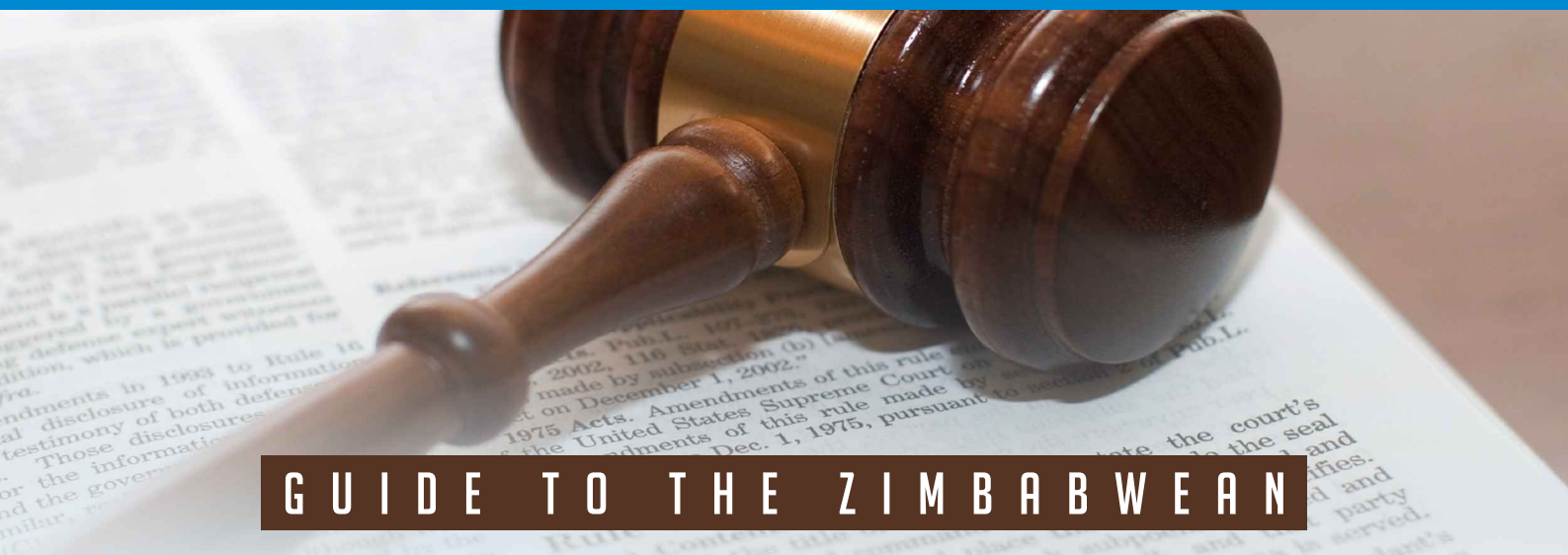
MISA ZIMBABWE



GUIDE TO THE ZIMBABWEAN

CYBER & DATA

Protection Act - 2022

This Guide was commissioned by the Media Institute of Southern Africa Zimbabwe Chapter and was produced by Otto Saki.

ABOUT MISA ZIMBABWE

The Zimbabwe Chapter of the Media Institute of Southern Africa was formed in 1996 and it defends and promotes media freedom, freedom of expression, access to information and the right to privacy in Zimbabwe.

ABOUT AUTHOR

Otto Saki holds a Bachelors' Law degree, and two Masters' in Law degrees with a focus on international human rights law and, in information technology law. Otto has keen interests in global and regional political economy, regional economic communities, health, information technology, and governance. He bears full responsibility of the contents of this guide.

CONTENTS

ABOUT THIS GUIDE

This Guide intends to assist ordinary citizens, data protection advocates, human rights advocates, media organisations and interested individuals in getting a basic understanding and application of the Cyber and Data Protection Act (Act). This guide aims to contribute to the general citizens' awareness of Zimbabwe's data protection legal framework. Contents of the guide are not intended to constitute legal advice. The guide will not include specific legal advice on how to comply with the Act. Compliance requires more than a legal analysis, as there are technical and organisational security requirements for effective data protection. However, some sections might provide basic checklists for ease of understanding and interpretation of the Act's provisions. For comparative regional and international experiences, reference and examples will be drawn from South Africa's Protection of Personal Information Act (POPIA), and the European Union General Data Protection Regulation (GDPR). Other regional standards might also be referenced for their persuasive value.[1] In addition, various court decisions will be referenced as relevant or necessary.

STRUCTURE OF THE GUIDE

For ease of reading, the Guide follows the structure and sections of Zimbabwe's Act. This will allow the Guide's user to read and analyse provisions of the Act against the Guide's commentary.

ACRONYMS

POPIA	Protection of Personal Information Act
GDPR	General Data Protection Regulation
FOIA	Freedom of Information Act
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
DPA	Data Protection Authority
DPO	Data Protection Officer

1 *These include the African Union Convention on Cybercrimes, Data Protection or the SADC Model Law on Data Protection.*

WHAT IS DATA PROTECTION?

In recent times due to the increase in use of technology, data protection has become extremely important. Data protection relates to the lawful use of information concerning or about people. This information is protected as it is recognised that individuals have a right to privacy, in that their information must not be shared, accessed or used without their approval or in the absence of other lawful grounds. The Constitution of Zimbabwe in Section 57, protects the right to privacy and provides that:

> *Every person has the right to privacy, which includes the right not to have - (a) their home, premises or property entered without their permission; (b) their person, home, premises or property searched; (c) their possessions seized; (d) the privacy of their communications infringed; or (e) their health condition disclosed.*

Data protection is primarily concerned with information of a personal nature. Under the Constitution, privacy includes property and premises, and if a search is conducted unlawfully, it would be violating personal privacy, and if personal information is collected, then it will be violating informational privacy. The Constitution does not mention personal data or information, however the mention of 'privacy of their communications' or 'health condition disclosed' indicates protection of personal data. Other rights in the Constitution relevant for protection of data include the right to personal security, freedom of expression and of the media and also the right to administrative justice among others[2].

Data protection intends to give and recognise that every person, including minors through their guardians, can control the use of their personal information, and determine their engagements with other societal actors, such as in conducting business, or work, visiting medical facilities, or internet use. Data protection is also necessary for the conducting of electronic commerce, trade or movement of goods and persons across borders and frontiers.

IS DATA EQUAL TO INFORMATION?

There are differences that have been given on this, for instance in the Act data is defined to mean 'any representation of facts, concepts, **information**, whether in text, audio, video, images, machine-readable code or instructions'. While information in the Freedom of Information Act (FOIA) includes, but is not limited to 'any original or copy of documentary material irrespective of its physical characteristics, such as records, correspondence, fact, opinion, advice, memorandum, **data**, statistics, book, drawing, plan, map, diagram, photograph, audio or visual record, and any other tangible or intangible material, regardless of the form or medium in which it is held'. The Act refers to personal information more than forty times, and only refers to personal data, once. This is not unusual as similar laws use personal information more than personal data. According to Professor Roos the difference between data and information is:

> *"Data are unstructured facts or raw material that needs to be processed and organised to produce information while information is data which has been organised, structured and meaningful to the recipient"* [3]

This is why data without any value addition (structuring, analysing, merging) might have no value on its own.

2 *Section 51 on the right to dignity; s52 on right to personal security; s 61 and 62 on freedom of expression, freedom of the media; s 68 on the right to administrative justice; s69 on right to a fair hearing; s70 on the rights of accused persons; s81 on rights of children protection from sexual exploitation*

3 *Roos A 'Data Privacy Law' in van der Merwe DP, Roos A, Pistorius T, Eiselen GTS, & Nel SS (ed) 'Information and Communications Technology Law' 2 ed (2016) 367-368.*

DATA PROTECTION AND HUMAN RIGHTS PROTECTION

Even though information about people or data is useful for other purposes, the fundamental reason why data protection laws exist, is to protect the rights of a data subject as human rights. In that regard, the preamble to the Act refers to the Constitution's Declaration of Rights. In addition, the judiciary and policy makers are required in terms of the Constitution to take into account international law when interpreting the Declaration of Rights.

Section 46 (1) of the Constitution provides that:

> *When interpreting this Chapter, a court, tribunal, forum or body*
> *(a) must give full effect to the rights and freedoms enshrined in this Chapter;*
> *(b) must promote the values and principles that underlie a democratic society based on openness, justice, human dignity, equality and freedom, and in particular, the values and principles set out in Section 3;*
> *(c) must take into account international law and all treaties and conventions to which Zimbabwe is a party;*
> *(d) must pay due regard to all the provisions of this Constitution, in particular the principles and objectives set out in Chapter 2; and*
> *(e) may consider relevant foreign law."*

IS RIGHT TO PRIVACY MORE IMPORTANT THAN OTHER RIGHTS?

The Constitution provides for freedom of expression under Section 61, while Section 62 promotes access to information. These provisions are further protected in the FOIA which stipulates the conditions and circumstances when information including personal information can be legally accessed.

The Act's application must therefore take into account the FOIA provisions. These laws must not be interpreted as conflicting, but as reinforcing one another. For instance, POPIA's purpose states that this 'includes balancing the right to privacy against other rights, particularly the right of access to information'.[4] While this Act has no equivalent provisions, this can be inferred as part of interpretation and enforcement of the rights. The rights are not in hierarchy and courts are required to balance the conflicting rights.

In the case of A v B Plc on the interpretation of Article 8 on the right to privacy and Article 10 on the right to freedom of expression of the Human Rights Act, the European Court of Human Rights observed the importance of striking a balance.

4 *POPIA section 2.*

Lord Woolf noted:

> *. . . . There is a tension between the two articles which requires the court to hold the balance between the conflicting interests they are designed to protect. This is not an easy task, but it can be achieved by the courts if, when holding the balance, they attach proper weight to the important rights both articles are designed to protect. Each article is qualified expressly in a way which allows the interests under the other article to be taken into account* [5].

In short, the right to privacy which incorporates the right to the protection of personal data must be balanced against the other rights and in particular access to information, and freedom of expression. The right to access to information and freedom of expression are important constitutional rights for transparency and accountability.

The protection of privacy is the basis of data protection. Access to personal data is not allowed unless certain conditions have been satisfied. With freedom of expression and access to information especially information held by the state, such information would be accessible unless other reasons prevent that access. There is a small but important difference; right to privacy starts from denial of access to protect individual privacy unless individual consent or some other reason exists; right to access and freedom of expression, starts from access and then moves to denial or preventing access if that is unwarranted or a material breach of privacy.

Q QUESTION

Do you think data protection must be viewed as a human right? If not, how else can it be viewed as and how can it be protected?

IS THE ACT THE ONLY LAW?

The Act does not state that it is the primary and only law on data protection in Zimbabwe, meaning that there might be some other relevant laws on data protection. Indeed, there are other laws that regulate collection and processing of specific types of data but might not provide better protection. For instance, the Postal and Telecommunications Act allows for collection of subscriber data information or personal call records; Banking Act records personal financial information; Interception of Communications Act authorises the collection or interception of communication information; the National Registration Act authorises the collection of personal identification information for issuance of national identity records such as birth certificates or passport. And this information is usually collected and stored in public databases.

WHEN, AND WHERE IS THE DATA PROTECTION ACT APPLICABLE?

The Act under Section 4 provides that the 'Act shall be interpreted as being in addition to and not in conflict with the Protection of Personal Information Act'. There is no Protection

5 *[2002] 2 All ER 545 5.*

of Personal Information Act in Zimbabwe, and this might be a drafting error or demonstration of intent to pass the Act.[6] Therefore, in interpretating the provisions of the Act, one must always take an approach that advances a higher level of data protection consistent with the Constitution and any other relevant international treaties and conventions. However, one might suggest that if any other laws are inconsistent with the provisions of the Act, then the Act prevails if it provides better and higher protection as long as that is not inconsistent with the Constitution.

South Africa's POPIA provides under Section2 (a) and (b) respectively that:

> *This Act applies, subject to paragraph (b), to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object, or a specific provision, of this Act…If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Chapter 3, the extensive conditions prevail*[7].

WHERE IS THE DATA PROCESSING TAKING PLACE?

Territorial Principle

The Act under Section 4 introduces a territorial scope of application of the Act. The Act is applicable if data processing is 'carried out in the context of the effective and actual activities of any data controller'. The Act requires that if data controller is not established in Zimbabwe, then a representative must be appointed in Zimbabwe [8]. This mean that any entity that processes Zimbabweans' personal data must designate a representative in Zimbabwe. The meaning of effective and actual activities of the data controller requires additional guidance. Actual activities of the data controller might be defined to mean an activity that is connected between the reason for existence of the data controller and the data processing in question. The two must be related. The GDPR territorial scope applies if the data controller has an establishment that economically supports the data processing carried out by the main company[9].

Establishment Principle

The Act in Section 4 (2) introduces the establishment principle allowing for the real exercise of data processing activity through some arrangements either of a temporary or permanent nature of the data controller. This principle also provides for choice of law depending on where the data controller is established. For the Act to apply, the data controller need not be permanently established in Zimbabwe.

6 *Even it was not an error, then the Cyber and Data Protection Act provisions might have to change to incorporate this proposed law.*
7 *POPIA section 3(2)(b).*
8 *This provision if widely interpretated sets the stage for legal liabilities for internet-based platforms.*
9 *European Court of Justice, Google Spain C-131/12.*

The meaning of established must be construed wider than being registered, legally incorporated or some physical, or virtual presence[10]. The EU case law and European Data Protection Board guidance on meaning of "in the context of the activities of an establishment" must not be interpreted restrictively[11]. On the other hand, the existence of an establishment within the meaning of the GDPR should not be interpreted too broadly[12].

WHEN IS THE ACT ENFORCEABLE?

The Act came into force the day it was gazetted. This means that compliance is immediate and therefore everyone concerned or conducting data processing must endeavour to comply with this law, within a reasonable period. This approach while intended to avoid gaps in regulatory enforcement of data protection, creates difficulties in compliance, oversight and implementation. The enforcement of POPIA was in stages, and had transitional provisions to allow individuals, companies and government sufficient time to put in place the required operational mechanisms[13]. Equally, under POPIA, the data protection Authority, the Information Regulator, required sufficient time to put in place necessary structures, funding and human resources[14].

WHAT DATA IS PROTECTED UNDER THE ACT?

The data protected is of any person; a natural person, meaning that the person should be living, and identifiable or identified as a person. Information of deceased persons is personal data but not considered as personal information for processing purposes and therefore not protected at the same levels as that of a living and identifiable individual.

In South Africa for example, POPIA Section 6(1) provides that information collected for individual personal use or family use is not considered personal data for purposes of compliance with POPIA. Zimbabwe's Act is silent. Further POPIA Section 7 excludes personal information that is being processed 'solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.'

The EU GDPR article 2(c) on material scope provides that the GDPR provisions does not apply when the processing of personal data is 'by a natural person in the course of a purely personal or household activity'. In that regard, while the Act is not explicit, the trend has been that data for personal use or family use is not covered as that does not constitute processing.

10 *GDPR recital 22. The "[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."*

11 *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018;*

12 *WP 179 update - Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, 16th December 2015*

13 *POPIA section 114.*

14 *Zimbabwe, POTRAZ as data authority was already in existence, and functional at the time of gazetting of the Act.*

QUESTION

Should personal data only be limited to identifiable living natural persons? What happens to personal information of deceased persons?

TYPES OF DATA CONTROLLERS AND PROCESSORS	
Data Controllers	**Data Processors**
Public	Media, government agencies; utility companies
Internet	Social media sites; search engines
Medical	Hospitals; pharmacies; medical professionals
Financial/Insurance	Insurance firms pension funds, banks
Telecommunications	ISP, MNO
Retail	Online stores; airlines, credit card companies
School	Universities: academic records
Labour	Trade Unions or Professional Associations

KEY DEFINITIONS

The Act has several terms and definitions that are essential for the proper understanding of what is protected, what is lawful and unlawful processing and what constitutes personal information or personal data. These definitions are consistent and similar to those in other laws such as the GDPR and POPIA. Section 3 of the Act provides for most definitions.

Consent

For personal information to be collected, the individual concerned must agree, either directly or indirectly through their guardian if minors or legally incapacitated, or if not consenting then some other legal and lawful grounds must authorise the processing of personal information. Consent has many attributes, and it must be:

- unambiguous, meaning no doubt of what the data subject intends
- clear affirmative action not only ticking boxes
- freely given by a capable individual or their representative
- freely given, not coerced or due to external pressure
- obtained on true information not on false or inaccurate information
- specific and informed

Data Controller

This is a natural person or legal person who is approved to process personal data. To explain this, an illustration will assist. Chad Gore owns a private company, Gore Technologies, providing digital and technology services including biometric data collection, facial recognition technologies and internet services. Chad Gore can be a data controller for purposes of offering his services. If the Zimbabwe Electoral Commission (ZEC) engages Gore Technologies to process voter registration information, Chad Gore, while a controller for other purposes (internet service provider), ceases to be a controller for purposes of implementing the arrangement with ZEC. Then, ZEC becomes the data controller.

The controller determines the purpose for the data collection, but the duties of how the collection and any technical measures can be delegated to another entity. A data controller determines the type of data and the use of the data, but company collecting is not allowed. **The controller determines the lawfulness of the data collection.**

Data Processor

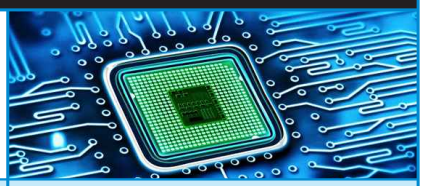
Using the scenario above, Gore Technologies once engaged by ZEC to collect information, becomes a data processor. Gore Technologies is not determining the use of the information collected, but can recommend data collection tools, for instance, which biometric reader works better or what information storage system are required to secure the information. Chad Gore might be engaged in their individual capacity or with Gore Technologies as the company since he is a sole proprietor.

A data processor can also be an individual under the employment of a company. For an entity to be considered a data processor it must meet two minimum elements:

- It must be a separate legal entity or individual or organisation with respect to the controller.
- The processing of the personal data must be on behalf of the controller.

The data processor must not exceed their mandate as this might make them a data controller or introduce **joint data controllership.**

The above is not an exhaustive list of distinguishing a data controller from a data processor but gives a sense of whether one is a controller or processor. The duties of data controller listed in Section 13 of the Act assists to determine whether one is a controller or processor. **The overall control of the purpose for collection and means of processing of the personal data distinguishes a controller from a processor.**

CHECKLIST CONTROLLER AND PROCESSOR	
	
Controller (ZEC)	**Processor (Gore Technologies)**
Decides to collect	Receives instructions to collect
Decides the data purpose	Receives the data from someone else
Decides the type of personal data	Directed to collect from who
Decides who data subject is	Directed type of data to collect
You gain, benefit from collecting	Not aware of collection purpose
Does a legal duty exist, contract	You have no data disclosure Authority
You make decisions based on data	Cannot decide on data storage
You have control on data processing	Cannot decide on data end product
You decide when data is destroyed	You are separate from instructor

Data Subject

The Act defines a data subject as 'an identifiable person and the subject of data'. **The person from whom data is collected is the data subject.** The individual must be an identifiable individual, who is identifiable based on the personal information collected. If one accesses the collected personal data and is not able to identify an individual or a person, then the information is not personal data. This is non-personal information or data. However, collected non-personal data may identify an individual when the information is combined with other details. The information becomes personal information. Identification of a data subject can also be direct or indirect using any of personal information such as numbers, mental, economic or other physical attributes[15].

WHAT IS PERSONAL INFORMATION?

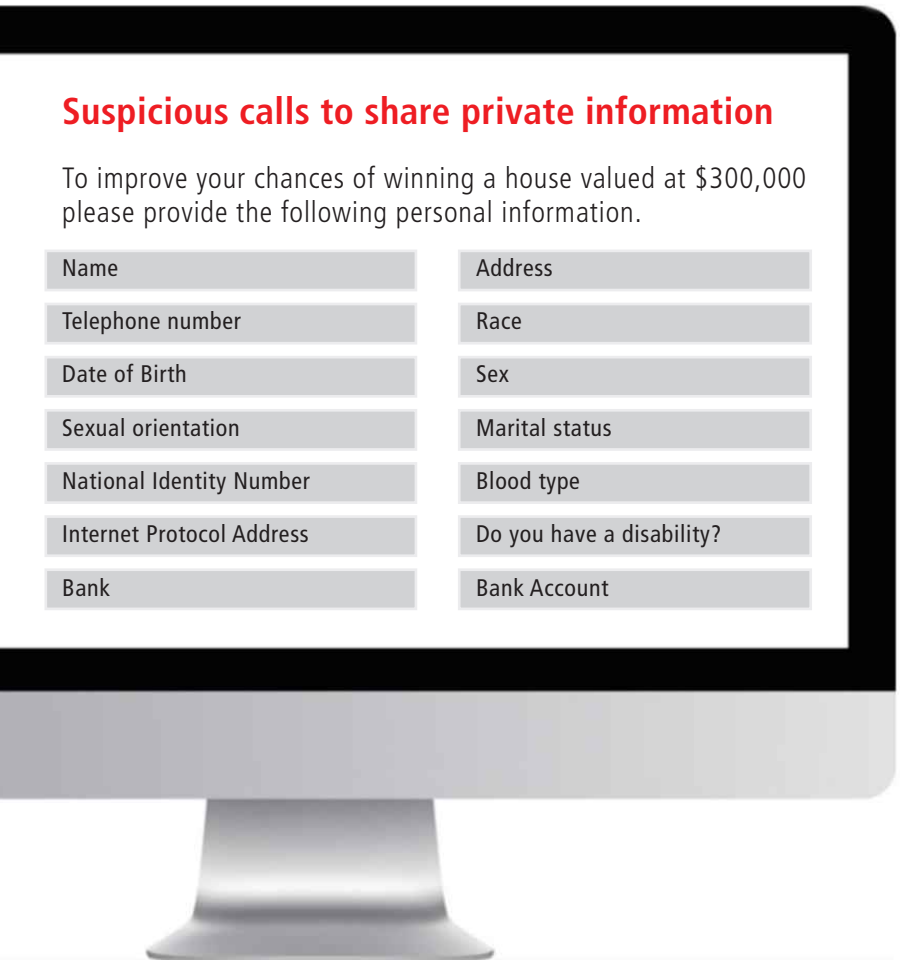
The Act provides for what constitutes personal information relating to an identifiable data subject, and this includes[16]:

- the person's name, address or telephone number
- the person's race, national or ethnic origin, colour, religious or political beliefs or associations: stating that the person was African, without sharing their name does not identify a data subject, of course it might raise other issues of concern such as racial profiling or discrimination
- the person's age, sex, sexual orientation[17], marital status or family status
- an identifying number, symbol or other particulars assigned to that person: if assigned a particular number such as national identity number; or patient number in hospital this is personal information. A number can include your internet protocol address
- fingerprints, blood type or inheritable characteristics: these are unique characteristics that identify an individual or a group of individuals such as a family

15 *POPIA data subject means the person to whom personal information relate.*

16 *POPIA defines personal data means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person. The major difference is the existing juristic person. The Data Protection Act does not cover legal persons as data subjects. This might be problematic as sometimes natural persons might be legal persons for instance sole proprietors or company owners.*

17 *Sexual orientation is different from same sex marriages. The law does not criminalise being attracted to someone of the different sex or being gender non-conforming*



- information about a person's health care history, including a physical or mental disability: example an individual's medical records at Parirenyatwa Hospital or with your local medical health provider, or with Health Worker.
- information about educational, financial, criminal or employment history: records kept at the University or High School; records kept at your bank; records of employment with your trade union or employer
- opinions expressed about an identifiable person; statements that disclose identity of a person.
- the individual's personal views or opinions, except if they are about someone else
- personal correspondence pertaining to home and family life: communication of any kind of a personal nature, written or electronic

The definition of personal information in Act is different from that in the FOIA, in that the FOIA appears to cover more areas of personal information, and also defines personal information not to include information about an individual who has been dead for more than 20 years.

Identifiable

Personal information is that information that should make it possible to identify an individual, meaning the individual is identifiable or identified. However, it is possible that the information is not directly identifiable, but can also be indirect such as a dynamic Internet Protocol address. Dynamic IP address are not fixed but have attributes that allow for indirect identification such as the user billing information[18].

Relates to

The information might be personal information but if it doesn't relate to a data subject then it is not protected personal information. 'Relates to' is subjective and contextual. Therefore, data controllers must take into account factors such as the purpose of collected information; the content of the information among other factors. Purposes of data collection might make information personal information for a different controller but not for others.

WHAT IS SENSITIVE DATA?

There is a category of personal information that is considered sensitive or sensitive data or sensitive personal information. This data refers to information of specific type or class whose disclosure can lead to specific targeted harms against the data subject.

18 *Benedik v. Slovenia, 2018, §§ 107-108.*

The harms can be in the following form:

- physical harms
- economic harms
- reputational harms
- psychological harms
- autonomy harms
- discrimination harms
- relationship harms[19]

These harms are not confined to disclosure of sensitive data but even to general personal data.

The disclosure of sensitive personal information might lead one or more harms, and even harming others associated with the data subject. Sensitive personal information or data means information that presents a major risk to the data subject if the information is processed without satisfying certain requirements at law.

CLASSIFICATION OF SENSITIVE DATA	
Data Type	**Specific harms**
Racial or ethnic	Relationship, physical, economic or psychological
Political opinions	Discrimination, relationships
Political party membership	Disclosure that you support a party
Religious beliefs/affiliations	Relationship, economic, relationship harms
Philosophical beliefs	Discriminated or harmed based on ideas
Trade union or professional	physical or discrimination, economic harms
Sex life	Discrimination, relationships, and psychological
Criminal records, education	Discrimination, relationships, and psychological
Financial employment history	Discrimination, relationships, and psychological
Gender, age, family status	Relationship, discrimination
Health or genetic information	Discrimination, economic harms and relationship harms

Processing

The definition of processing is

"Any operation or set of operations which are performed upon data, whether or not by automatic means such as obtaining recording or holding the data or carrying out any operation or set of operations on data, including-(a) organisation, adaptation or alteration of the data; (b) retrieval, consultation or use of the data; or (c) alignment, combination, blocking, erasure or destruction of the data".

This definition means that when data is collected from an individual, there are means and ways that are used to make that data relevant or usable. For instance, it can be recording of your cell phone number in a database; or it can be correction of your home address with the local council who are not sending bills or are sending erroneous readings of bills; it can be the destroying of COVID-19 test results and associated diagnosis used for travelling purposes by a medical laboratory. The Act doesn't define what automatic processing is but mentions automatic data processing in several sections including Section 25.

In comparison, POPIA under Section 3(4) defines automatic to mean that there is equipment that is capable of operating automatically in responses to instructions given for purposes of processing information.

19 *Danielle Keats Citron & Daniel J. Solove (2022).*

Most data protection laws seem to focus on this aspect, as it relates to digital or computerised processing, however, non-automated processing is still used. Non-automated relates to use of manually collected information in documents and may be part of a filling system or records or manual archives.

The word 'processing' is very wide to cover anything that a data processor, or data controller can do with personal information or personal data.

Examples of Processing

- Collecting current and historical medical information during COVID-19 testing.
- Recording in public spaces through video surveillance cameras.
- Storing the information in data centres, or storage even in simple formats such a spreadsheet.
- Using of data in making decisions based on data collected for informing policy or interests of the data subject.
- Disclosing whether the public or private disclosure is lawful or unlawful.
- Deleting of the information before or after use or during use, which can also be lawful or unlawful.
- Uploading on internet of personal details to open a webpage or registration.
- Recording of biometrics when issuing digital identity cards or records.
- Registration of SIM cards by mobile telephone operators[20].

WHAT IS A DATA PROTECTION AUTHORITY?

Part II of the Act provides for a Data Protection Authority (Authority). The Act stipulates that the Postal and Telecommunications Regulatory Authority (POTRAZ), is designated as the data protection Authority under Section 5. The Authority is usually an independent, public institution that is capable of enforcing, supervising, and monitoring the application of the data protection law in a country. In some countries, the Authority provides guidance on key issues or approves codes of conducts, among other functions. Section 6 of the Act provides for the function of the Authority. Reading through the functions of the Authority under Section 6, considerable powers have been conferred to POTRAZ. This means that POTRAZ has become a super-regulatory agency, accountable to the Executive[21].

The Act provides for the Authority to be working with different ministries. For instance, Section 6 (d) of the Act requires the Authority to consult the Ministry of Information when submitting court complaints on administrative acts that are inconsistent with the protection of personal information. Equally, the Authority must advise the minister on right to privacy and access to information under Section 6 (e)[22].

Further, the Act provides under Section 11 (4) on processing of sensitive information that the Minister responsible for cyber security and monitoring centre, the Minister of state security and intelligence in the presidency and responsible minister may give directions [to the Authority, data controllers] on processing of sensitive information affecting national security or interests of the state. The independence, and functions of the Authority were taken lightly, however this is an area that leads to certification of a country as not providing adequate protection[23].

20 *Collection of traffic calls and call data is contested as some argue that metadata is not personal data, but data about data.*

21 *Sections 6 -7 of Postal and Telecommunications Act, POTRAZ is presided over by 5 -7 members appointed by the President after consultation with the Minister. The Board in consultation with the Minister appoints a Director General, who is responsible for the day-to-day operations of the Authority.*

22 *The minister responsible is information communication technologies which is the line ministry for POTRAZ.*

23 *This is a longer discussion that cannot be exhausted in this commentary.*

Comparative appointment processes of data protection authorities

In Kenya, the Data Protection Act provides for the position of the Data Commissioner who is appointed after a public open and transparent process with interviews led by the Public Service Commission[24]. A list of the final three candidates is sent to the President in order of merit. Section 6 (4) of the Kenyan Act requires that the President nominates from the list and, with approval of the National Assembly, appoints the Data Commissioner. The data commissioner has a six-year non-renewable term. The Data Protection Commissioner qualifications are provided in terms of the law. The Data Commissioner is an independent office, and reports to the National Assembly annually through the relevant ministry[25]. Procedure for removal from office is clearly stipulated including the grounds such as failure to abide by requirements of leadership integrity.

South Africa has an Information Regulator established under Section 39 of POPIA. The information regulator is an independent office, subject to the constitution and reports to the National Assembly. The POPIA's Section 41 outlines details on the appointment, qualifications and removal of the information regulator. The information regulator consists of a chairperson and four other members. At least one member must be a practising advocate or attorney or a professor of law at a university; or possess any other "qualifications, expertise and experience relating to the objects of the Regulator". The term of office is five years with reappointment eligibility[26]. The Information Regulator is also responsible for processing of access to information requests under the Promotion of Access to Information Act (PAIA)[27].

24 *Kenya Data Protection Act s 6 (1)-(3).*

25 *Kenya Data Protection Act s70 (1)-(3).*

26 *These were part of submissions made to the Parliament of Zimbabwe during the discussions on the Data Protection Bill, by MISA Zimbabwe, and the author made similar submissions to the Portfolio Committee on Media.*

27 *Zimbabwe has a separate body attending to access to information requests under the FOIA. This is not unusual but can create implementation challenges of both laws.*

Q QUESTION

From the above comparative appointment of data protection authorities, is POTRAZ as the data protection Authority in Zimbabwe independent? If so, what are the elements of independence, and if not, how can that be a risk to data protection?

CAN DECISIONS OF THE DATA PROTECTION AUTHORITY BE CHALLENGED?

If anyone is aggrieved by the decision of the Authority in its mandate as a Data Protection Authority, they can approach the courts. The POTRAZ as the Authority is obliged under Section 68 of the Constitution and provisions of the Administration of Justice Act to adhere to procedural fairness, and lawful administrative action. Section 68 (1) and (2) of the Constitution provides that:

> *Every person has a right to administrative conduct that is lawful, prompt, efficient, reasonable, proportionate, impartial and both substantively and procedurally fair…Any person whose right, freedom, interest or legitimate expectation has been adversely affected by administrative conduct has the right to be given promptly and in writing the reasons for the conduct.*

According to the Constitution, an Act of Parliament must give effect to these rights; being the Administration of Justice Act. Section 3 (1) (a) of the Administration of Justice Act provides that:

> *An administrative Authority which has the responsibility or power to take any administrative action which may affect the rights, interests or legitimate expectations of any person shall-act lawfully, reasonably and in a fair manner…*

The Authority is an administrative body as defined in the Administration of Justice Act in that it is a committee or board appointed in terms of the Act and the Postal and Telecommunications Act and further performs administrative power and duties.

Quality of Data

Quality of Data is covered under Part III of the Act. Section 7 of the Act provides for several data processing principles, and these are necessary conditions for processing or collecting of personal information. This Section is also read in conjunction with the definition of data controller and data processor as that helps to understand the data processing principles. Section 7(1)(a) Adequate, relevant and not excessive The data must be adequate, relevant and not excessive, meaning if the data collected is not adequate it will still be personal data but might not be sufficient, and therefore not relevant for the collected purposes. If more data is collected than is required and therefore excessive, it therefore becomes unlawful collection.

Section 7(1) (b) Accurate, and Up to date

Inaccurate data while it might not lead to identification of an individual, might also lead to deprival of benefits to the data subject or specific harms. The data controller has a responsibility to ensure that the data collected is accurate, and up to date. Records that have inaccurate information for instance a voter's roll can impact on one's right to participate in electoral matters, but also the controller. ZEC must ensure that the roll is updated, this duty also extends to the data subject (the voter) to inspect and correct or update details on the voter's roll. Accurate data means that the personal details are correct. **Inaccurate information can be harmful.** For information to be accurate it must be regularly updated, though accurate and updated can exist as separate elements of data processing they are related. Updated means, if a data subject, changes their name, or address, or a record is expunged any database holding the initial information must be updated or reflect the same changes. The duty to update is not entirely of the data controller nor of the data subject, it is a shared duty.

Section 7 (1) (c) Storage Limitation

When collected, the information must allow for the identification of the data subject, and only kept for a necessary period and time to allow the purposes of its collection to be satisfied, unless other reasons exist to keep the data longer.

Section 7 (2) Accessibility of Data and Technical Measures

Data is usually processed using different technological measures. These measures must allow for the data to be accessible, meaning if given to a data subject they should be able to read it, or anyone with lawful access is able to process the data regardless of the technology used.

Section 7 (3) Controller delegated Authority

If any individual is given Authority to collect information for the controller, such as a data processor, they must comply with all provisions under Section 7. This includes people that the data processor has contracted.

DATA PROCESSING PRINCIPLES

Part IV of the Act covers areas of the general rules on processing of data, which include generality; purpose, non-sensitive data; sensitive information; Data Processing Principles. The Act contains several data processing principles as reflected in most national and regional data protection laws[28]. While other laws list the eight principles in clear order, the Act has placed them in different sections, and might not be clearly outlined as data processing principles.

GENERALITY

Section 8 of the Act requires that the Data controller ensures that processing of data is **necessary**, and that data is processed **fairly and lawfully.**

What is the meaning of necessary; fairly; and lawfully?

Necessary: is the data required and if so, what purposes is the data required for. Before processing commences, the data controller must identify the necessity of the data to be processed. In addition, the data collected must not be more than is required. **For instance, if the purpose of the data is for opening a bank account, there is no necessity for asking personal information on data subject's trade union affiliations.**

Fairly: in processing data, the data controller must abide by principles of natural justice which allows for a data subject to know of the decisions made; identity of the data controller; reasons for the data processing. Fairness requires one to consider all different issues in relation on how data processing is handled. Being informed of the data collection and providing consent if required constitutes fair processing[29].

Lawfully: This means that processing must comply with the provisions of the Act. However, lawfulness goes beyond a single law or the Act, but to include the Constitution, other laws for instance FOIA, or if it is sector specific, the Banking Act or the National Registration Act. In addition, lawfulness covers other international obligations and instruments that Zimbabwe has ratified and domesticated.

Do you satisfy only one condition therefore proceed with processing information?

Compliance with one condition is not sufficient. If the processing of data is necessary, it should be lawfully and fairly processed. If it is not necessary, then it cannot be lawful as the information is outside the legal scope of what is required.

PURPOSE

Section 9 of the Act requires that the data controller ensures that data collection is **specified, explicit** and for **legitimate** purposes. Again, to satisfy this provision the data controller must ensure that:

- Specified: The type of data to be collected is known, or clear
- Explicit: The data controller must be clear why they are collecting personal data
- Legitimate: The data controller must indicate what they will use the data for.

In addition to the above, the data controller must:

- document compliance with all the requirements for processing
- meet and comply with the expectations of the data subject as laid out in legal provisions for lawfulness, and fairness

[28] *The GDPR and POPIA lists them as clear conditions of processing. Article 5 of GDPR lays out the principles as follows; lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.*

[29] *See GDPR Preamble, GDPR Article 20.*

What is processing which is 'incompatible with original purpose' mean?

The data controller must ensure that if data is then used for other processes different from the initial reason for collection, that additional use must be compatible with the original collection process. The data subject must ensure that they are not accepting additional uses without reading terms and conditions of services for instance when opening accounts, you might be asked if you accept promotional materials to be sent to your address or credit facilities asking if they can share your details with other loan providers.

ILLUSTRATION OF ORIGINAL USE AND COMPATIBLE USE		
Data Collected	**Original Use**	**Compatible Use**
Nasal fluids	COVID-19 testing	Genome sequencing to trace virus
Cell number	Voter registration	Notifying of your polling station
Educational qualifications	Accreditation	Register of Qualified professionals
Nasal fluids	COVID-19 testing	Trading with medical insurance firms.
Cell phone number	Voter registration	Unsolicited messages by political parties.
Educational qualifications	Accreditation	Selling of third-party training programmes.

However, there other legitimate purposes, which do not need to satisfy the compatibility test. These are usually public interest purposes not the original purpose but will be deemed acceptable if they satisfy conditions issued by the Authority. These conditions include further processing for historical, statistical, or scientific research or archiving purposes. That said, the Authority must include in its conditions for further processing that the information must not be identifiable to a data subject.

ORIGINAL USE	LEGITIMATE USE
Nasal fluids	Scientific medical research of viruses (medical)
Cell phone	Measurement of cell phone coverage (statistical)
Educational qualifications	Audit of professional skills movement (historical)

POINTS TO REMEMBER

While the law prohibits further processing, remember that:

- if the new purpose is compatible with the original purpose, then it's acceptable
- if the data subject agrees or gives specific consent to further processing though incompatible with original collection then it becomes lawful
- if there are legal grounds allowing for further processing in the public interest then such is lawful

Specific, explicit and legitimate processing enables transparency, and accountability and data subject control of personal information processing[30].

The data controller must specify the data before commencing processing. This must be clear. It must not be uncertain or for illegal or unlawful purposes. Further data processing must be compatible with original purposes unless if public interest purposes exceptions apply, or the data subject has consented[31]. **It is also possible that data might have multiple purpose when collected. Then the data controller must for each purpose be specific, meaning compliance with all data processing requirements for each purpose[32].**

30 *Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation 13.*

31 *GDPR art 6(4); GDPR Art 14 (1) (a)-(f); POPIA s12(2)(a) -(f); see Article 29 Data Protection Working Party (203) 24-27.*

32 *Article 29 Data Protection Working Party 'Opinion 03/2013 on Purpose Limitation 12; 16.*

NON-SENSITIVE DATA

Consent is required

Section 10 of the Act provides for conditions of processing of what the Act calls **non-sensitive data.** This is personal information as defined above in Part I of the Act. The section 10 (1) starts off with consent as a condition of processing, for a data subject or consent of guardian of minor.

Consent is required but can be implied

Section 10 (2) of the Act allows for consent not to be specific or explicit, but it can be implied, if data subject is an adult. The implied, does not mean that there are no other grounds to process the data which the adult subject is aware of. This Section introduces a 'legal persona'. This term is not defined in the Act, nor are there any indications of what this means in relation to data processing. This means that other than a natural identifiable data subject consenting, other forms of legal existence such as companies, or trusts can consent to data processing[33].

If Chad Gore (natural person) registers a company Gore Technologies (legal persona, juristic person) the information of Gore Technologies on credit rating is then processed by Credit Rating Bureau, then such information constitutes juristic-personal information. It is not possible to separate Gore Technologies from Chad Gore.

Consent is not necessary

Section 10 (3) (a)-(e) of the Act lists instances were consent, even implied consent is not required of the data subject, natural or legal persona if the information is:

(a) required for criminal offence proof

(b) for compliance with law or controller requirement

(c) for protecting interests of data subject

(d) for public interest

(e) for promotion of the legitimate interests of the data controller or third party unless other fundamental rights exist[34]

Legitimate interests are different and wide. Using the guidance developed for the GDPR, data controller must therefore consider a test of what constitutes legitimate interest as this can be subjective. This test has been used in courts[35] and the three aspects must be satisfied:

- **Purpose test:** are you pursuing a legitimate interest?
- **Necessity test:** is the processing necessary for that purpose?
- **Balancing test:** do the individual's interests override the legitimate interest?

ILLUSTRATION

Chad Gore Medical Scheme wants to process personal data to remove fraudulent medical aid claims on grounds of legitimate interests. First is this in the interests of Chad Gore Medical business interests to ensure that medical aid claims are genuine. Second, if legitimate interest is satisfied, then consider whether processing of that specific personal information is necessary. Necessity asks whether there are other means to achieve the same objective which are less invasive to privacy, for instance, the level of data collected, do you need to know the medical conditions claimed for or you will only need to know the claimed amounts?

33 *POPIA section 1, includes identifiable juristic persons in definition of personal information.*

34 *See GDPR article 6(1)(f)*

35 *Rigas case (C-13/16, 4 May 2017*

Third, if prevention of fraud is a legitimate interest for Chad Gore Medical Scheme, and even other end users, do the individual interests override the legitimate interest. At this stage, the data controller is asking whether the decision is proportionate, or the interests of the data subject, which is the protection of fundamental rights and freedoms, override the data controller's legitimate interests.

Considerations on Legitimate Interest

While these are not exhaustive, a data subject can inquire if these have been met, while data controller must ensure these are satisfied.

- There are no other grounds for processing and legitimate basis is the most relevant.
- There is a record of assessing that legitimate interest is the only relevant.
- The controller or processor has identified the interest and not just vaguely stated.
- The controller has checked that processing is:
  - Necessary and no other way of achieving the result
  - Balancing of interests and that data subject interests are protected but they do not override legitimate interests
  - Proportionate means were used and not to invade into data subject privacy

POINTS TO REMEMBER

From this section, what is important to note that processing of personal information can occur without the consent of the data subject if any other lawful or legitimate ground exists, unless if the other fundamental rights override these provisions. Further, the data controller stating that there are legitimate interests without stating what those are is not enough to constitute a lawful processing.

SENSITIVE INFORMATION

This provision refers to sensitive data under Part I of the Act. Sensitive information requires safeguards as its unlawful collection or processing might result in grave violations for the data subject. There are several options for the processing of sensitive information.

Consent is required

First, consent is required, and it must be explicit, and in writing from the data subject. The data controller cannot process sensitive data without explicit consent under Section 11 (1) of the Act.

Consent can be withdrawn

Further, Section 11 (2) of the Act allows for consent to be withdrawn, at any time free of charge. Even in instances of consent, the Authority is permitted under Section 11 (3) of the Act to refuse the consent to processing of sensitive information.

National Security Sensitive Information

Section 11 (4) of the Act allows the minister responsible[36] for the Act to issue directions on how sensitive information relating to national security or state interests is processed through the Cyber Security and Monitoring Centre.[37] This Section shows that surveillance and monitoring occur, and the sensitive information will be collected.

Consent is not the only condition for processing

Section 11(5) does not require the application of Section11 (1) on consent for controller processing of sensitive information if:

(a) the information is for employment purposes such as complying with tax requirements
(b) the information is for protecting vital interest of data subject e.g., medical emergencies or life threatening should be deemed as vital; or data subject is not capable
(c) the processing is for purposes associated with legitimate activities of the processing institution such as trade unions, political parties, provided the information is not shared with third parties
(d) the processing is for compliance with national security law for instance such as national security locations, fingerprints collection or biometrics access
(e) the processing is for legal claims or defence of claims for instance financial records in a dispute about loans
(f) data subject has already disclosed the sensitive data for instance if medical records were public for health campaigns
(g) data is processed for scientific research; this relates to medical or other sensitive data, but conditions must be put in place such as how to make information not identifiable to a natural person
(h) the processing is authorised by law or other regulation for substantial public interest[38]

GENETIC DATA, BIOMETRIC SENSITIVE DATA AND HEALTH DATA

Section 12 (1) of the Act prohibits the processing of genetic, biometric and health data without written consent as they constitute sensitive data. The Act defines genetic data as any personal information stemming from a Deoxyribonucleic acid (DNA) analysis.[39] Biometric data is not defined in the Act. Under GDPR biometric data means

> *'Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.*

Health data under the GDPR is defined as personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.[40]

The data controller or data processor must receive an express written permission to collect the genetic, biometric sensitive personal data. As part of the data subject's right, consent can be withdrawn anytime, at no cost, Section12(2). It is important to note that consent is not the only ground for processing personal and sensitive information. Section12(3) lists several exceptions to the Section12(1) on written consent.

36 *The minister responsible for the Act means the minister responsible for information and communication technologies.*
37 *The Cyber Security and Monitoring Centre is established through the Interception of Communications Act*
38 *The Act has no definition of substantial public interest. However, substantial public interest should be considered as such if processing is lawful, necessary, and proportionate and there are sufficient safeguards for data protection and privacy.*
39 *This definition is not entirely complete, and the GDPR definition might be helpful. Under GDPR Article 4 (13) and recitals 34, 'genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained'.*
40 *GDPR article 4 (15)*

a) the processing is necessary to carry out the specific obligations and rights of the controller in the field of employment law
b) the processing is necessary to comply with national security laws
c) the processing is necessary for the promotion and protection of public health, including medical examination of the population
d) the processing is required by or by virtue of a law or any equivalent legislative act for reasons of substantial public interest
e) the processing is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving his or her consent or is not represented by his or her legal, judicial or agreed representative
f) the processing is necessary for the prevention of imminent danger or the mitigation of a specific criminal offence
g) the processing relates to data which has apparently been made public by the data subject
h) the processing is necessary for the establishment, exercise or defence or legal rights
i) the processing is required for the purposes of scientific research
j) the processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment for the data subject or to one of his or her relatives, or the management of health-care services in the interest of the data subject, and the data is processed under the supervision of a health professional

As health data is sensitive personal information, it must be processed under the responsibility of a health care professional, under Section 12 (4) again unless if one has consented to processing by non-health care professional or if the purpose is for prevention of imminent danger or for mitigation of a specific criminal offence. A health care professional is defined in the Act, as any individual determined as a health care professional in the Health Professions Act [41]. In addition, conditions for such processing must be specified by the Authority. This means that guidelines will be produced to be used by health care professionals as provided under Section 12(5) of the Act.

EXERCISE

For each of the exceptions to written consent for processing sensitive data, list any examples that would meet these lawful exceptions.

Source of Health Data

Health data must be collected from the data subject, unless if the data subject is incapable of providing the data. This might mean that health data might be collected from other sources such as medical insurance or attending health care professionals and past medical records. Section 12 (6) of the Act does not give what other sources for health data might be used.

QUESTION

Can a media report of a data subject's medical data be considered as any other source for purposes of Section 12 (6) of the Act? Must this collection comply with purpose specification?

Professional Secrecy, Confidentiality

Health care professionals are bound by oath and secrecy. Section 12 (7) of the Act reinforces this requirement of ethics and confidentiality. This means they will not disclose or handle the health data contrary to the Health Professions Act and laws which they are sworn to uphold. Section 12 (8) of the Act requires that health data be associated with unique identifiers that do not disclose the data subject. For instance, the medical institution cannot use your national identity number for purposes of identifying your medical records. While the use of other identifiers with health data records or information is permissible, this is subject to authorisation of the Authority under Section 12(9) of the Act.

41 *Chapter 27:19.*

QUESTION

Can individuals from government departments seconded to assist with vaccinations, or testing for COVID-19 be defined as health care professionals? Can these individuals be bound by the provisions of the Health Professions Act, or guidelines issued for Health Professionals?

DUTIES OF DATA CONTROLLER

Part V of the Act is titled duties of data controller and data processor. To safeguard data privacy and protection of data subject rights, data controllers and data processors must be accountable in the performance of their duties. Under Section 13 of the Act, processing of personal information shall ensure that:

(a) processing is in accordance with the right to privacy of the data subject, meaning the first priority is privacy preservation before pursuit of data controller interests
(b) processing is lawful, fair, and transparent for the data subject: these are fundamental provisions of data processing
(c) processing of data is for explicit, specified, and legitimate purposes and not further processed for original incompatible processes
(d) processing is adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed
(e) collection is only where valid explanation is given for family and private affairs
(f) personal or sensitive data must be accurate, and inaccurate personal data is erased or rectified without delay;
(g) data or information must be kept in eligible format but not beyond the purposes of the collection, meaning that any further storage should be anonymised

DATA SUBJECT RIGHTS

As indicated, data protection laws are about protection of individual data subject rights as provided in the Constitution or other international instruments that protect the right to privacy, and equally, right to freedom of expression, or access to information. Under the GDPR, there are over eight data subject rights; being the right to information; right of access; right to rectification; right to erasure; right to restriction of processing; right to data portability[42], right to object; right to not be subjected to automated processing.

Some of the rights are covered in the Act, but not in sequence. Section14 of the Act provides for some of the rights as follows:

(a) right to be informed: requiring that the use of the personal information is known to the data subject
(b) rights to access personal information in custody of data controller or processor: this is part of enforcing privacy right but also access to information[43]
(c) right to object to processing, allowing for data subject to object or refuse to have their personal data processed
(d) right to correction of false or misleading information, requires that if information is incorrect, inaccurate then it must be corrected
(e) right to deletion of false or misleading data[44]

42 *This is not reflected in any parts of the Act.*
43 *One might argue that this right includes right to information and access. Right of access to information is controlled by another act, the Freedom of Information Act. This means that the Data Protection Authority and the Freedom of Information Authority (or Commission) must develop clear and shared processes on how the information will be accessed.*
44 *The use of false and misleading information is an unusual addition in the Act. The information might be true but when collected for a different purpose and used for incompatible purposes then it becomes unlawful but not necessarily false.*

Exception to the Data Subject Rights

There are exceptions to enforcement of these rights. For instance, on the right to be informed, the data controller or representative might be unable to comply or it is not necessary. These are some of the possible situations:

- The data subject is already aware of the information and therefore needs to provide it, only provide what they do not know.
- If information is obtained from another source, then data controller can demonstrate that they already had the information.
- When providing the information is impossible especially when you have no contact details of the data subject.
- When providing the information to the data subject would constitute disproportionate effort.
- If providing the data subject with the information might hinder ongoing processes such as public health responses or in investigations.
- If the information is required by law, and the third-party holder of such information must disclose such information.
- If you are compelled by virtue of professional and confidentiality requirements under the law for instance with health or financial or taxation information.

For each of these circumstances, the data controller must clearly provide enough explanation for accountability purposes. If reliance on existing law, that law must clearly state the obligation to process, and the data controller must reference the specific law. The data controller must document all these decisions and include additional information in a privacy statement or policy that might stipulate the conditions for when exceptions apply.

EXERCISE

Looking at the data subject rights, what other exceptions do you see as justifiable and permissible?

DATA COLLECTED FROM DATA SUBJECT

When collecting data from the data subject, the data controller or data processor must provide certain information which makes it possible for the data subject to exercise their rights. Section 15 of the Act provides for these as necessary requirements for processing. A data controller must develop a set of questions to satisfy themselves of compliance with these provisions as part of their duties. This information must be provided on collection, unless if there is proof that the information has been provided. The data controller must satisfy themselves that the data subject has this information, and this includes:

- the name and address of data controller or data processor or their representatives
- the purposes of the processing
- the rights of data subject that exist, including right to object
- the lawful basis of processing, and implications of failure to comply
- the recipients or categories of recipients of the personal data

POINT TO REMEMBER

The data controller or data processor must provide this information in a concise, clear and easily understood information, meaning that the forms must not have unclear statements or be ambiguous. Simple and clear language is expected, otherwise this will be inaccessible and not compliant with the Act.

DATA NOT COLLECTED FROM DATA SUBJECT

The data controller or data processor or their representative are required to communicate with the data subject if the data is not collected directly from the data subject unless if the data subject is already in receipt of that information in terms of Section 16 of the Act. To comply with this Section the data controller must provide:

- the name and address of data controller or data processor or their representatives
- the purposes of the processing
- the lawful basis of processing, and implications of failure to comply
- the rights of data subject that exist, including right to object if information is obtained for direct marketing purposes, the data subject shall be informed
- the categories of data concerned
- the recipients or categories of recipients of the personal data
- the right to access or rectify the personal data

Disproportionate Effort to Comply

This situation arises when compliance with providing the data subject with information when data is indirectly collected from the data subject might be impossible or difficult. The Act provides in Section 16 (2), that if informing the data subject requires disproportionate effort especially for data collected for statistical, historical, scientific or public heath protecting and promotion, or if data is recorded or provided in terms of the law, then Section 16 (1) will not apply. **The meaning of disproportionate in the Act means effort that is so labour intensive as to consume a lot of time, money and manpower resources.**

This exception should not be arbitrarily invoked. The data controller must take steps to satisfy themselves that there are no other less costly means to comply with informing data subject. Therefore, the data controller must consider all their duties under Section 13 of the Act:

- The lawfulness, fairness and transparency.
- Provide information on your privacy policy to allow individuals some knowledge that processing might be taking place.
- Consider conducting a data privacy impact assessment to understand the risks[45].

POINT TO REMEMBER

While the data controller might have a legitimate interest or other reason to justify data processing or invoke exceptions, those exceptions might be overridden by the data subjects' fundamental rights and any processing has taken account of the individual right to privacy and that the least invasive approach has been used. The data protection Authority is required to set guidelines or conditions for application of these exceptions, in terms of Section 16 (3) of the Act.

45 *This is required under the GDPR Article 35 (1) if processing is likely to result in a high risk to the rights and freedoms of individuals. The GDPR lists examples of what might constitute high rights under Article 35 (3). For instance, processing of information for public monitoring (surveillance) or large-scale data or automated data processing profiling.*

AUTHORITY TO PROCESS

Section 17 of the Act requires that processing of personal information is done only as the controller instructs. This means that data processor, or their representatives must not process if not under instruction to do so by the controller. Authority to process constitutes part of security and safeguards for personal data.

SECURITY

Section 18 of the Act provides for the security measures that must be implemented to safeguard personal data[46]. Security, integrity and confidentiality of data is the responsibility of the data controller or data processor or their representative. For POPIA, this is the safeguard principle which the data controller or the responsible party must comply with[47]. Section 18 (4) of the Act requires that appropriate technical and organisational measures are taken to protect data. The Act requires under Section 18 (5) that appropriate measures be implemented. The Section does not define what constitutes appropriate measures, and there are several, as long as they can satisfy that sufficient safeguard where and are in place.

Examples of appropriate measures may include:

- minimising the processing of personal data. This does not mean, not processing, but processing data which is required and necessary
- pseudonymisation[48] of the personal data to make identification impossible without additional information
- allowing the data subject to monitor the data processing through invoking any of their data subject rights
- use of preventative concepts such as privacy by design or privacy by default
    - o **Privacy by design** is an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle[49].
    - o **Privacy by default** compels the data controller to ensure that the data processes is necessary to achieve specific purpose; data minimisation and purpose limitation are consistent with privacy by default.
- Encryption of the data and making sure that the data is easily available when a technical incident occurs[50].
- Physical measures such as building of secured rooms for data servers or use of strong access passwords, and two factor authentication.

When deciding on the appropriate technical measures, the Act requires under Section 18 (5) that the data controller takes into account costs, state of technology, nature of data, and any potential risks to processing. The Authority can under Section 18 (6) issue guidance on appropriate standards for certain types of data or data categories. This guidance might also be issued as industry wide guidance for certification purposes for instance to banks, or insurance or medical institutions. Every data controller must satisfy themselves that the data processor they have appointed have sufficient technical and organisational measures to protect the data and that such policies are being adhered to.

46 *There are drafting numbering errors on this section. Its starts from 18 (4) to 18 (8). For purposes of this commentary*

47 *POPIA s19(2)*

48 *GDPR Article 4 (5) 'the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information provided that additional information is kept separately and is subject to technical and organisational measures…'.*

49 *GDPR Article 25 (1)-(2)*

50 *Availability of information on demand is important and can be ensured if there are sufficient technical measures at appropriate levels.*

ADDITIONAL CHECKLIST ON TECHNICAL MEASURES

- An information security policy which is implemented.
- Conducting regular review of policies and improvement to meet industrial levels and changes.
- Conducting training and skills up-tooling for all the individuals involved in data processing.
- Conducting regular testing and review of the measures to ensure that they are effective, such as conducting network penetration tests.
- Implementing industry certified standards or those approved in a code of conduct by the data protection Authority.
- Enforce the technical measures on any data processor, and this should be reflected in the contracting agreement between data controller and data processor s18(8).

NOTIFICATIONS

The Act provides for two forms of notification to the data protection Authority by the data controller. The first is security breach notification, and second is notification of processing through automated means.

Security Breach

In the event of an unauthorised destruction, negligent loss, unauthorised alteration or access and any other unauthorised processing of the data, the data controller must notify the DPA within 24 hours of any security in terms of Section 19 of the Act. Under POPIA notification to the data subject is required unless if their identity cannot be established or if the notification will impede investigations by concerned authorities[51]. The Authority must provide guidelines that specify the content of the security breach notification such as:

- Nature of the security breach.
- Number of data subjects affected if possible.
- Categories of personal data breached.
- Measures taken to mitigate or resolve the breach.
- Measures to prevent or mitigate adverse effects of the breach on data subjects.

Automated Processing Notification

Section 20 (1) of the Act requires the data controller to inform the Authority of any automated data processing that might be taking place, wholly or partly. The exceptions under Section 20 (3) are when the information is for purposes of keeping a register for public use by operation of law or when the data controller is pursuing a legitimate interest. Further exemptions can be decided by the Authority from notification if Section 20 (4) is complied with and:

- There is no apparent risk of infringing data subject rights and freedoms.
- If the data processing purpose; categories of data being processed; categories of data subjects; categories of data recipients; and data retention period are specified.
- If the data controller has appointed a data protection officer.

WHO IS A DATA PROTECTION OFFICER?

The data protection officer (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'. The appointment of a DPO is important in public institutions, or institutions that process large scale personal data. Section 20(5) of the Act requires data controller to notify the Authority on the appointment of the DPO whose qualifications must meet the criteria set out under Section 20(6) and conduct specified tasks.

51 *POPIA s22(3).*

DPO Appointment Considerations

- Is the DPO independent, capable and qualified for this position; remember the DPO must report to senior management and has independence to ensure compliance of the Act by the data controller;
- Is DPO able to deal with requests made to the data controller; the DPO must be involved in all critical processes relating to protection of personal data so that they are able to respond to requests.
- Is the DPO a staff of the organisation; if so then they must be well resourced to play this role and must not be penalised for either whistleblowing or in the performance of their duties.
- Is the DPO accessible, known and contactable; this is important as the DPO will be the contact person for data subjects, data controller or data representative officials/employees or for the Authority.

CONTENT OF NOTIFICATION

If required to notify the Authority on certain automated data processing provided under Section 20, the data controller must meet the requirements of Section 21(1)(a)-(m). The notification must include information that makes it possible for the Authority and the data subject to exercise their oversight and enforcement of their rights respectively. The notification must include:

- the date of notification and the law authorising the automatic data processing
- the contact details of the data controller or processor of their representative
- the denomination of the automatic processing
- the purpose or the set of related purposes of the automatic processing
- the categories of data being processed, and a detailed description of the sensitive data being processed
- a description of the category or categories of the data subjects
- the safeguards that must be linked to the disclosure of the data to third parties
- 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
- the inter-related processing planned or any other form of linking with other processing
- the period of time after the expiration of which the data may no longer be stored, used or disclosed
- a general description containing a preliminary assessment of whether the security measures are adequate[52]
- the recourse to a data processor, if any
- the transfers of data to a third country as planned by the data controller (see Section on data transfers)

The Authority is allowed to prescribe other information to be included in the notification, as per Section 20 (2) of the Act. Furthermore, the Authority can inspect and assess security and organisational measures before processing or transfer of the data commences. This provision is important as this process constitutes a data privacy impact assessment (DPIA), designed to establish the level of safeguards and privacy protection for the data subject. The Act empowers the Authority to inspect and assess security and organisational measures taken by data controller.

AUTHORISATION

The processing of certain classes of personal data might require specific authorisation before processing commences. The Authority under Section 22 of the Act is empowered to establish the various categories of data that requires authorisation based on the specific risks to the fundamental rights of the data subject.

52 *Section 13 does not seem to speak to issues raised here. This might be a drafting error.*

OPENNESS OF PROCESSING

The Authority is required under Section 23 to have openness in processing of personal data. This is considered as the ***openness principle***. First, Section 23(1) requires that a register, meaning a record of all activities of automatic data processing carried out by data controllers be kept. The data controllers must inform the Authority of these cases. The register according to Section 23 (2) must contain all information contained in Section16(1). The register will be available for inspection by the public as determined by the Authority, as provided under Section 23 (3). This provision is important to enforce data subject rights to be informed. Further, Section 23 (4) allows Authority to compel data controllers to disclose any processing of information that might have taken place even if the data constitutes exempted data.

The POPIA requires under the openness principle that all documentation associated with data processing be kept as they can be subject to information requests under promotion of access to information laws[53].

ACCOUNTABILITY

At the root of data protection, is the protection of the interests of the data subject and preservation of personal privacy. This is considered as the accountability principle of data processing. Section 24 promotes accountability of the data controller in all material respects of the Act. The data controller has duties mentioned under Section 13, and in addition to that Section 24 (1) (a) emphasises that the data controller shall 'take all the necessary measures to comply with the principles and obligations set out in this Act'. Similarly worded provisions are found in the GDPR and POPIA[54]. The GDPR **Articles 5 (1) and 5 (2):**

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

While under **POPIA Section 8**

The responsible party [data controller] must ensure that the conditions set out in this Chapter [POPIA], and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

Further, the Act under Section 24 (1) (b) compels that data controllers must 'have the necessary internal mechanisms in place for demonstrating such compliance [24 (1) (a)] to both the data subjects and the Authority in the exercise of its powers.' The responsibility for compliance and the burden of proof rests with the data controller to satisfy the data subject and the Authority. The accountability principle, in summary provides for the data controller to be ***responsible for compliance*** with provisions of the Act. Therefore, every data controller needs to be compliant. Lastly, the data controller must be able to demonstrate or prove that such mechanisms for compliance are in place.

53 *POPIA s17.*

54 *The main difference with the GDPR is that these provisions are directly enforceable with a fine under art 83.*

QUESTION

How does the data controller, their representative or data processes prove compliance with provisions of the Act?

DECISION TAKEN ON BASIS OF AUTOMATIC DATA PROCESSING

Part VI focuses on automated data processing broadly as well as for children or minors and other persons who are incapacitated to make decisions on processing of their personal data. In terms of Section 25 (1) of the Act, a data subject shall have the right not to be subjected to automated data processing, resulting in some legal decision or other impacts on their person, such as but not limited to profiling.

What is automated data processing?

This is personal information collected or processed automatically and a decision made without the involvement of any human or manual effort. For example, online loan applications not human mediated can deny an individual access to loans as not credit worthy or not reliable and economic unstable.

What is profiling?

This is an automated processing of personal information or data, including sensitive data to evaluate certain things about an individual and making a conclusion on that person with legal effects or implications. The implications of profiling culminate in conclusions about a person on for instance; their ability to perform a task such as use of algorithmic aptitude tests deployed during job interviews; or likely behaviour conducted through predictive analysis and concluding that someone is of criminal disposition. Profiling can therefore be part of an automated decision-making process. The GDPR Article 4 (4) defines:

> *Profiling is "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*

Is automated processing and decisions lawful?

Yes, under the Act, Section 25 (2) approves, if any individual has consented to the decision being made based on automated data processing or the processing is pursuant to a provision established by law. The consent must be explicit and not implied. It can also be based on legally authorised requirements such as employment contract or investigation of fraud or tax related matters.

There is limited clarity in the Act on how automated data processing of sensitive data must be handled. General practice, and under the GDPR[55] , however, is that a data controller must obtain explicit consent from the data subject and that the processing is necessary for reasons of substantial public interest. Automated processing of sensitive personal data must be accompanied by appropriate safeguards and measures that reduces or eliminates inaccuracies that have potential impact on data subjects, and prevents the different harms from occurring.

55 *GDPR Article 22*

QUESTION

What recourse exist for data subjects if they are subjected to automated data processing?

REPRESENTATION OF DATA SUBJECT WHO IS CHILD[56]

Section 26 of the Act provides that processing of personal and sensitive information of minors requires parental or guardian consent or approval. This Section is very important as most children are now having access to digital or internet platforms which require that an individual indicate their age or at least that they are not under 18 years. The data controller must consider having tools that help to ascertain the age of the user and that they are not under 18 years. The GDPR recognises a child or minor is 16 years, however countries can reduce that but not below 13 years for purposes of data processing[57]. This is for purposes of assessing digital maturity and attaining digital consent. The Authority must develop additional guidance.

CONSIDERATION FOR PROCESSING OF CHILDREN PERSONAL INFORMATION

- Data subject or user must confirm whether they are under or over 18 years.
- If data subject or user is below 18, then platform or data controller informs child that parental consent is need.
- User shares email address or contact details of the guardian or parent.
- Data controller contacts parent or guardian who shares consent or declines.
- Data controller must be satisfied that parent or guardian has parental Authority.
- Data controller then proceeds to process information.

These steps are relevant for manual data processing.

QUESTION

Can the processing of data of minor be only based on consent of parents, or other exceptions can also apply?

REPRESENTATION OF PHYSICALLY, MENTALLY OR LEGALLY INCAPACITATED DATA SUBJECTS

Under Section 27, the Act protects the processing of data of individuals who are physically, mentally, or legally incapacitated. In other words, these individuals may not be capable of exercising their rights as provided in the Act. Individuals whose incapacity has been medically proven by a qualified physician may exercise such rights through parents or guardians as provided by law or designated by court.

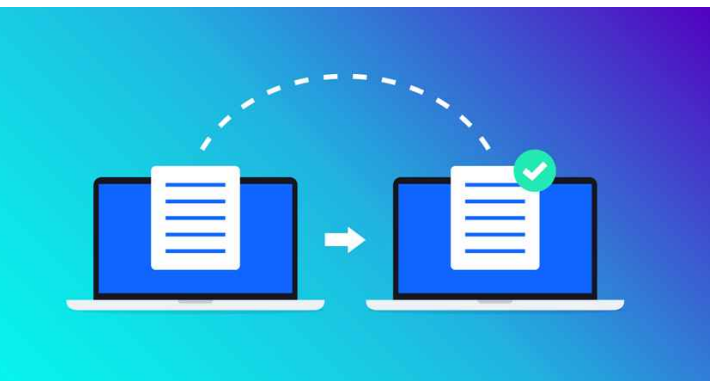
56 *This section would have benefitted from referencing of other sections as grounds for processing or alternatively framed as POPIA Section 35 providing for the General authorisation concerning personal information of children.*

57 *GDPR Article 8 (1)-(3).*

TRANSFER OF PERSONAL INFORMATION OUTSIDE ZIMBABWE

As data processing is happening on digital platforms or even manually, then stored on digital platforms, it means that data will move across borders. This is what has become known as cross border data transfers or data transfers. Part VII of the Act regulates the transborder flow of information. Remember that privacy is about protecting personal information while freedom of expression and access to information depend on the free movement of personal information across frontiers, and even for economic and trade purposes[58].

What is data transfer?



Transfer is the intentional sending of personal information by a data controller or data processor to a third-party recipient either through a data controller or data processor, in another country or an international organisation and the data is accessible and available. The third-party recipient in the other country or international organisation is not the data subject.

Data transfer is not ***data transit.*** Data transit is where personal information or data is sent through an intermediary such as an internet host, internet service provider, and the intermediary have no access to the information for purposes of any action, decisions or otherwise during the transit period. This is not to suggest that there will be no unauthorised access, interception or collection during transit period.

Data subject and data controller can be in the same country, and no transfer takes place as this is purely data collection. They can be in different countries, and still remains as data collection, but becomes **cross border data collection** if data controller is outside the country and authorising an in-country data processor.

E EXERCISE

In these scenarios identify if there is a data transfer or not.

Scenario 1:
Chad Gore Technologies posts on their website and social media platforms that as a company ZEC has approved them to support the voter registration taking place countrywide.

Scenario 2:
Chad Gore Technologies collects personal information in Zimbabwe and sends this to local storage in Harare industrial area and simultaneously sends the information on a cloud system located in a different country.

Scenario 3:
Chad Gore Technologies collects personal information from their base in Zambia from data subjects in Zimbabwe.

Section 28 (1) of the Act provides for the **transfer** of personal information by a data controller to a foreign country or international organisation if there is adequate level of protection in the country or international organisation. The determination of **adequate levels of protection** are listed under Section 28 (2) of the Act. These circumstances for the data transfer must take into account:

- nature of the data
- purpose and duration of the processing
- recipient country or international organisation

58 *GDPR preamble 101.*

- laws relating to data protection in the country or international organisation
- profession rules and security measures which are complied with in that country or international organisation

Adequacy Levels Assessment

The GDPR Article 46 sets conditions for data transfer which are reflected in most laws including this Act and POPIA, Section 72. These conditions were also discussed in the famous case before the European Court of Justice involving the ***Ireland Data Protection Commissioner v Facebook Ireland Ltd*** [59] Adequate level of protection is reached through a clear assessment of various elements and surrounding circumstances all relevant for data protection, but not only what is provided in the data protection law.

*• The observance of the rule including respect for human rights
- Analysis of relevant laws, and legislation including security criminal laws.
- Access of public authorities to personal information.
- Data protection rules, professional rules and security measures.
- Judicial precedents/case law on enforcement of data protection laws.
- Effective administrative and judicial remedies for data subjects on data transfer.
- Presence of independent and functional one or more data supervisory/protection Authority:

    o Capable of enforcing compliance with data protections laws.
    o Sufficient powers to enforce laws.
    o Capable of assisting data subjects in exercising their rights.
    o International cooperation with other data supervisory authorities.

- International law commitments through conventions and treaties such as those that relate to data protection, for instance, the Council of Europe Convention on Personal Data,

Section 28 (3) of the Act provides that the Authority shall provide categories of data processing and transfers to other countries which is not authorised. Further, there is oversight and control in the implementation of this provision by the Cyber Security and Monitoring Centre as per Section 28 (4). These provisions might be interpretated as encouraging **data localisation**, and therefore restricting the movement or processing of personal data outside Zimbabwe.

The Act lists circumstances in which transfer takes place under Section 28. However, a data controller might need to take additional steps to satisfy themselves on the provision of adequate data protection in the third country or international organisation.

If that is not possible, then other means to transfer data might be used such as **binding corporate rules** (BCR) or **standard contract clauses** (SCC) which confirm that there are appropriate technical and organisational safeguards for data protection of a similar standing in the recipient country or organisation.

BINDING CORPORATE RULES

Chad Gore Technologies has an operating unit and company in Zambia which is solely responsible for data warehousing and providing of data processing tools and resources for Chad Gore Technologies. Chad Gore Technologies will develop data protection policies that will be adhered to by all the companies for transfers of personal data outside Zimbabwe. The BCR must, however, be approved by DPA. Multinational companies usually use BCRs.

59 *Facebook Case C-311/18.*

The Act does not specifically provide for BCR, however, comparative laws such as POPIA provide for such under data transfer provisions. POPIA defines BCRs as 'personal information processing policies, within a group of undertakings, which are adhered to by a responsible party [controller] or operator [processor] within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country[60].

STANDARD CONTRACT CLAUSES

SADC as a regional economic community adopts its data protection laws and requires all members that intend to send data from SADC to abide by set standard of rules. These rules will be applicable to all member states intending to send data to a non-SADC member state.

Such BCR and SCC rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers and protection of data subject's rights. They must be legally binding and enforced by every member concerned of the group.

TRANSFER TO COUNTRY OUTSIDE ZIMBABWE WHICH DOES NOT ASSURE ADEQUATE LEVEL OF PROTECTION

The transfer of data is intended to advance the data subject rights, or pursuit of legitimate controller interests or other basis provided at law. Therefore, even if there is no adequate protection offered in the recipient country or international organisation, data transfers can take place according to Section 29 (1) if the:

(a) data subject has consent to the transfer
(b) transfer is for performance of a contract between data subject and controller in response to data subject
(c) transfer is for conclusion of contract or to be concluded in the interest of data subject
(d) transfer is necessary or legally required on public interest grounds
(e) transfer is to protect vital interests of the data subject
(f) transfer is made from public register and information is publicly available

These provisions are similar to the POPIA under Section 72(1).

Code of Conduct

Part VIII of the Act provides for the adoption of codes of conduct. Section 30 (1) allows the Authority to adopt guidelines and approve codes of conduct and ethics governing data controllers conduct and the various categories of data controllers.

WHAT IS A CODE OF CONDUCT?

The Act defines a code of conduct as "data use charters drafted by the controller in order to institute rightful use of IT resources, the Internet, and electronic communications of the structure concerned, and which have been approved by the Data Protection Authority".

A code of conduct is a set of rules laid down by an association, or by an industry, or profession with the intention of regulating the conduct of the association members, industry members or professionals in respect of data processing. The codes of conduct can be classified according to different associations. The codes of conduct ordinarily include voluntary monitoring mechanisms to allow for members compliance, enforcement and supervision, though the final supervisory body is the Authority. Codes of conduct are helpful for data controllers to enforce good industry or profession wide data processing practices and challenges can be resolved through an industry wide approach.

60 *POPIA section 72 (2).*

What if codes of conduct already exist?

The Act is not the only law regulating data processing in Zimbabwe, and associations might already exist with codes of conduct. For instance, data controllers in banking institutions or health institutions. If these are in existence, they can be amended or extended under Section30 (2). The Authority must approve codes of conduct based on the provisions of the Act and other considerations as per Section 30 (3). In terms of Section 30 (4), the Authority may consult data subjects or representatives likely to be affected by the code of conduct.

What must be contained in a code of conduct?

The Act is not exhaustive in this respect, and this will certainly be covered by statutory instruments. However, POPIA sections 60 (1)-(4) provides guidance on provisions and application of codes of conduct.

For instance, the code must:

- incorporate all the conditions for the lawful processing of personal information or set out obligations that provide a functional equivalent of all the obligations set out in those conditions; and
- prescribe how the conditions for the lawful processing of personal information are to be applied, or are to be complied with, given the particular features of the sector or sectors of society in which the relevant responsible parties are operating.

Further the code must also specify appropriate measures for:

- information matching programmes if such programmes are used within a specific sector; or
- protecting the legitimate interests of data subjects insofar as automated decision making, as referred to in Section 71, is concerned

And lastly the code of conduct must provide for the review of the code by the Information Regulator [Authority]; and provide for the expiry of the code.

What is the importance of code of conduct?

Data subjects will benefit from associations adopting codes of conduct as they will receive and expect a fair and balanced processing of personal information. The Authority will also benefit from codes of conduct as it will reduce the number of disputes, and complaints to adjudicate. Signing up to a code of conduct for data controllers shows compliance with data protection laws and a good practice for transparency, accountability and openness in data processing.

WHISTLE-BLOWER

Part IX of the Act provides for rules authorising and governing the whistleblowing system. Section 31(1) of the Act gives power to the Authority to establish rules giving the authorisation and governing of the whistleblowing system. This Section is important and will require further clarification from the Authority.

REGULATIONS, OFFENCES, PENALTIES AND APPEALS

Part X of the Act which constitutes general provisions has a section on regulations, offences and penalties and appeals in terms of the Act.

Regulations

Section 32 of the Act gives powers to the Minister in consultation with Authority to make regulations for matters related to the Act. These regulations can also cover some of the specified areas such as Sections 25 to 27 which deal with decisions on automated data processing, representation of the data subject who is a child; and representation of physically, mentally or legally incapacitated.

Offences and Penalties

There are various offences and penalties under the Act. Section 33 (1) penalises any member of the Authority including an expert or contractor who violates provisions of the Act. In addition, Section 33 (2) criminalises violation of several sections by data controller or representative. These sections are:

- Section 11 on sensitive data
- Section 13 on duties of the controller
- Section 18 (4) on appropriate technical and organisational measures to safeguard data security, integrity and confidentiality
- Section 24 on accountability
- Section 28 on transfer of personal information.

In the event of data that is unlawfully acquired, the courts are authorised to order seizure of the materials or deletion under Section 33 (3), 33 (4) and 33 (5). Data controller or their representative are liable for any fines that are imposed on their agents.

E EXERCISE

Chad Gore Technologies have completed the collection of voter registration biometric information for ZEC. To achieve a quick turnaround exercise Chad Gore Technologies sub-contracted Chigs Technologies to provide additional collection and storage support. Chigs Technologies creates a backdoor access to the data servers for Asphalt Marketing to collect numbers, biometrics and all personal data, which they are using for marketing and screening for employment. Chigs Technologies, further shares biometrics (eye and fingerprints) to Catch Them All private investigators. ZEC proves no knowledge of all these transactions and fails to confirm that Chad Gore Technologies had implemented appropriate technical and organisational measures. Further, several political parties have started sending messages to registered voters urging them to vote in the coming 2028 elections.

1. Identify the data breaches and violations?
2. Who is liable for the various data breaches?
3. Who should notify the DPA?
4. Should the data subjects be notified, if not why?

MISA ZIMBABWE

84 McChlery Avenue, Eastlea, Harare, Zimbabwe

www.zimbabwe.misa.org • @misazimbabwe • MISA Zimbabwe • +263 784 437 338