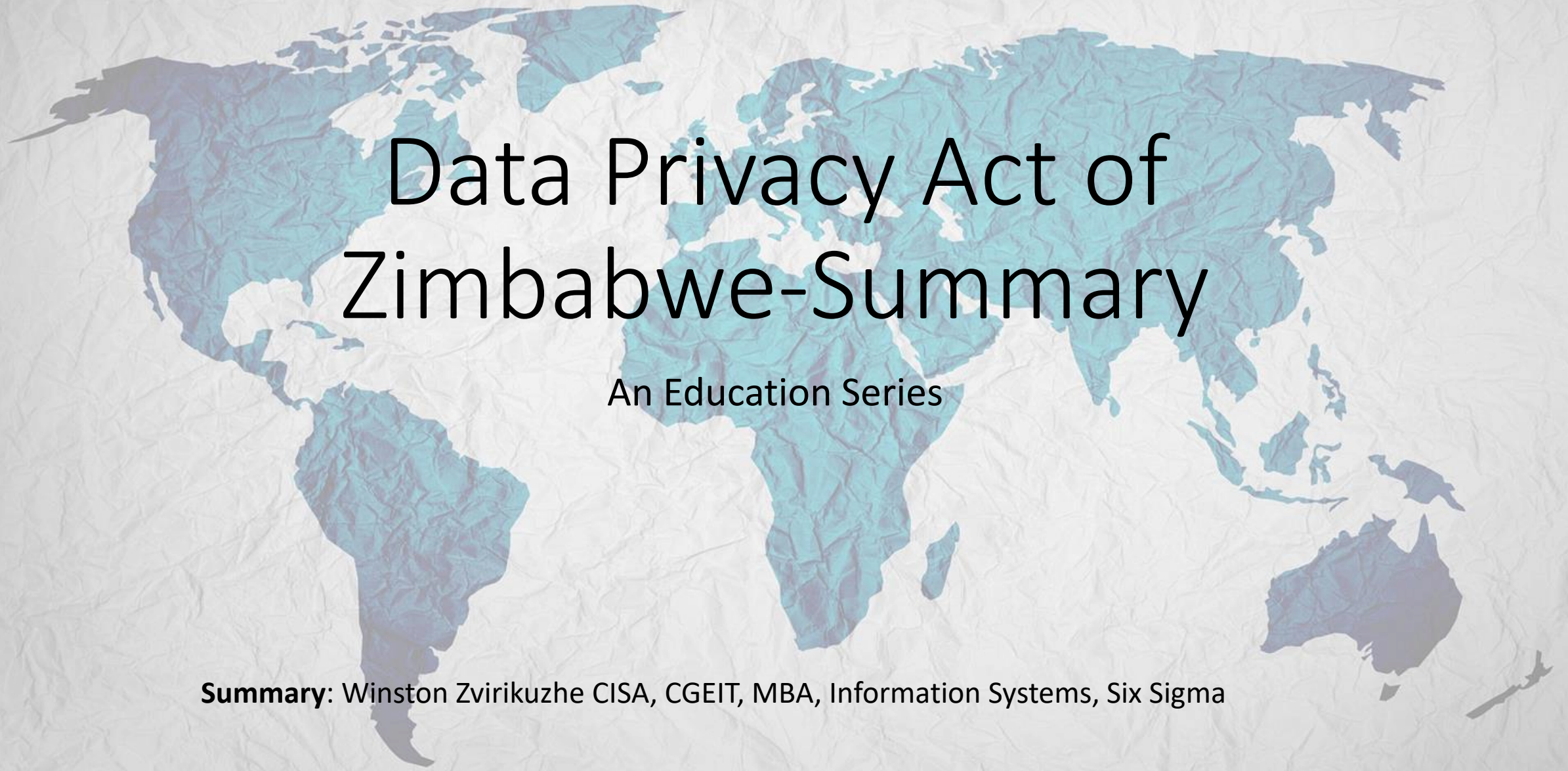


Data Privacy Act of Zimbabwe-Summary

An Education Series

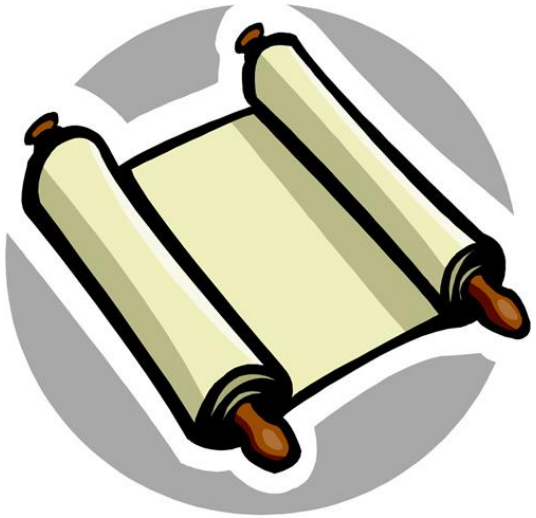
Summary: Winston Zvirikuzhe CISA, CGEIT, MBA, Information Systems, Six Sigma

Disclaimer Warning

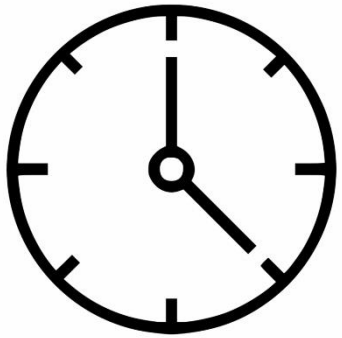
This presentation is meant for education and awareness purposes only and is in no way meant to be a substitute for the Act, legal interpretation or an authority on the law. It is advised to obtain a copy of the Act and receive appropriate guidance on any subject with regard to data privacy

Breaking it Down-ACT

- An Act to provide for data protection with due regard to the Declaration of Rights under the Constitution and the public and national interest;
- To establish a Data Protection Authority and to provide for their functions;
- To create a technology driven business environment and encourage technological development and the lawful use of technology;
- To amend sections 162 to 166 of the Criminal Code (Codification and Reform) Act [*Chapter 9:23*] to provide for investigation and collection of evidence of cyber crime and unauthorised data collection and breaches, and to provide for admissibility of electronic evidence for such offences;
- To amend the Interception of Communications Act [*Chapter 11:20*] to establish a Cyber Security Centre and to provide for matters connected with or incidental to the foregoing.



1. Declaration of Rights under the Constitution



2. Establish a Data Protection Authority

3. To create a technology driven business environment and encourage technological development and the lawful use of technology

4. Enable investigation, collection of evidence, breach notification and admissibility of evidence

5. Establish a Cyber Security Centre (Amend Interception of Communications Act [Chapter 11:20])

To understand the Act: The Objective

The object of this Act is to increase data protection in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects.

First and Foremost it is a Zimbabwean Act

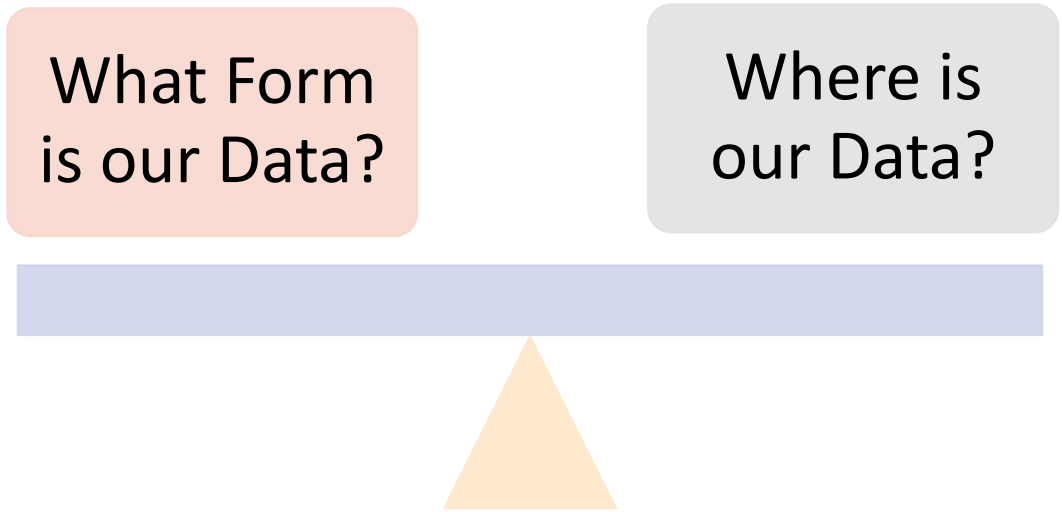
The Topic is DATA

“means any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data;”

Is your Definition of Data Compliant?

Data Questions

- Privacy is a function of what and where?
- Afterwards we can ask who, when and how.



PART III-Quality of Data

How to keep the data quality and responsibility of the controller.

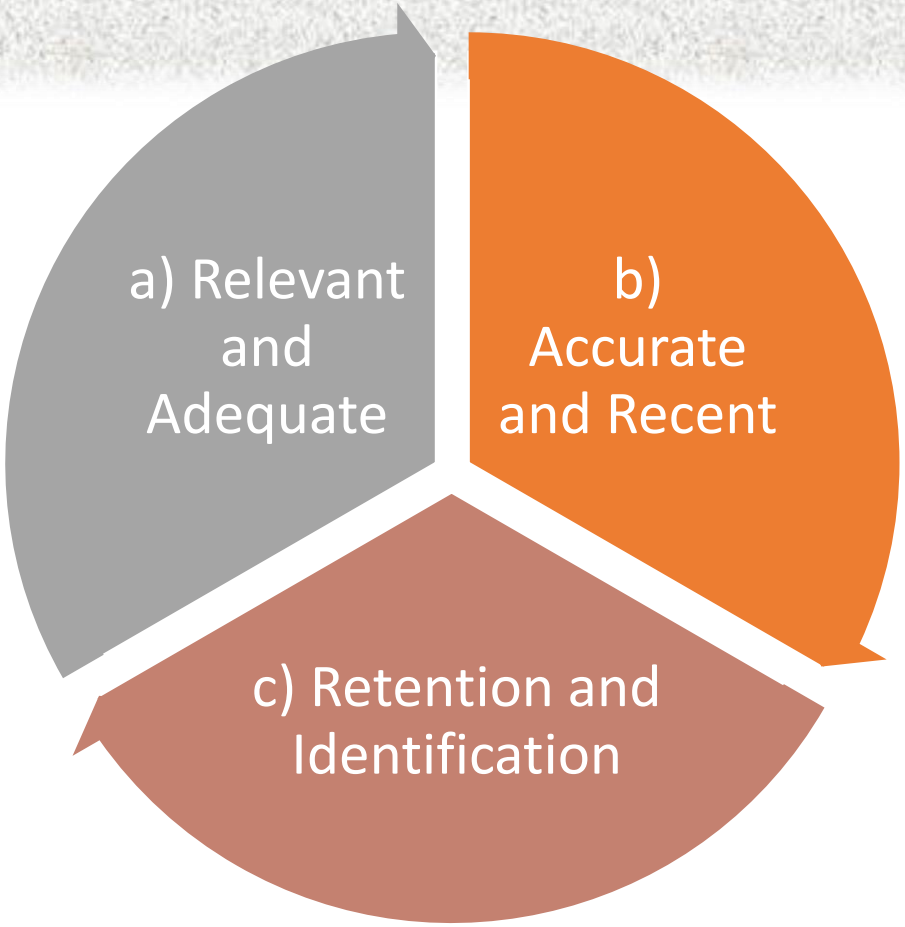
Data Cycle of Quality

(1) The data controller shall ensure that data processed is—

(a) adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;

(b) accurate and, where necessary, kept up-to-date;

(c) retained in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed.



Data Controller Data Quality Responsibility

(2) The data controller shall take all appropriate measures to ensure that data processed shall be accessible regardless of the technology used and ensure that the evolution of technology shall not be an obstacle to the access or processing of such data.

(3) The controller shall ensure compliance with the obligations set out in subsections (1)

PART IV-General Rules on the Processing of Data

How is data processed

Purpose

(1) The data controller shall ensure that data is collected for specified, explicit and legitimate purposes and, taking into account all relevant factors, especially the reasonable expectations of the data subject and the applicable legal and regulatory provisions, that the data is not further processed in a way incompatible with such purposes.

(2) Under the conditions established by the Authority, further processing of data for historical, statistical or scientific research purposes is not considered incompatible.

Personal Information (What it is)

“personal information” means information relating to a data subject, and

includes—

(a) the person’s name, address or telephone number;

(b) the person’s race, national or ethnic origin, colour, religious or political beliefs or associations;

(c) the person’s age, sex, sexual orientation, marital status or family status;

(d) an identifying number, symbol or other particulars assigned to that person;

(e) fingerprints, blood type or inheritable characteristics;

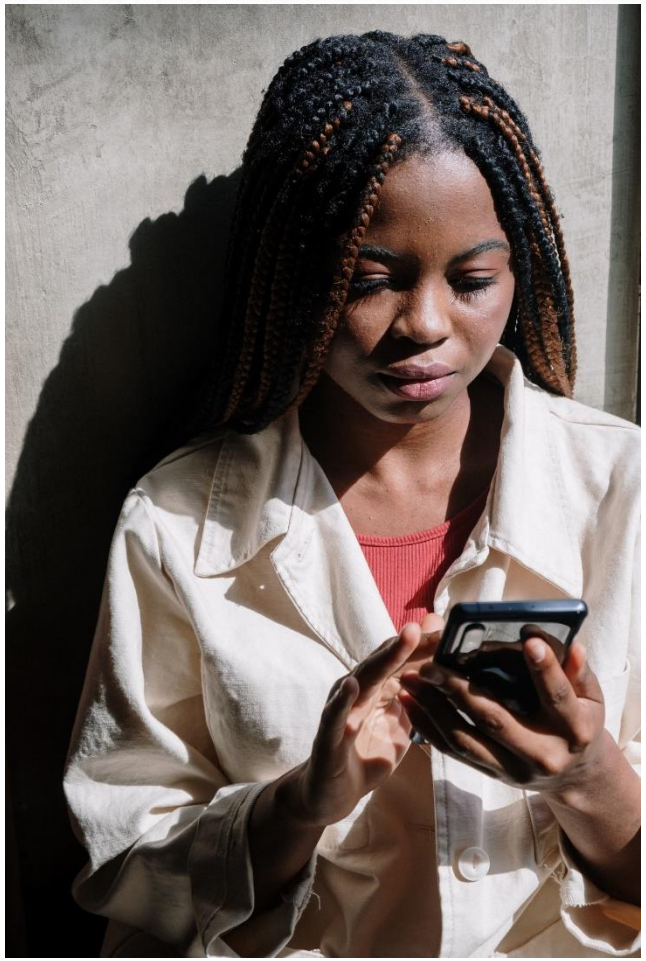
(f) information about a person’s health care history, including a physical or mental disability;

(g) information about educational, financial, criminal or employment history;

(h) opinions expressed about an identifiable person;

(i) the individual’s personal views or opinions, except if they are about someone else; and

(j) personal correspondence pertaining to home and family life;



Personal Information

- Where is personal information being kept and in what form?
  - Cellphones
  - Social media companies
  - Personal laptops
  - Internet cafes
  - Bank cards
  - Restaurants
  - WhatsApp groups
  - Medical records

Processing Non-Sensitive Data without Consent

The processing of non-sensitive data is permitted, without the consent of the data subject, where necessary for purposes of—

- (a) being material as evidence in proving an offence; or
- (b) compliance with an obligation to which the controller is subject by or by virtue of a law; or
- (c) protecting the vital interests of the data subject; or
- (d) performing a task carried out in the public interest, or in the exercise of the official authority vested in the controller, or in a third party to whom the data is disclosed; or
- (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.

The 4 Pillars of Sensitive Information

- "sensitive data" refers to—

(a) information or any opinion about an individual which reveals or

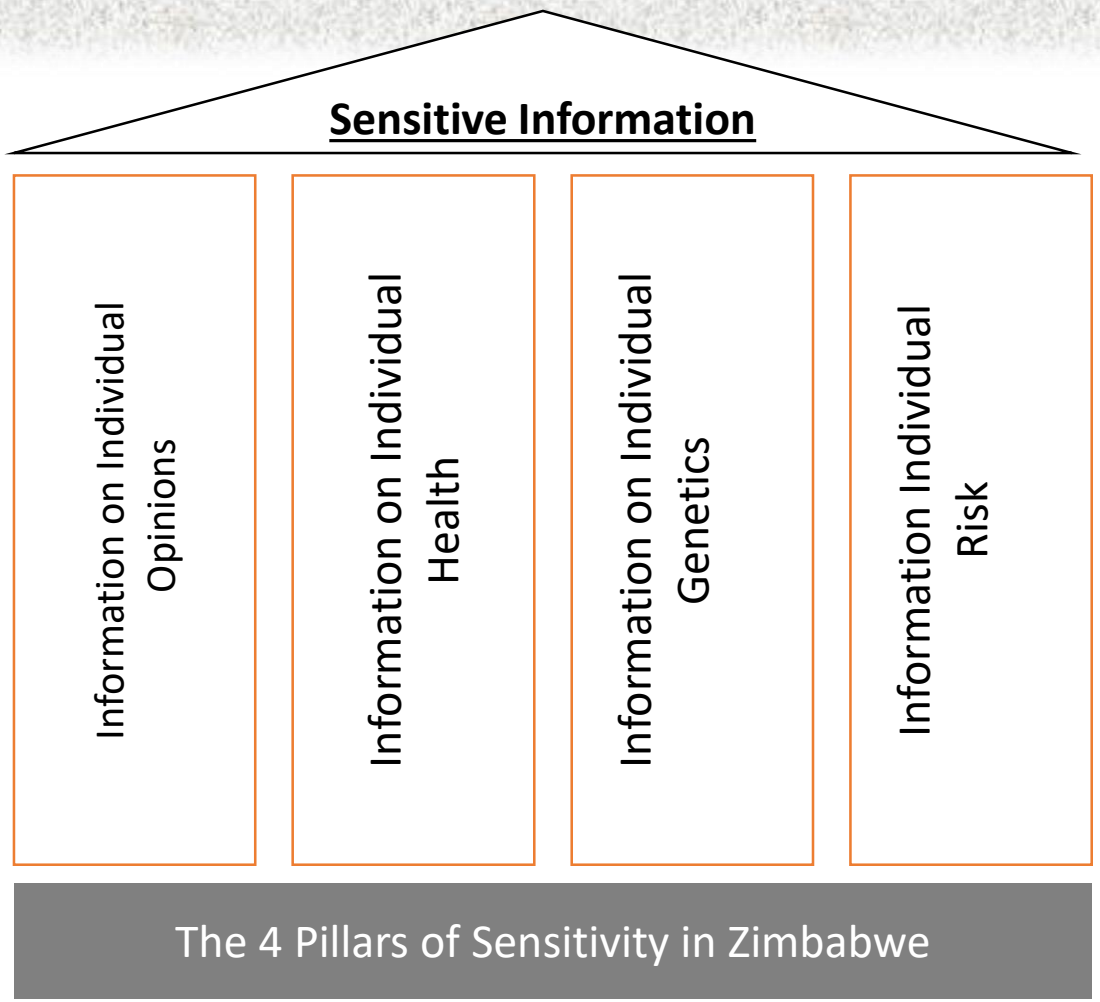
contains the following—

(i) racial or ethnic origin;
(ii) political opinions;
(iii) membership of a political association;
(iv) religious beliefs or affiliations;
(v) philosophical beliefs;
(vi) membership of a professional or trade association;
(vii) membership of a trade union;
(viii) sex life;
(ix) criminal educational, financial or employment history;
(x) gender, age, marital status or family status;

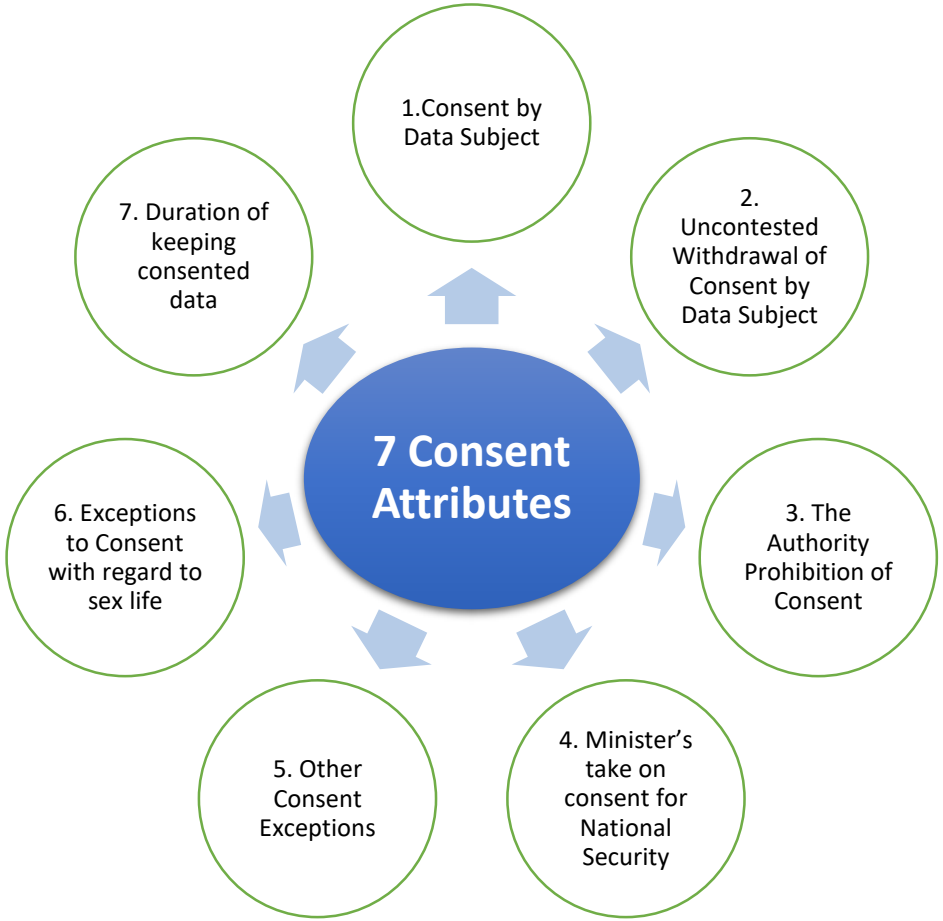
(b) health information about an individual;

(c) genetic information about an individual; or

(d) any information which may be considered as presenting a major risk to the rights of the data subject;



The 7 Consent Attributes-Section 11



PART V-Duties of Data Controller and Data Processor

Identify the duties of the data controller and the data processor.

Duties of Data Controller: R.L.C.R.E.A

Every data controller or data processor shall ensure that personal information is—

(a) processed in accordance with the right to privacy of the data subject;

(b) processed lawfully, fairly and in a transparent manner in relation to any data subject;

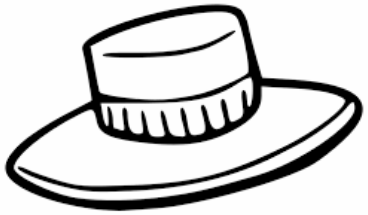
(c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

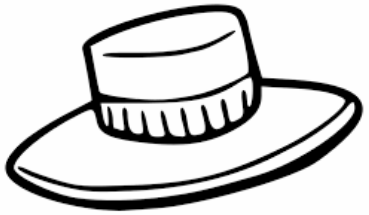
(e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

(f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; and

The 6 Hats of Processing Duties

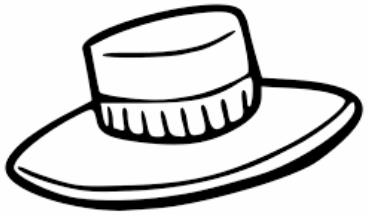


1. Right to Privacy

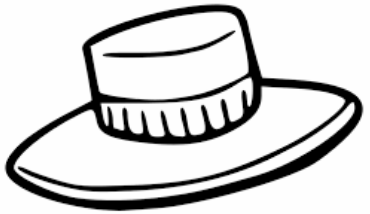


2. Lawfully, fairly and Transparency

3. Clarity



4. Relevance



5. Explainable

6. Accuracy

Duties of Data Controller e.g. Website

Requirements	Self Assessment Questions
(a) processed in accordance with the right to privacy of the data subject;	• Privacy statement?
(b) processed lawfully, fairly and in a transparent manner in relation to any data subject;	• Are cookies transparent?
(c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;	• Are we not using data for advertising?
(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed	• Are collecting the data related to what we need for business?
(e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;	• Can we explain the reason for the data we collect?
(f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; and	• How accurate is our data that we correct?

Rights of Data Subject

- A data subject has a right to—

(a) be informed of the use to which their personal information is to be put;

(b) access their personal information in custody of data controller or data processor;

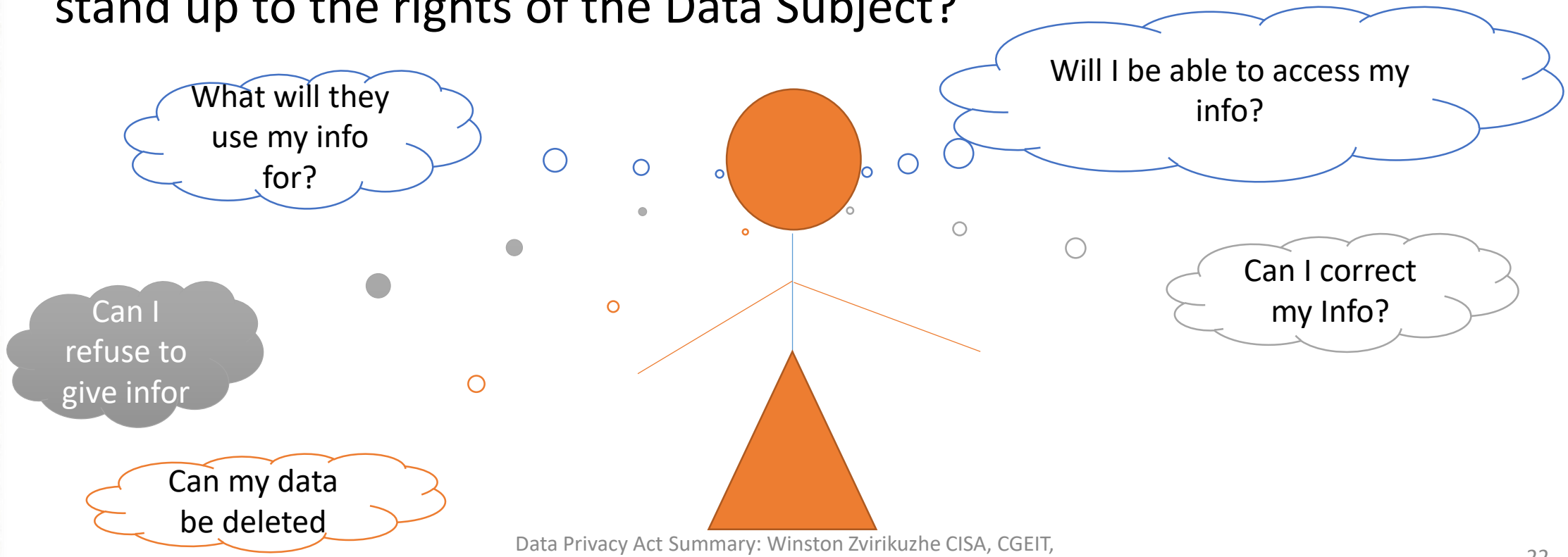
(c) object to the processing of all or part of their personal information;

(d) correction of false or misleading personal information; and;

(e) deletion of false or misleading data about them.

Rights of Data Subject

- Tinashe comes to access your banking website which promotes self registration and processing. How will your business web application stand up to the rights of the Data Subject?



Security

- Define: 1. The security, integrity and confidentiality of the data
- Define: 2. Technological development and the cost of implementation
- Define: 3. Appropriate standards as recommended by the authority
- Define: 4. The data processor who provide sufficient guarantees
- Define: 5. Legal Contracts for safe guard of information

Data Breach Notification

Security breach notification

- The data controller shall notify the Authority “within twenty-four (24) hours of any security breach affecting data he or she processes.

Possible Exemptions from Notification

- Certain categories of Exemption for notification maybe given such as the following
  - (a) taking into account the data being processed, there is no apparent risk of infringement of the data subjects' rights and freedoms, and if the purposes of the processing, the categories of data being processed, the categories of data subjects, the categories of recipients and the data retention period are specified;
  - (b) the data controller has appointed a data protection officer.

Notification Content Checklist

Data Privacy Act Notes		Checkilst Item	Notes
(a) the date of notification and the law or regulatory instrument permitting the automatic processing of data;	1	Date of Notification	
	2	Refering Act for Data Processing	
(b) the surname, first names and complete address or the name and registered offices of the controller and of his or her representative, if any;	3	Controller Contact Details • First Name • Surname • Address operating from(representative address)	
(c) the denomination of the automatic processing;	4	Data Denomination(refer to definition of data)	
(d) the purpose or the set of related purposes of the automatic processing;	5	Data Processing Purpose	
(e) the categories of data being processed and a detailed description of the sensitive data being processed;	6	Data Category	
	7	Sensitive Data Breach identification (refere to sensitive data)	
(f) a description of the category or categories of the data subjects;	8	Data Subject Category	

Notification Content Checklist

Data Privacy Act Notes		Checkilst Item	Notes
(g) the safeguards that must be linked to the disclosure of the data to third parties;	9	Data Disclosure Safeguards	
(h) the manner in which the data subjects are informed, the service providing for the exercise of the right to access and the measures taken to facilitate the exercise of that right;	10	Data Access Communication with Data Subject	
	11	Method of Access	
(i) the inter-related processing planned or any other form of linking with other processing;	12	Other processing related to original processing	
(j) the period of time after the expiration of which the data may no longer be stored, used or disclosed;	13	Data expiry time	
(k) a general description containing a preliminary assessment of whether the security measures provided for pursuant to section 13 above are adequate;	14	Secueity Meaures in Place	
(l) the recourse to a data processor, if any;	15	Action taken	
(m) the transfers of data to a third country as planned by the data controller.	16	Transfer of Data to another country	

PART VI-Data Subject

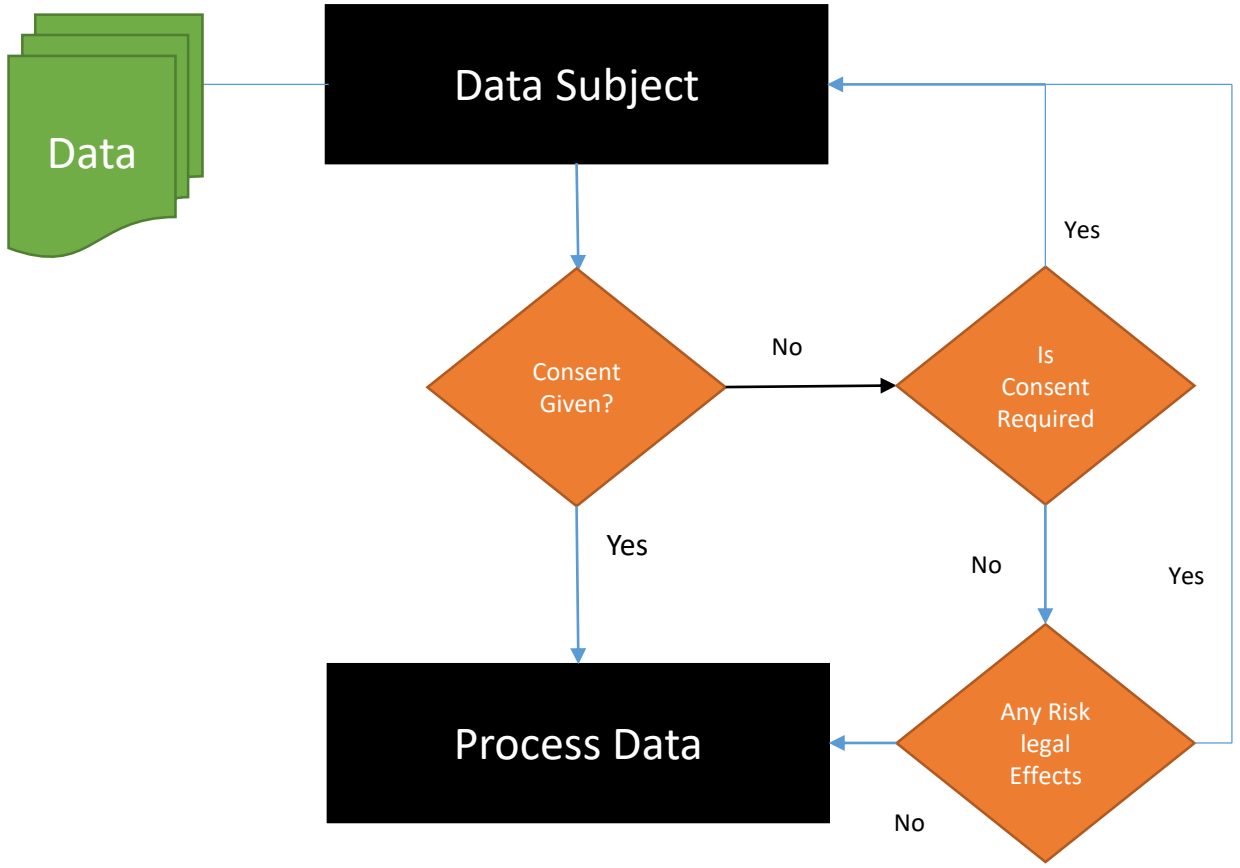
Refers to an individual who is an identifiable person and the subject of data;

Rights of the Data Subject

(1) The data subject shall have the 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.

(2) The right referred to in subsection (1) shall not be applicable if the decision based solely on automated processing is taken on the basis of the data subject having consented to such decision or is based on a provision established by law.



Representation of Data Subject

Representation of data subject who is child

- Where the data subject is a child, his or her rights pursuant to this law may be exercised by his or her parents or legal guardian.

Representation of physically, mentally or legally incapacitated data subjects

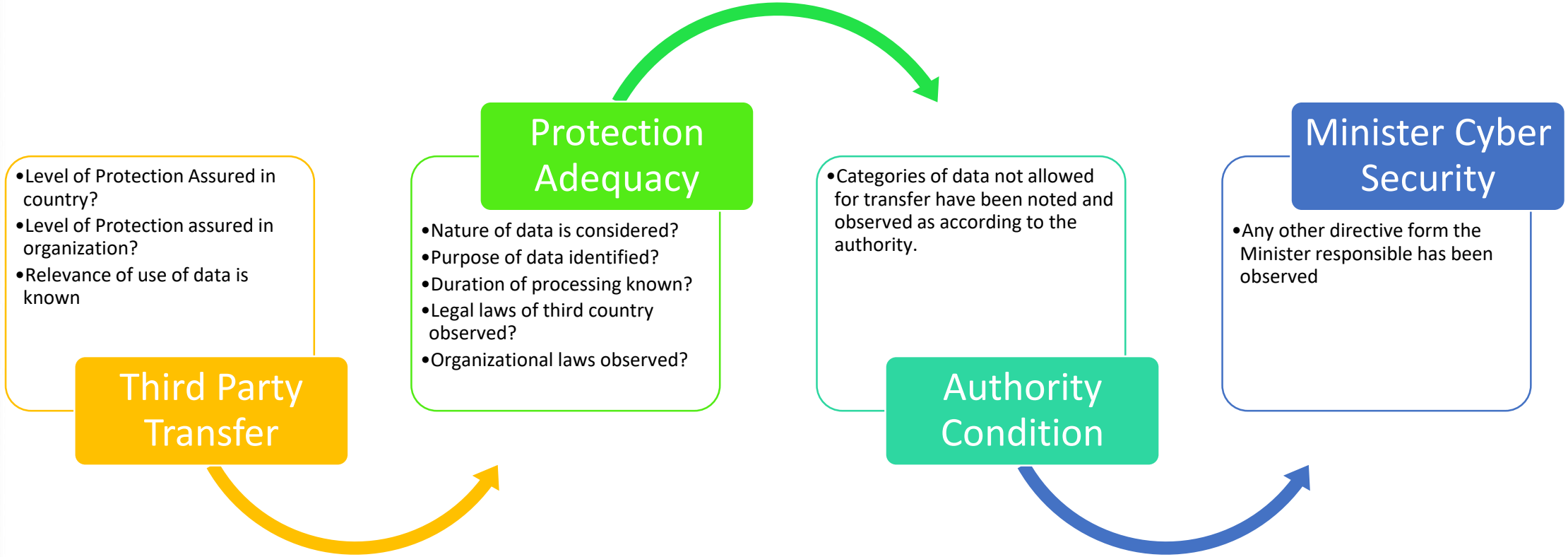
(1) A data subject who is physically, mentally or legally incapable of exercising the rights given under this Act and who is not subject to the provisions of section 26, may exercise such rights through a parent or guardian or as provided for by law or as designated by a Court of competent jurisdiction.

(2) Incapacity as referred to in subsection (1) shall be proven by a physician or a person legally competent to do so.

PAR T VII-Transborder Flow

refers to international flows of data by the means of transmission including data transmission electronically or by satellite;

Data Transfer ACID test



Transfer to country outside Zimbabwe which does not assure adequate level of protection

- (a) the data subject has unambiguously given his or her consent to the proposed transfer;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and a third party in the interest of the data subject;
- (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;
- (e) the transfer is necessary in order to protect the vital interests of the data subject;
- (f) the transfer is made from a register which, according to acts or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the case at hand.

PART VIII-Code of Conduct

Transfer of personal data outside Zimbabwe

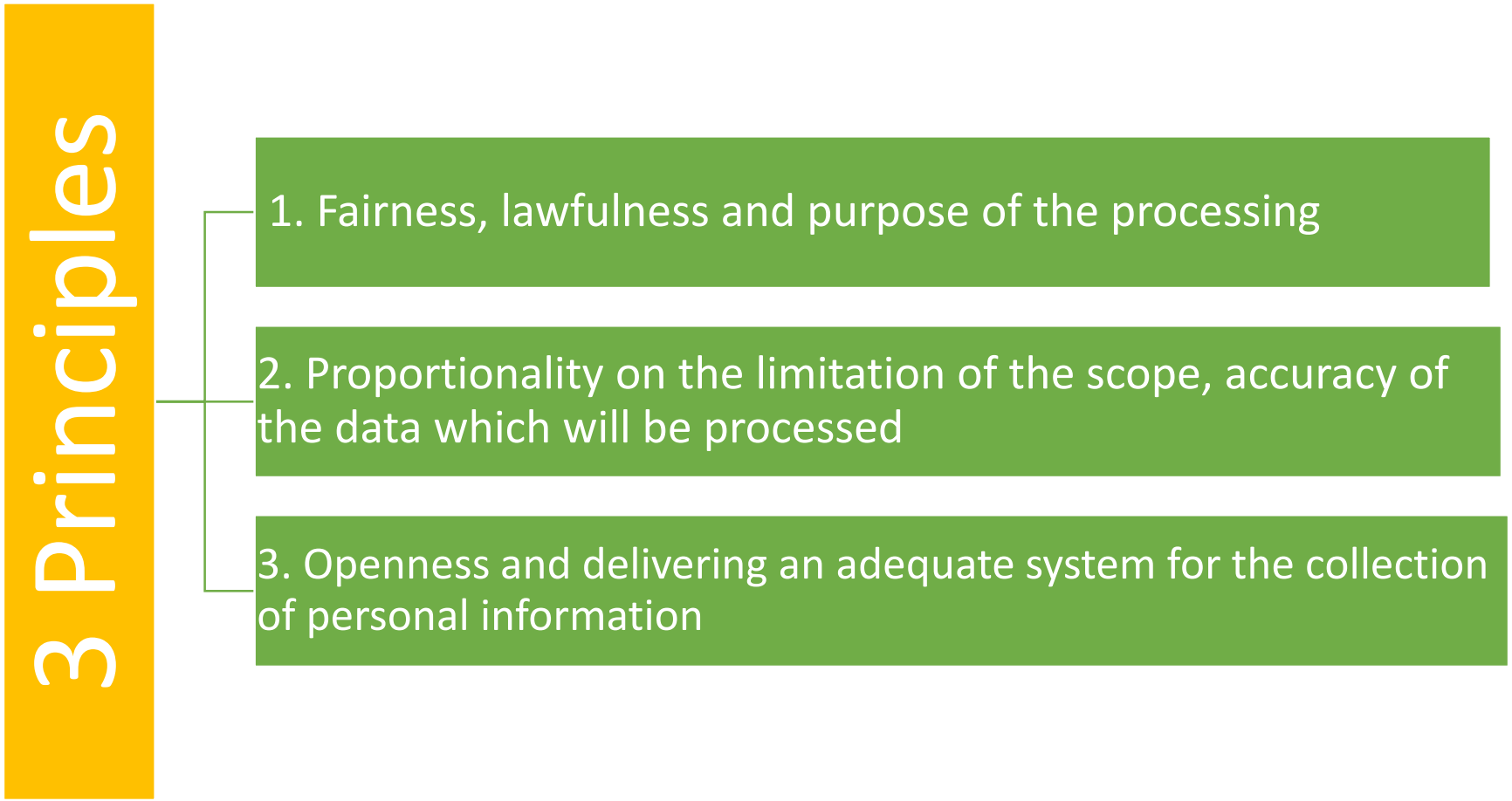
Code of Conduct

- (1) The Authority shall provide guidelines and approve codes of conduct and ethics governing the rules of conduct to be observed by data controllers and categories of data controllers.
- (2) In effecting (1) above, the Authority shall consider trade associations and other bodies representing other categories of controllers who have national codes or have the intention of amending or extending existing national codes and allow them to submit such codes for the approval of the Authority.
- (3) The Authority in considering codes of conduct for approval, shall ascertain, among other things, whether the Codes submitted comply with the provisions of this Act.
- (4) If it deems it fit, the Authority shall seek the views of affected data subjects or their representatives.

PART IX- WhistleBlower

refers to legal provisions permitting individuals to report the behaviour of a member of their organisation which, they consider contrary to a law or regulation or fundamental rules established by their organisation.

The 3 Principles for Whistleblower



Principle Number 3 of Whistleblower

(i) the scope and purpose of the whistleblowing;

(ii) the processing of reporting;

(iii) the consequences of the justified and unjustified reporting;

(iv) the way of exercising the rights of access, correction, deletion as well as the competent authority to which a request can be made; and

(v) the third party who may receive data concerning the informer and the person who is implicated in the scope of the processing of the report;

(vi) the technical and organisational rules;

(vii) rules concerning the rights of the data subject by making clear that the right of access doesn't allow to access to data linked to a third person without his or her express and written consent; and

(viii) the method of notifying the Authority.

Release of Information Balance- Whistleblower

The person who is implicated shall be informed as soon as possible of the

existence of the report and about the facts which he or she is accused of in order to

exercise the rights established in this Act.

The release of information to the person who is implicated may be withheld

in exceptional circumstances.

Definitions of Note

Definitions of Note

"***data controller***" or "controller"—

- (a) refers to any natural person or legal person who is licensable by the Authority;
- (b) includes public bodies and any other person who determines the purpose and means of processing data;

"***data controller's representative" or "controller's representative***" refers to any natural person or legal person who performs the functions of the data controller in compliance with obligations set forth in this Act;

"***Data processor***" refers to a natural person or legal person, who processes data for and on behalf of the controller and under the controller's instruction, except for the persons who, under the direct employment or similar authority of the controller, are authorised to process the data;

Definitions of Note

"***consent***" refers to any manifestation of specific unequivocal, freely given,informed expression of will by which the data subject or his or her legal,judicial or legally

"***data protection officer***" or "DPO" refers to any individual appointed by the data controller and is charged with ensuring, in an independent manner, compliance with the obligations provided for in this Act;

"***code of conduct***" refers to the Data Use Charters drafted by the data controller in order to institute the rightful use of IT resources, the Internet, and electronic communications of the structure concerned, and which have been approved by the Data Protection Authority;


Thank
you