory
Email: bsitamulaho@deloitte.co.zm
Tel: +260 975 146 209

Deloitte.