ANTHONY BABAJIDE BALOGUN
ID No: **UB73361SIN82521**

COURSE TOPIC:

PROTECTION OF PERSONAL INFORMATION (PoPI) (South Africa as a case study)

ATLANTIC INTERNATIONAL UNIVERSITY
MAY 2022

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

Information is a knowledge communicated or received concerning a particular thing or situation such as; news concerning a crime, an invention, knowledge gained through study, communication and even research. In actual fact, humans have been storing, retrieving, manipulating and communicating information sometimes since the 3000 BC but the term information technology first appeared in around 1958 when Harold J. Leavitt and Thomas L. Whisler published an article where they commented that the new technology does not yet have a single established name

In actual sense of it, everyone has the right to be told if someone is collecting his or her information or if any of his or her information has been accessed in one way or the other by an authorized person or group of people. Everyone can also request for his or her personal information either to be corrected or to be destroyed outrightly.

Protection of personal information refers to the collection, processing, recording, sharing of personal information by a responsible party which could be a website, company or organization that is located in the republic of South Africa or outside. The scope of PoPIA in the republic of South Africa is limited compare to the scope of the GDPR in Europe no matter which country or geographical location in Europe.

South African Constitution with regards to personal information states that, everyone has the right to privacy and access any information that is held by another person. However, personal information can only be processed with the consent of the data subject. Therefore, the Protection of Personal Information Act (PoPIA) gives data subject the right to privacy. The Act also regulates the collection, processing, storage and disclosure of confidential information with justifiable means.

South Africa's Protection of Personal Information Act (PoPIA) draft and documentation could be traced back to 2003 and it was closely modelled after the European data privacy legislation at the time known as GDPR (General Data Protection Regulation). So, in July 1 2021, PoPIA finally came into effect and became operational in South Africa.

In this essay, I shall be analysing the protection of personal information with regard to the South African Constitution and as a case study. I will also analyse a bit of the GDPR (General Data Protection Regulation), the EU data privacy standard.

2.0 PROTECTION OF PERSONAL INFORMATION (PoPI)

2.1 Key Definitions

2.1.1 Information

Information is a knowledge communicated or received concerning a particular thing or situation such as; news concerning a crime, an invention, exposure acquired via study, communication and even research. In actual fact, humans have been storing, retrieving, manipulating and communicating information sometimes since the 3000 BC but the term information technology first appeared in around 1958 when Harold J. Leavitt and Thomas L. Whisler published an article where they commented that the new technology does not yet have a single established name.

2.1.2 Data Subject (DS)

A data subject is referred to as a person or an individual who can be identified either directly or indirectly through an identifier such as a name and an identity number (ID number). In other words, a data subject could be regarded as either you or me whom personal information relates to.

2.1.3 Directing Marketing (DM)

This is a process of sending to a person or individual otherwise known as a data subject an electronic communication about goods and services their organization or company produces in order to promote such goods. It may also be in form of a donation of any kind towards the promotion of goods and services in the course of running a business.

2.1.4 Processing (P)

This is the manipulation or conversion of raw data in order to produce a meaningful and useful information. It also involves the capturing of information in a type of a format can be easily retrievable and analyzable.

2.1.5 Record (R)

A record is defined as a documented information regardless of when it came into an existence. It is also being referred to as evidence kept concerning an event that took place in the past.

2.1.6 Responsible Party (RP)

The function of a responsible party which can either be a public or private institution or even an individual in the protection of personal information is to ascertain the purpose of and the means of processing a personal information.

3.0 PERSONAL INFORMATION DEFINITION AND CLASSIFICATION

3.1 Personal Information

According to cloudflare, “Personal information, also called personal data, is any information that relates to a specific person. Some of the most obvious examples of personal information include someone's name, mailing address, email address, phone number, and medical records (if they can be used to identify the person). In addition, some privacy frameworks consider anything that can help determine someone's identity, such as online identifiers or Internet browsing history, to be personal information”. (cloudflare, n.d.)

3.2 Classification

Personal information can be classified into the following:

- Name of person
- Age
- Gender
- Physical or mental health
- Well-being
- Disability
- Medical/financial history
- ID number
- e-mail

- Physical address
- Telephone numbers
- Biometric information e.g., DNA, fingerprint, blood type
- Personal opinions (views, preferences of person)
- Correspondence of private or confidential nature
- Views or opinions of another individual about a person

3.3 Processing Personal Information

The processing of personal information can either be automatic or manual and it covers aspects such as;

- Collection
- Receipt
- Recording
- Storage
- Updating
- Use
- Dissemination
- Merging
- Destruction

4.0 PROTECTION OF PERSONAL INFORMATION ACT (PoPIA)

(South Africa as a case study)

4.1 Background

In actual sense of it, everyone has the right to be told if someone is collecting his or her information or if any of his or her information has been accessed by an authorized person. Everyone can also request for his or her personal information either to be corrected to be destroyed outrightly.

With regards to the South African Constitution on protection of personal information, everyone has the right to privacy and to access any information that is held by another person. However, processing of personal information depends solely on the consent of the data subject. Therefore, the Protection of Personal Information Act (POPIA) gives data subject the right to privacy. The act also guides the collection, processing and revealing of confidential information.

The Protection of Personal Information Act protects the data subjects from danger by; protecting their personal information from being stolen or have access to illegally, to stop their money from being stolen through an illegal fraudulent activity, to prevent their identity from being stolen and ultimately to protect their privacy which is their main fundamental human right.

South Africa's Protection of Personal Information Act (POPIA) draft and documentation could be traced back to 2003 and it was closely modelled after the European data privacy legislation at the time known as GDPR (General Data Protection Regulation). PoPIA became operational in South Africa in July 1, 2021.

4.2 Scope and Application

Protection of personal information is the process of collecting, processing and sharing of personal information by a responsible party which could be a website or organization in South Africa or outside. It has been observed that, the scope of PoPIA in South Africa is minute compared to the scope of the GDPR in Europe no matter which country or geographical location.

For example, if you design a website for your organization and uses it to process personal information, you are obligated to comply with the protection of personal information act operational in South Africa.

4.3 PoPIA Conditions for lawful data processing

The protection of personal information act in South African establishes eight conditions for lawful processing of data and the include the following;

Accountability: to be certain that the processing of data and information is lawful and done in such a non-privacy and infringing way.

Processing limitation: this means, processing of data and information is only done for the given purpose

Purpose specification: here, specific purpose for data processing must be explicitly defined

Further processing limitation: this simply means that, any other processing must be in accordance with original purpose that the end-user provided their consent to

Information quality: "data completeness and accuracy"

Openness: all processing operations and processes must be properly documented for future use

Security: the protection and confidentiality of personal information must exist at all times

Data subject participation: in every process, the end-users must be able to exercise their rights in order to access, update and destroy their personal data

4.4 PoPIA rights for South African citizens

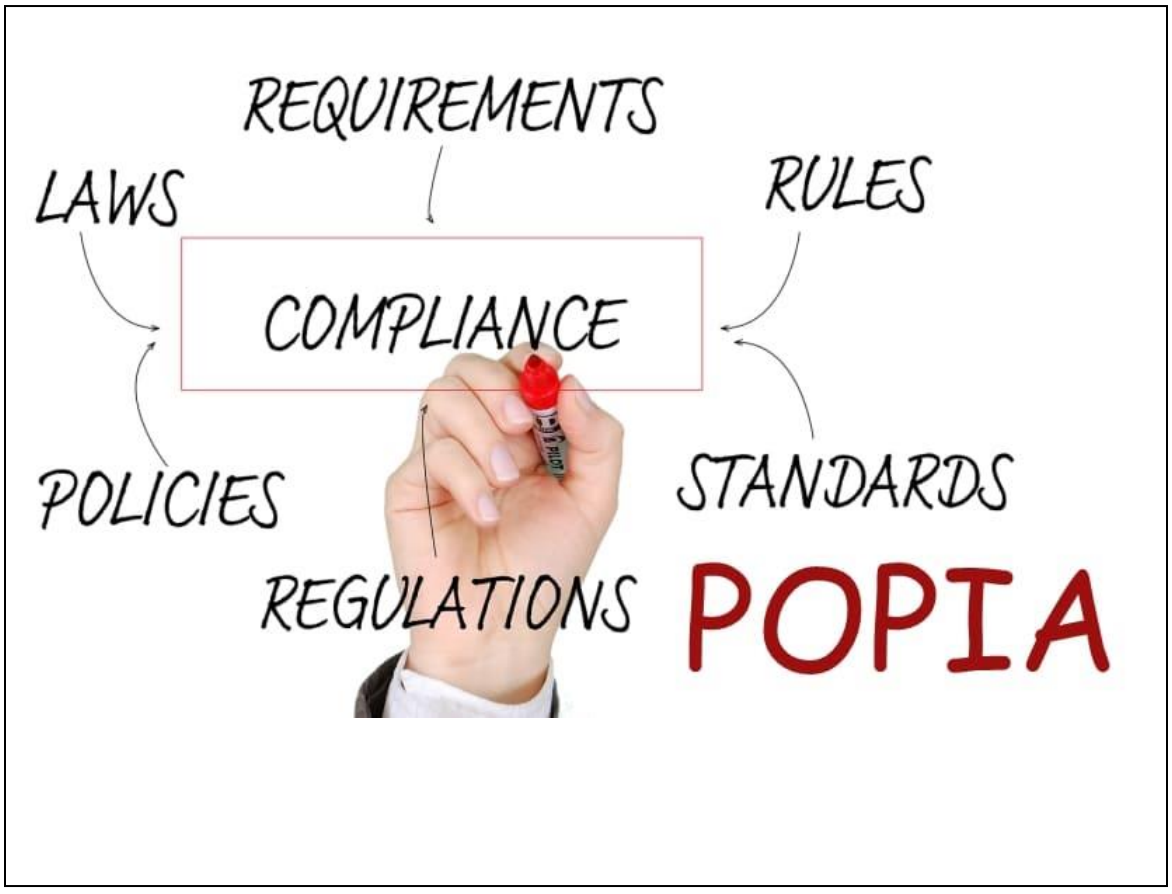
The following rights were established by PoPIA for data subject before his or her data could be collected and processed:

- Right to be informed of data collection and processing of personal information
- Right to access personal information
- Right to request the update of personal information
- Right to request destroying of personal information
- Right not to allow the processing of personal information
- Right to denied the direct marketing processing making use of personal information
- Right to not be subject to a decision resulting in legal circumstances
- Right to lay complaints before the Information Regulators
- Right to effect judicial remedy

5.0 ENSURING COMPLIANCE TO PoPIA

It is the responsibility of a business owner to make sure that; all personal information is documented and stored safely and also make sure that, access to that information is not given to an unauthorized individual or group of people who may want to misuse or share such information for any malicious intent.

Figure 1



(Pretorius, 2021)

Figure 1: showing PoPIA compliance

The following practical steps can be put in place in order to safeguard personal information:

5.1 Compile and document a strategy

Developed strategies to show how the data being collected is going to be protected which must include the process of data backup. The strategies must be able to show the risks connected to data violation or breach. Mitigating the risks should also be paramount and a response strategy to such risks should be put in place. Ultimately, the strategy must be readily available and accessible with a plan to review it regularly.

5.2 Protect against malware

All information technology appliances and devices such as; PCs, network devices must be secured by making use of a firewall and ensuring that all passwords are confidential and strong in structure.

Moreover, security software for protection such as anti-spam and anti-malware must be installed and monitored regularly. Employee’s devices that are being used remotely to access organization's networking facility must also be secured. If Wi-fi access is being to employees, it must be ensured that, a strong encryption be deployed and all the SSID broadcast must be turned off in order to make the network invisible to the prying eyes of the hackers.

5.3 Use the cloud

"Cloud computing is another technology" that is worthwhile to look into by selecting a reputable cloud service provider that can be of a great assistance with storing of information with an adequate security measure. There are few of such providers with great expertise which include; "Microsoft, Amazon, IBM, Google and Oracle" to mention just a few.

5.4 Inform employees

It is essential and very important for every employee in any business to understand the position of the organization's security policy. Training employees on the PoPIA compliant and to ensure that they handle information in a confidential and highly integrity manner. Furthermore, refresher training and course must be conducted regularly which should include the induction process for newly employed staff at all levels.

5.5 Gain consent from those concerned

Relevant authorization and consent must be taken from the respective individual or organization in order to process and store their information including what the information gathered is going to be used for. Only the information that is relevant to the business transaction should be collected and it is always advisable to be upfront with the intentions around all the data collected.

5.6 Storage period

Personal and confidential record should only be kept for the duration of its usage. Determine exactly when the data collected will no longer be useful in order to completely destroy it.

5.7 Destroying records

With adequate consideration, determine the best way to delete or destroy information that is no more needed. Keeping data that is no more relevant or useful for business transaction does not only attract great risk but it also consumes data backup resources which could be costly to handle.

It is very important to notify the information regulator of a situation where it is believed that personal and confidential information has been breached or violated.

6.0 HOW TO HANDLE PERSONAL INFORMATION

Everybody has the right to make an enquiry as to whether someone else is in possession of his or her personal information. What to be done in that situation is to provide an adequate proof of identity and such enquiry will be processed and this information must be given free of charge.

In order to handle personal information efficiently and securely, the following steps must be implemented:

6.1 Identify all risks

All risks linked to data must be thoroughly established and adequately identified. It must also be ensured that, data are safeguard by implementing a robust security control around the data. Such security controls must be reviewed regularly in order to identify deficiencies and weaknesses in the controls.

6.2 Proper Authorization

Whoever is processing personal information on behalf of an employer must have a proper authorization from such an employer in order to be able to have access to the information. Such personal information must also be treated with high confidentiality.

6.3 Confidentiality

A written contract must be drafted and agreed on by both parties where pledges will be made in order to specifically obliged to maintain the integrity and confidentiality of the personal information and to implement a robust security policies and measures to safeguards against any of the identified risks.

In the same vein, every employee is also obliged to inform his or her employer if they believe or noticed that, personal information got into the wrong hands.

6.4 Information Regulator

In a situation where personal information has been breached or compromised by an authorized person, the incident must be reported immediately to the Information Regulator, and more particularly if the subject involved is well known with a genuine proof.

However, the Information Regulator has the power to grant exemptions which will allow people to process personal information without complying with the Act, although such exemption will be given or approved with certain condition which must be met. Furthermore, exemptions may also be granted for the purposes of discharging what is known as a relevant function.

This is a processing of personal information with protecting the members of the public in mind against such occurrence as; financial loss due to dishonesty and also dishonesty by employees authorized to perform any profession work or other related activity.

6.5 Right to update

Every data subject has the right to have his or her personal information corrected or deleted if it is considered to be inaccurate, or if his or her personal information has been fraudulently obtained, or in a situation where the responsible party does not have the authorization to retain the such information any longer.

7.0 STEPS TO PROTECTION OF PERSONAL INFORMATION

There are various ways in which an individual can adopt in order to make sure that his or her personal information stays secured and private at all times. They include but not limited to the following;

7.1 Use HTTPS websites only

Individual should try as much as possible to avoid websites that do not use encryption to protect data going to and from their servers. Such websites use HTTP instead of HTTPS and it is easier for the hackers to penetrate such websites in order to perform their unlawful activity.

7.2 Review terms of service and privacy policy

It is very important for an individual before making use of a website to review and understand how much personal information a website or its applications collects and what happens to such personal information when collected.

7.3 Strong passwords and two-factor authentication

Users should endeavor to use strong passwords and two-factor authentication when login into a website.

Reusing of passwords or weaker passwords which can easily be guessed should be avoided. Furthermore, a two-factor authentication (2FA) has been known to secure online accounts much more.

7.4 Control cookie usage

A few browsers requires that cookies are enabled in order for their website to function properly. However, blocking unnecessary cookies, when possible, assist in mitigating the risk of the third parties that are tracking and monitoring individual online activities in an attempt to gather personal information.

7.5 Use end-to-end encryption

End-to-end encryption guarantees that, messages remain private from everyone. In other words, it's only an authorized person which the encrypted message is meant for with an appropriate key that can de-encrypt an encrypted message.

7.6 Use secured DNS

DNS resolvers sometimes track and monitors which domains and particular websites a person visit. The results of this tracking are sometimes sold to advertisers for direct marketing purposes. A privacy-focused and a secured DNS resolver helps internet users to keep their browsing history protected from prying eyes of hackers.

8.0 TRANSBORDER FLOW OF PERSONAL INFORMATION

There is possibility of an individual personal information to be transferred by a third party to a foreign land without his or her consent. In the light of this, personal information of a data subject may only be transferred to a third party in a foreign country if:

- Such transfer benefits the data subject
- Such transfer is necessary for the conclusion of a contract carried out in the best interest of the data subject
- Such transfer is necessary for the performance of contract between data subject (DS)and the responsible party (RP)
- Such transfer is carried out with the consent of the data subject (DS)
- The recipient is subject to some form of law or agreement
- Such transfers should have an adequate level of protection

9.0 PoPIA vs GDPR

Below is the comparison between PoPIA and GDPR.

	Protection of Personal Information Act (POPIA)	**General Data Protection Regulation (GDPR)**
Personal scope	Applies to the data subject who is an identified or identifiable natural person	Applies to the data subject who is an identified or identifiable natural person
Territorial scope	Applies to organizations which process personal data based in South Africa	Applies to organizations which process personal data based in EU
Regulator	Established under Section 39 of PoPIA	Members can establish and determine the roles and responsibilities of a Supervisory Authority
Penalties	Maximum fine is ZAR10 million which is approximately €490,000. Up to 10 years imprisonment	Up to 4% of global annual turnover or €20 million. No provisions for imprisonment
Data transfer	Transborder data flow are permitted to a third country with an adequate level of protection	Transborder data flow is not permitted where the recipient is not subject to a law
Data breach	Data breach must be notified to the supervisory authority within 72 hours after the discovery of such breach	Regulator must be notified of any data breach as soon as possible after the discovery of the compromise

10.0 CONCLUSION

Everyone has the right to be told if someone is collecting his or her information or if any of his or her information has been accessed by an authorized person. Everyone can also request for his or her personal information either to be corrected to be destroyed outrightly.

With regards to the South African Constitution on protection of personal information, everyone has the right to privacy and to access any information that is held by another person. However, processing of personal information depends solely on the consent of the data subject. Therefore, the Protection of Personal Information Act (POPIA) gives data subject the right to privacy. The act also guides the collection, processing and revealing of confidential information.

The Protection of Personal Information Act protects the data subjects from danger by; protecting their personal information from being stolen or have access to illegally, to stop their money from being stolen through an illegal fraudulent activity, to prevent their identity from being stolen and ultimately to protect their privacy which is their main fundamental human right.

It is the responsibility of a business owner to make sure that; all personal information is documented and stored safely and also make sure that, access to that information is not given to an unauthorized individual or group of people who may want to misuse or share such information for any malicious intent.

In a situation where personal information has been breached or compromised by an authorized person, the incident must be reported immediately to the Information Regulator, and more particularly if the subject involved is well known with a genuine proof.

However, the Information Regulator has the power to grant exemptions which will allow people to process personal information without complying with the Act, although such exemption will be given or approved with certain condition which must be met. Furthermore, exemptions may also be granted for the purposes of discharging what is known as a relevant function.

Finally, whoever is processing personal information on behalf of an employer must have a proper authorization from such an employer in order to be able to have access to the information. Such personal information must also be treated with high confidentiality.

11.0 BIBLOGRAPHY

cloudflare. (n.d.). *What is personal information? | Personal data*. Retrieved from What is personal information or personal data?: https://www.cloudflare.com/learning/privacy/what-is-personal-information/

Pretorius, E. (2021, Jul 21). *PoPI – Do you need to comply?* Retrieved from PoPI – Do you need to comply?: https://www.tat.accountant/popi-do-you-need-to-comply/