Office: 010 597 0835 | **Facilitator:** 083 821 8801 | **E-mail:** anna@compliancelearningcenter.net
Website: www.compliancelearningcenter.net |
Address: 10A Lever Street Brackenhurst Alberton, South Africa
Registration nr: 2018/242685/07 | **Vat nr:** 4070281904

Study Guide

PROTECTION OF PERSONAL INFORMATION ACT: ONLINE CPD COURSE 2020 / 2021

Anna Bouhail ©

May 2020

Course summary

All entities handling personal information of clients, employees and suppliers need to adhere to the requirement stipulated under the Protection of Personal Information (POPI) Act. These entities need to ensure that all employees handling personal information is aware of the data processing conditions stipulated under the POPI Act.

The POPI Workshop is an introductory program outlining the conditions of data processing imposed on any organisation handling personal information of individuals and/or entities. Apart from providing an overview of the framework in which the processing of data is regulated, the workshop also considers the data processing restrictions and best practice protocol.

The workshop provides evidence that employees are aware of the regulatory framework in which personal information must be processed.

Time allotted for course

The course consists of 4 topics with an assessment that needs to be completed. The time allotted for each aspect is as follows:

Topic number	Title	Word count	Level	Time allotted
Topic 1	Introduction to the POPI Act	1681	Entry level	15 minutes
Topic 2	Data collection conditions	2844	Entry level	35 minutes
Topic 3	Other stipulations	3292	Entry level	35 minutes
Topic 4	Enforcement	2511	Entry level	35 minutes
	Assessment			45 minutes

Total time	**2 hours**

Assessment and certification

After completion of the workshop the learner must complete an electronic assessment on the learning management system.

- **Form of assessment:** Multiple Choice Questions
- **Number of questions**: 15 questions
- **Duration:** 45 minutes
- **Competency mark:** 60%

Upon obtaining a competency mark of 60% the learning will receive a certificate of completion. The learner will be afforded an opportunity to re-do the workshop should a competency mark not be attained.

Course accreditation

CPD Category: Online program

COB Category: All classes of business

Financial planning component: Ethics & Practice Standards Management

Financial Advice: Ethics, Standards & Compliance

Accreditation valid until: 31 May 2021

CPD Points allocated: 2.0 hours | points on successful completion and pass of assessment

FPI approval number: FPI20050211

Table of contents

Copyright notice

Anna Bouhail
10A Lever Street
Brackenhurst
Alberton
1449
South Africa

Ordering information
If you would like to order the publication, please contact author at address above.

TOPIC 1 INTRODUCTION TO THE POPI ACT

LEARNING OUTCOMES

After studying the topic, the learner should be able to-

- Understand the regulatory framework under which the processing of personal information is regulated.

1.1 Introduction

Ever receive unsolicited calls from call centers to sell you a product or service, text messages at all hours of the night and day, unsolicited email communications (a.k.a. SPAM) attempting to sell you a product or inform you that you have won the lottery?

Ever wonder how and where they got your details?

These direct marketing efforts are probably the most tangible example of how most people are affected directly when their personal information is abused because there is no real protection of and consequence for sharing their information with other parties.

The Protection of Personal Information (POPI) Act addresses this issue by making sure everyone from government and the big financial institutions down to the security guard who records details in the visitor's log have a good enough reason (purpose) for collecting information and is responsible (can be held accountable) for protecting it.

The POPI Act plays an important part in increasing consumer protection and information control in a world where information abuse and exploitation are rampant.

WHEN THEY SAID I'LL GET UNLIMITED CALLS AND TEXTS WITH MY NEW MOBILE CONTRACT, I DIDN'T REALISE THEY WOULD ALL BE FROM PPI INSURANCE COMPANIES....

Recent Case Study of Information Leaked

In October 2017, the personal details of 33 million people were leaked by a company called Jigsaw Holdings. About 27 gigabytes of data containing the names, full identity numbers, income, employment history and even home addresses of South Africans have been uploaded to an insecure server.

The Information Regulator is investigating the matter, but the company admitted to inadequate safeguards to ensure the security of the information.

1.2 Objective of the Act

The Protection of Personal Information Act (POPI) became law on 26 November 2013. POPI essentially regulates how anyone who processes personal information must handle, keep and secure that information.

The purpose of the POPI Act is to ensure that all South African organisations conduct themselves in a responsible manner when processing another entity's or individual's information. The POPI Act holds these organisations accountable should they abuse or compromise personal information in any way.

Although, various pieces of legislation already advocate the protection of personal information, the POPI Act ensure that the requirements regarding protection of personal information is addressed in one Act, regulating how personal information must be processed.

The Act also provides for a regulator specifically dedicated to regulating issues pertaining to personal information. This regulator is called the Information Regulator. The Information administrates both the POPI Act and the Promotion of Access to Information Act (PAIA).

Advocate Pansy Tlakula was appointed as the information Regulator with effect from 1 December 2016. The Information Regulator is an independent body and is subject only to the law and the constitution. The Information Regulatory is accountable to the National Assembly.

The Information Regulator is empowered to monitor and enforce compliance by public and private organisations with the provisions of the Protection of Personal Information Act. Furthermore, the information Regulator is responsible for education, perform research and facilitate cross-border cooperation.

The website of the information regulator is http://www.justice.gov.za/inforeg/index.html

Applicable organisations will have one year from the announcement of the effective date to conform to the requirements relating to the processing of personal information.

The Information Regulator has already received hundreds of complaints pertaining to the unlawful accessing of information. Most of these complaints relate to the banking, telecoms and insurance industry's practice of direct marketing through unsolicited, targeted communication.

1.3 Scope of POPI

The POPI Act regulates the processing of personal information. Therefore, the Act applies to a particular activity rather than a specific person or type of organisation. Therefore, any organisation (both public and private) that processes personal information must comply with the Act.

Processing of personal information include one or more of the following actions:

- Collecting, receiving, updating and retrieval of personal information of individuals and entities.
- Using personal information of individuals and entities.
- Disclosing personal information to third parties.
- Keeping personal information of individuals and entities.
- Destroying personal information.

Information can be processed manually or by automated means. Automated means are any equipment capable of operating automatically in response to instructions given for the purpose of processing information.

If information is processed by non-automated means the information must form part of a filing system. A filing system is any structured set of personal information whether centralized, decentralized or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

Therefore, it is particularly important that all employees of an organisation that process personal information of an identifiable individual or company, handle this information in accordance with POPI's data protection conditions.

The scope of POPI is very wide and it applies to almost everything you might do with personal details including details of employees. POPI applies even to public records such as personal information of grant beneficiaries and health records.

Therefore, it is particularly important that all employees of an organisation that process personal information of an identifiable individual or company, handle this information in accordance with POPI's data protection conditions.

The table below outlines examples of personal information of an entity or individual.

Identity / passport number	Date of birth and age	Phone numbers
E-mail addresses	Online/instant message ID's	Physical address
Gender, race and ethnic origin	Photos, recordings, videos	Biometric data
Material Relationship status	Family relations	Criminal record
Private correspondence	Religion	Personal & Political opinions
Employment history	Salary information	Financial information
Educational information	Health information	Membership information

However, not all the information can identify a person. Therefore, the data must include data which will identify a specific individual - called a unique identifier. Examples of unique identifiers is the name and surname, ID number, employee number, bank account number ext.

1.4 Who is Responsible for Data Protection?

Who is responsible for complying with POPI where you process personal information together with someone else?

Most organisations have many relationships where they process personal information together with other organisations, including insurance-broker, vendor-buyer, and contractor-client relationships.

POPI distinguishes between the responsible party and the operator. The responsible party decides the purpose or way of processing the personal information and the operator processes the personal information on behalf of a responsible party without being directly controlled by them. The responsible party carries most of the responsibility, while the operator carries much less.

Where you process personal information together with someone else, whether you are the responsible party, or the operator depends on your relationship with them.

1.5 Prior authorisation

Most responsible parties will not need to obtain prior authorisation from the Information Regulator to process information. However, each responsible party must register their Information Officer with the Information Regulator.

Authorisation need to be obtained if the responsible party plan to-

- Process any unique identifiers of individuals for a purpose other than the one for which the identifier was specifically intended at collection with the aim of linking the information together with information processed by other responsible parties.
- Process information on criminal behavior or on unlawful or objectionable conduct on behalf of third parties.
- Process information for purposes of credit reporting.
- Transfer special information or information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

1.6 Rights of individuals (data subjects)

The person or entity of which the personal information is processed is referred to as a data subject. From now on this text will refer to an individual but it also includes entities whose personal information is processed by the responsible party.

The rights of an individual regarding the processing of the individual's personal information are as follows:

1. An individual has the right to have his, her or its personal information processed in accordance with the condition for lawful processing of personal information.
2. An individual has the right to be notified that personal information about that individual is being collected.
3. An individual has the right to be notified that personal information about that individual has been accessed or acquired by an unauthorized person.
4. An individual has the right to establish whether a responsible party holds personal information and to request access to the individual's personal information.
5. The individual has the right to request the correction, destruction or deletion of the individual's personal information.

6. The individual has the right to object on reasonable grounds to the individual's personal information being processed to protect a legitimate interest of the individual or processing is necessary for pursuing the legitimate interest of the responsible party.

7. The individual has the right to object to the processing of the individual's personal information at any time for purposes of direct marketing.

8. The individual has the right to not be subject, under certain circumstances, to a decision which is based solely based on the automated processing of the individual's personal information intended to provide a profile of such an individual.

9. The individual has the right to submit a complaint to the Information Regulator regarding the alleged interference with the protection of personal information of any individual or to submit a complaint to the Information Regulator in respect of a determination of an adjudicator.

10. The individual has the right to institute civil proceeding regarding the alleged interference with protection of the individual's personal information.

1.7 Exclusions

The POPI Act does not apply to the processing of personal information in the following circumstances:

- Processing of personal information during a purely personal or household activity.
- Processing of personal information that has been de-identified to the extent that it cannot be re-identified again.
- Processing of personal information by or on behalf of a public body which involves national security or for the prevention of unlawful activities to the extent that adequate safeguards have been established in legislation for the protection of such personal information.
- Processing of personal information by the Cabinet and its committees or the Executive Council of a province.
- Processing of personal information relating to the judicial functions of a court.
- Processing of personal information solely for journalistic literacy 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.

TOPIC 2 DATA COLLECTION CONDITIONS

LEARNING OUTCOMES

After studying the topic, the learner should be able to-

- Outline the 8 data processing conditions imposed on responsible parties and operators.
- Apply the 8 data processing conditions in the day to day activities performed by the learner.

The POPI Act lays down eight conditions with witch processing of information should comply with. These conditions are applicable to new and existing personal information.

2.1 Condition ① - Accountability

Any person who processes personal information have the responsibility to ensure that all the Act's conditions and the measures are complied with.

The consequence of non-compliance could result in fines of up to R10 million and/or up to 10 years in jail time for some offences. Any person that is also aware of a breach, must report such breach.

2.2 Condition ② - Limit data processing

2.2.1 Lawfulness

Processing of information must be done lawfully and, in a manner, that does not infringe the privacy of the individual.

2.2.2 Minimality

Personal information can only be processed if the processing is adequate, relevant and not excessive, given the purpose for which it is to be used.

2.2.3 Consent and objection

Personal information may only be processed if the individual gives consent to the processing of personal information or if processing is necessary to carry out an action for the conclusion or performance of a contract to which the individual is a party. If the individual is a child, a competent person must give consent. The responsible party must be able to provide proof that the individual gave consent.

The individual may withdraw consent at any time. However, the lawfulness of the processing of information before withdrawal is not affected.

An individual can at any time object to the processing of personal information for purposes of direct marketing. If the individual objected, the responsible party may no longer processes the information.

Consent definition

Consent means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

Processing of personal information is also allowed under the following special circumstances:

- Processing complies with an obligation imposed by law on the responsible party.
- Processing protects a legitimate interest of the individual.
- Processing is necessary for the proper performance of a public law duty by any department of state.
- Processing is necessary for the pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

An individual can object to the processing of information for the purpose mentioned above on reasonable grounds relating to his/her situation unless legislation provides for such processing.

2.2.4 Collection directly from individual

Personal information must be collected directly from the individual unless-

- The information is derived from a public record or has been made public by the individual.
- The individual has consented to the collection of the information from another source.

- Collection of information from another source will not prejudice a legitimate interest of the individual.
- Compliance would prejudice a lawful purpose of the collection.
- Compliance is not reasonable practical in the circumstances of a particular case.
- Collection of the information from another source is necessary-
    - To avoid prejudice to the maintenance of the law by a government.
    - To comply with a tax collection obligation.
    - For court proceeding or tribunal proceedings.
    - In the interest of national security.
    - To maintain the legitimate interest of the responsible party or of a third party to whom the information is supplied.

What do you think is the practical implications of Condition 2?

2.3 Condition ③ - Purpose specific

2.3.1 Collection for specific purpose

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

Steps must be taken to ensure that the individual is aware of the purpose of the collection by disclosing the information prescribed under Condition 6.

2.3.2 Retention and restriction of records

Personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected unless-

- Retention of the information is required or authorised by law.
- The responsible party reasonably required the information for lawful purposes related to its function or activities.
- Retention of information is required by an agreement between the parties.
- The individual has consented to the retention of the information.

Personal information may be kept for a longer period for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.

A responsible party that uses personal information to make a decision about the individual must-

- Retain the information for such period as may be required by law or code of conduct. If there is no law or code of conduct applicable, the responsible party must retain the record for a period which will allow the individual reasonable opportunity to request access to the information.
- A responsible party must destroy, delete or de-identify the information as soon as reasonably practical possible after the responsible party is no longer required to retain these records in terms of law or a code of conduct.

De-identify definition

De-identify means to delete any information that-

- Identifies the individual.
- Can be used or manipulated to identify the individual.
- Can be linked to other information that identifies the individual.

The destruction or deletion of personal information must be done in a manner that prevents its reconstruction in an understandable form.

The responsible party must restrict processing of personal information if-

- The accuracy is contested by the individual, for a period enabling the responsible party to verify the accuracy of the information.
- The responsible party no longer needs the personal information for achieving the purpose for which the information was collected but it has to be maintained for purposes of proof.
- The processing of the information is unlawful, and the individual opposes its destruction or deletion and requests the restriction of its use instead.
- The individual request to transmit the personal information into another automated processing system.

Where processing of personal information is restricted the responsible party must inform the individual before the lifting of the restriction on processing.

What do you think is the practical implications of Condition 3?

2.4 Condition ④ - Limit further data processing

2.4.1 Further processing of the information must be compatible with the purpose of collection

Further processing of personal information must be in accordance or compatible with the purpose for which it was collected as set out in Condition 2.

To assess whether further processing is compatible with the purpose of collection, the responsible party must take account of-

- The relationship between the purpose of the intended further processing and the purpose for which the information has been collected.
- The nature of the information concerned.
- The consequences of the intended further processing for the individual.
- The way the information has been collected.
- Any contractual rights and obligations between the parties.

The further processing of personal information is compatible with the purpose of collection if-

- The individual has consented to the further processing of the information.
- The information is open to the public or has been made deliberately public by the individual.
- Further processing is necessary –
    - To avoid prejudice to maintaining the law by any public body.
    - To comply with tax collection obligations.
    - For court proceeding or tribunal proceedings.
    - In the interest of national security.

- Further process of information is necessary to-
    - Prevent a serious threat to public health, the life or health of the individual or another individual.
    - The information is used for historical, statistical or research purposes and the responsible party ensures that further processing is carried out solely for such purposes and will not be published in an identifiable form.
    - The further processing of information is in accordance with an exemption granted by the Information Regulator.

What do you think is the practical implications of Condition 4?

2.5 Condition ⑤ - Quality of information

The responsible party must take reasonable steps to ensure that personal information is complete, accurate, not misleading and updated when necessary. All the while, considering the purpose for which the information was initially collected.

What do you think is the practical implications of Condition 5?

2.6 Condition ⑥ - Openness

2.6.1 Documentation

A responsible party must maintain the documentation for all processing operations including the complaints process in this regard in the information manual prescribed under the Promotion of Access to Information (PAIA) Act Section 14 and section 51.

2.6.2 Notification to data subject when collecting personal information

If personal information is collected, the responsible party must take reasonable practical step to ensure that the individual is aware of –

- The information being collected and where the information is not collected from the individual the source from which it is collected.
- The name and address of the responsible party.
- The purpose for which the information is being collected.
- Whether or not the supply of the information by the individual is voluntary or mandatory.
- The consequences of failure to provide the information.
- Any particular law authorising the collection of the information.
- Where applicable, the fact that the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation.
- Any further information such as the-
    - Recipient or category of recipients of the information.
    - Nature or category of information.
    - Existence of the right of access to and the right to rectify the information collected.
    - Existence of the right to object to the processing of personal information collected.
    - Existence of the rights to object to the processing of information under special circumstances as detailed under condition 2.

- Existence of the right to lodge a complaint to the Information Regulator and all the contact details of the Information Regulator.

- Any other information as is necessary, having regard to the specific circumstance in which the information is or is not to be processed, to enable processing in respect of the individual to be reasonable.

This notification must be given to the individual before the information is collected unless the individual is already aware of the information in the notice. Therefore, subsequent collection of information does not need to give notice to the client.

It is not necessary for the responsible party to give a notification if-

- The individual has provided consent for the non-compliance.
- Non-compliance would not prejudice the legitimate interest of the individual.
- Non-compliance is necessary-
  - To avoid prejudice to maintaining the law by any public body.
  - To comply with tax collection obligations.
  - For court proceeding or tribunal proceedings.
  - In the interest of national security.
- Compliance would prejudice a lawful purpose of the collection.
- Compliance is not reasonably practical in the circumstances of the particular case.
- The information will not be used in a form in which the individual can be identified or be used for historical, statistical or research purposes.

What do you think is the practical implications of Condition 6?

2.7 Condition ⑦ - Security Safeguards

2.7.1 Security measures on integrity and confidentiality of personal information

A responsible party must secure the integrity and confidentiality of personal information in its possession by taking appropriate, reasonable technical and measures to prevent-

- Loss of, damage to or unauthorized destruction of personal information.
- Unlawful access to or processing of personal information.
- The responsible party must take reasonable measures to-
    - Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control.
    - Establish and maintain appropriate safeguards against the risks identified.
    - Regularly verify that the safeguards are effectively implemented.
    - Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

The responsible party must have regard to the general accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

2.7.2 Information processed by operators

An operator is a person or entity mandated (but not employed) by a responsible party to process information.

The responsible party must have a written contract with the operator to ensure that the operator maintains the security measures. An operator must process information only with the knowledge or authorisation of the responsible party.

An operator must treat personal information which comes to their knowledge as confidential and must not disclose it unless require by law or during proper performance of their duties.

The operator must notify the responsible party immediately where there are reasonable grounds to belief that the personal information of an individual has been accessed or acquired by any unauthorized person.

2.7.3 Notification of security compromises

Where there are reasonable grounds to believe that the personal information of an individual has been accessed by an unauthorized person the responsible party must notify the Information Regulator and the individual. The individual need not to be notified if the identity of the individual cannot be established.

The notification must be made as soon as is reasonably possible. The responsible party may only delay notification if notification will obstruct a criminal investigation.

The notification must be in writing and the individual can be informed by any of the following ways:

Mailed letter | an email | communication on website | published in news media

The notification must provide sufficient information to allow the individual to take protective measures against the potential consequences of the compromise including-

- A description of the possible consequences of the security compromise.
- A description of the measures that the responsible party intends to take or has taken to address the security compromise.
- A recommendation regarding the measures to be taken by the individual to mitigate the possible adverse effects of the security compromise.
- The identity of the unauthorized person who have access the personal information - if known.

The Information Regulator may direct a responsible party to publicize the fact of any compromise to the integrity or confidentiality of personal information.

What do you think is the practical implications of Condition 7?

2.8 Condition ⑧ - Client participation

2.8.1 Access to personal information

An individual, having adequate proof of identity, has the right to -

- Request a responsible party to confirm, free of charge, whether the responsible party holds personal information about the data subject.
- Request from the responsible party the record or description of the personal information held including the identity of all third parties who have or had access to the information within a reasonable time at a prescribed fee in a form that is generally understandable.

If the responsible party charges a fee for providing information, the responsible party-

- Must give the individual a written estimate of the fee before providing the service.
- May require the individual to pay a deposit for all or part of the fee.

If a request for access to personal information is denied based on the provisions of section 30 and 60 of the Promotion of Information Act (Health Records); every other part must be disclosed.

2.8.2 Correction of personal information

An individual may in the prescribed manner request a responsible party to-

- Correct or delete personal information about the individual in its possession that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
- Destroy or delete a record of personal information about the individual that the responsible party is no longer authorised to used.

On receipt of a request the responsible party must as soon as possible adhere to the request.

If the responsible party and individual cannot reach an agreement, reasonable steps must be taken to attach to the information an indication that a correction of information was request but has not been granted.

If a change in information has been made and the changed information has an impact on decisions that have been or will be taken, the responsible party must inform each person or party to whom the information has been disclosed of those steps.

The responsible party must notify an individual of the action taken relating to the request.

2.8.3 Manner of access

The provisions of section 18 and 53 of the Promotion of Access to Information (PAIA) Act applies to requests made to correct personal information.

A request for access must be made in the prescribe form to the Information Officer at his or her address or fax number or e-mail address.

The form for a request of access prescribed must at least require the individual to-

- Provide sufficient particulars to identify the record requested and the individual.
- To state whether the record is preferred in a particular language.
- To specify a postal address or fax number of the individual in South Africa.
- How the individual would like to be informed of the outcome of the request.
- If the request is made on behalf of a person, to submit proof of the capacity in which the requester is making the request, to the reasonable satisfaction of the Information Officer.

If an individual who because of illiteracy or a disability is unable to make a written request, a request may be made verbally. The information officer must reduce all verbal requests to writing.

What do you think is the practical implications of Condition 8?

TOPIC 3 OTHER STIPULATIONS

LEARNING OUTCOMES

After studying the topic, the learner should be able to-

- Describe the conditions relating to the processing of information of children and other special information.
- Outline the role of the information officer and deputy information officer.
- Describe the stipulations imposed by the Protection of Personal Information Act relating to direct marketing, automated decision making, directories and transfer of information outside South Africa.

3.1 Processing of special personal information

A responsible party may not process personal information concerning-

- The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of an individual.
- The criminal behavior of an individual to the extent that such information relates to the alleged commission of any offence or any proceeding in respect of any offence allegedly committed by an individual or the discarding of such proceeding.

This prohibition does not apply if the-

- Processing is carried out with the consent of the individual.
- Processing is necessary for the establishment, exercise or defense of a right or obligation in law.
- Processing is for historical, statistical or research purposes to the extent that the purpose serves a public interest, or it appears to be impossible to ask for consent and processing does not affect the privacy of the individual.

The Information Regulator may upon application by a responsible party authorise the responsible party to process special information if it is in public interest and reasonable. The Information Regulator may impose conditions in this regard.

3.1.1 Authorisation concerning an individual's religious or philosophical beliefs

The prohibition on processing personal information concerning an individual's religious or philosophical belief does not apply if processing is carried out by spiritual or religious organisations of which the individual is a member. However, no personal information may be supplied to third parties without the consent of the data subject.

3.1.2 Authorisation concerning an individual's race or ethnic origin

The prohibition on processing personal information concerning an individual's race or ethnic origin does not apply if the processing is carried out to identify individuals and only when this is essential for that purpose and to comply with laws and other measures designed to protect or advance persons or categories of persons, disadvantaged by unfair discrimination.

3.1.3 Authorisation concerning individual's trade union membership

The prohibition on processing personal information concerning an individual's trade union membership does not apply to the processing by the trade union to which the individual belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union or federation. However, no personal information may be supplied to third parties without the consent of the data subject.

3.1.4 Authorisation concerning an individual's political persuasion

The prohibition on processing personal information concerning an individual's political persuasion does not apply to processing by or for an institution, founded on political principles for their members. However, no personal information may be supplied to third parties without the consent of the data subject.

3.1.5 Authorisation concerning an individual's health or sex life

The prohibition on processing personal information concerning an individual's health or sex life does not apply to the processing by-

- Medical professionals if processing is needed for the care of the individual.
- Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations if such processing is necessary for-

- Assessing the risk to be insured by the insurance company or covered by the medical scheme and the individual has not objected to the processing.
- The performance of an insurance or medical scheme agreement.
- The enforcement of any contractual rights and obligations.

(More detailed rules may be prescribed regarding processing of information for this purpose)

- Schools to provide special support for pupils regarding their health or sex life.
- Any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties.
- Any public body, if such processing is necessary regarding the implementation of prison sentences or detention measure
- Administrative bodies, pension funds or employers if such processing is necessary for –
  - The implementation of the provision of laws, pensions regulations or collective agreements which create rights dependent on the health or sex life of the individual.
  - The reintegration of or support for workers or persons entitled to benefit regarding sickness or work incapacity.

(More detailed rules may be prescribed regarding processing of information for this purpose)

This information may only be processed by responsible parties' subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision or established by a written agreement between the responsible party and the individual.

A responsible party that is permitted to process information concerning a data subject's health or sex life and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, must treat the information as confidential unless the responsible party is required by law or regarding their duties to communicate the information to other parties who are authorised to process such information.

Personal information concerning inherited characteristics may not be processed in respect of an individual from who the information concerned has been obtained unless a serious medical interest prevails, or the processing is necessary for historical, statistical or research activity.

3.1.6 Authorisation concerning individual's criminal behavior or biometric information

The prohibition on processing personal information concerning an individual's criminal behavior or biometric information does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law.

The processing of information concerning employees must take place in accordance with the rules established in compliance with labour legislation.

Biometric information definition

Biometric information means personal identification of a person based on physical, physiological or behavioral characteristics including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3.2 Processing of personal information of children

A responsible party may not process personal information concerning a child (natural person under the age of 18) except if the processing is-

- Carried out with the prior consent of a competent person.
- Necessary for the establishment, exercise or defense of a right or obligation in law.
- Necessary to comply with an obligation of international public law.
- For historical, statistical or research purposes to the extent that the purpose serves a public interest, or it appears to be impossible to ask for consent.
- Personal information which has deliberately been made public by the child with the consent of a competent person.

The Information Regulator may on application authorise a responsible party to process personal information of children if the processing is in public interest and appropriate safeguards have been put in place to protect the personal information of the child.

The Information Regulator may impose reasonable conditions in respect of this authorisation, including how a responsible party must-

- Upon request of a competent person, provide a reasonable means for that person to review the personal information and refuse to permit its further processing.
- Provide notice regarding the nature of the personal information of children that is processed, how it is processed and any further processing practices.
- Refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him/herself than is reasonably necessary given the purpose for which it is intended.
- Establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

3.3 Direct marketing

Direct marketing means to approach an individual either in person or by mail or electronic communication including automatic calling machines for the direct or indirect purpose of-

- Promoting or offering any goods or services to the individual.
- Requesting the individual to make a donation of any kind for any reason.

Any communication for purpose of direct marketing must contain:

- Details of the identity of the sender or the person on whose behalf the communication has been sent.
- An address or other contact details to which the recipient may send a request that such communications cease.

In the case of a direct marketing organisation, individuals must have *opted in*. The individual can only opt in in one of two ways:

① **The individual can give his or her explicit consent to receive direct marketing**

- This would ideally be obtained when the information is collected, but a direct marketer can also approach an individual for consent later. If it does this, it can only approach the individual once for consent.

- A direct marketer must get an individual's contact details in the first place to approach the individual for consent. Unless these contact details were in the public domain, such as a telephone directory, merely obtaining the contact details could be an infringement of POPI.

For example, if a direct marketer received a list of individuals and their contact details from a company that collects and sells marketing information, the data vendor would itself have infringed POPI by passing the list on to the direct marketer, even if the direct marketer never actually uses any of the information contained in the list. Unless the individual specifically consented to their information being passed on.

② **If the individual is a client of the direct marketer (and not of anyone else) then the direct marketer can use their information for direct marketing ONLY if all of the following conditions are met:**

- The information was obtained in the context of the sale of a product or service.

- The direct marketing will be in respect of the marketer's OWN similar goods or services.

- The client has been given a reasonable opportunity to object to receipt of direct marketing both when the data was first collected and, on each occasion, when direct marketing is made to the client. The objection must be free of charge.

The proposed consent form in the draft regulations is detailed below.

FORM 4

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017
[Regulation 6]

TO: _____ (Name and address of data subject)

FROM: _____ (Name, address and contact details of responsible party)

Contact number(s): _____

Fax number: _____

E-mail address: _____

*Dear *Mr./Ms/Dr/Adv/Prof _____*

PART A

1. In terms of section 69 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), the processing of personal information of a data subject (the person to whom personal information relates) for direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless written consent to the processing is given by the data subject. You may only be approached once for your consent by this responsible party. After you have indicated your wishes in Part B, you are kindly requested to submit this Form either by post, facsimile or e-mail to the address, facsimile number or e-mail address as stated above.

2. "Processing" means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including—

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

3. "Personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

_____ *(Signature of person authorised by responsible party)*

Full names and designation of person signing on behalf of responsible party:

*Date:*_____

PART B

I, _____(full names) hereby:

Consent to goods and services to be marketed by means of unsolicited electronic communication.

SPECIFY GOODS AND SERVICES:

SPECIFY METHOD OF COMMUNICATION: FAX

OTHERS – SPECIFY:

☐Give my consent. ☐ Do not give my consent.

Signed at ..... this ..... day of .....20……..

..... (Signature of data subject)

3.4 Automated decision making

An individual may not be subject to a decision which results in legal consequences for the individual or which affects the individual which is based solely based on the automated processing of personal information intended to provide a profile of such person including work performance, credit worthiness, reliability, location, health, personal preferences or conduct.

This provision is not applicable if the decision-

- Has been taken relating to the conclusion or execution of a contract and the request of the individual in terms of the contract has been met or appropriate measures have been taken to protect the individual's legitimate interest.
- Is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of individuals. These appropriate measures must provide an opportunity for an individual make representations about a decision and require a responsible party to provide an individual with sufficient information about the underlying logic of the automated processing of the information relating to the individual to enable that individual to make representations.

3.5 Directories

An individual who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through enquiry services in which personal information is included, must be informed, free of charge and before the information is included about the purpose of the directory and about any further uses to which the directory may possibly be put, based on search functions embedded in electronic version of the directory.

An individual must be given a reasonable opportunity to object, free of charge and in an easy manner to such use of personal information or request verification, confirmation or withdrawal of such information if the individual did not initially refuse such use.

The section does not apply to editions of directories that were produced in printed or off-line electronic form prior to the commencement of this stipulation.

If the personal information of individuals who are subscribers to fixed or mobile public voice telephonic services have been included in a public subscriber directory prior to the commencement of the POPI Act, the personal information of such subscriber may remain included in the public directory after the subscriber was informed of the purpose of the directory and about any further uses to which the directory may possibly be put, based on search functions embedded in electronic version of the directory.

3.6 Transfer of information outside South Africa.

A responsible party in South Africa may not transfer personal information about an individual to a third party who is in a foreign country unless-

- That third party is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection of information and includes provisions that relates to the further transfer of personal information to any other third parties who are in a foreign country.
- The individual consents to the transfer.
- The transfer is necessary for the performance of a contract between the individual and the responsible party or for the implementation of pre-contractual measures taken in response to the individual's request.

- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the responsible party and the third party.

- The transfer if for the benefit of the individual and it is not reasonably practical to obtain the consent of the individual and if practical, the individual would have been likely to give consent.

3.7 Information Officer

The Promotion of Access to Information Act (PAIA) automatically designates a person in each organisation as the Information Officer – historically, referred to as the Information Protection Officer or Privacy Officer.

Every organisation must have an Information Officer and no entity is exempt under PAIA from this requirement. The POPI Act requires that the Information Officer also be registered with the Information Regulator as such as this will be the person designated to ensure compliance of the organisation with the POPI Act.

An information officer's responsibilities include the following:

- The encouragement of compliance with the conditions for the lawful processing of personal information. The draft regulations state that the Information Officer must ensure that a compliance framework is developed, implemented and monitored.

- Dealing with requests made to the responsible party by individuals. The draft regulations state that the Information Officer must develop internal measures together with adequate systems to process requests for information or access thereto.

- Working with the information Regulator in relation to investigations conducted.

- Ensuring compliance by the responsible party with the provisions of the POPI Act. The draft regulations state that the Information Officer must ensure that awareness session is created regarding the provisions of the Act, regulation and codes of Conduct.

These duties can be delegated to deputy Information Officers. Responsible parties must designate such number of persons as deputy information officers as are necessary to process requests pertaining to personal information. The Information Officer has direction and control over every deputy Information Officer.

Any power or duty delegated must be exercised or performed subject to such condition as the Information Officer considered necessary.

Delegation of duties must adhere to the following prescriptions:

- Delegation must be in writing.
- Delegation must not prohibit the Information Officer from exercising the power concerned or performing the duty concerned himself.
- The delegation may at any time be withdrawn or amended in writing by that person.

Any right or privilege acquired, or any obligation or liability incurred because of a decision in terms of a delegation is not affected by any subsequent withdrawal of amendment of that decision.

3.7.1 Who should the Information Officer be?

The Information Officer can be selected from the following positions:

- The chief Information Officer
- The IT Manager
- The information Security Officer
- The Compliance Officer

It is advisable to have at least one Information Officer that is responsible for the compliance processes and oversight. Two or more deputies can assist with requests. It is best practice to make one deputy responsible for requests in terms of the Promotion of Access to Information (PAIA) Act and the other for requests in terms of the POPI Act.

It is especially important to appoint the Information Officer and deputies correctly by clarifying their responsibility in their letter of appointment.

3.8 Protection of Personal Information Manual

The Information Officer must develop a Protection of Personal Information Manual detailing the following:

- The purpose of the processing of information.
- A description of the categories of data subjects and of the information or categories of information relating to them.
- The recipient or categories of recipients to whom the personal information may be supplied.
- The planned trans-border or cross border flows of personal information.
- A general description allowing preliminary assessment of the suitability of information security measures to be implemented and monitored by the responsible party.

The manual must be available on the website of the responsible party and must be available at all offices of the responsible party for public inspection during normal business hours.

Copies of the manual must be provided on request at a cost of not more than R3.50 per page.

TOPIC 4 ENFORCEMENT

LEARNING OUTCOMES

After studying the topic, the learner should be able to-

- Describe the process should the stipulation under the Protection of Personal Information Act not be complied with or personal information of a data subject be compromised.

4.1 Complaints

Interference with the protection of personal information of an individual is a breach of the conditions stipulated under the POPI Act or non-compliance with any Code of Conduct issued in terms of the POPI Act.

Any person may submit a complaint in writing to the Regulator alleging interference with the protection of personal information of an individual.

The Information Regulator, may on its own initiative start an investigation into the interference with the protection of personal information of an individual.

The Information Regulator must as soon as possible advice the complainant and the responsible party of the course of action taken.

The Information Regulator has the discretion to refer the complaint to another Regulatory Body.

4.2 Investigations

Before starting to investigate any matter, the Information Regulator must inform-

- The complainant, the individual and any person alleged to be aggrieved of the Information Regulator's intention to conduct the investigation.
- The responsible party of the details of the complaint and the right to submit to the Information Regulator, within a reasonable period, a written response in relation to the complaint.

The Information Regulator may, if it appears from a complaint or the response of the responsible party, secure a settlement between any of the parties concerned and if appropriate obtain a satisfactory assurance against the repetition of any action that is the subject matter of the complaint.

For the purposes of the investigation of a complaint the Information Regulator may-

- Summon and enforce the appearance of persons before the Information Regulator and compel them to give verbal or written evidence on oath and to produce any records that the Information Regulator deems necessary to investigate the complaint.
- Receive and accept any evidence and other information relevant.
- At any reasonable time enter and search any premises occupied by a responsible party and interview any person on the premises by virtue of a warrant issued by a magistrate or a judge.

A responsible party or individual may submit a complaint to the Regulator in the prescribed manner and form if he, she or it is aggrieved by the determination of an adjudicator.

4.3 Assessments

Any person can request the Information Regulator to assess a company's protection of personal information practices. The Information Regulator can also make an assessment on its own initiative as well. The Information Regulator must inform the responsible party if it has decided to conduct an assessment.

After completing the assessment, the Information Regulator must report to the responsible party the results of the assessment and any recommendations that the Information Regulator considers appropriate and may require the responsible party to inform the Information Regulator of any action taken or proposed to be taken to implement the recommendation.

The Information Regulator may make public any information relating to the personal information management practices of a responsible party that has been subject to an investigation.

A report made by the Information Regulator is deemed to be the equivalent to an enforcement notice.

4.4 Matters referred to the Enforcement Committee

After completing the investigation of a complaint or other matter, the Information Regulator may refer such complaint or matter to the Enforcement Committee for consideration and recommendation in respect of the proposed action to be taken by the Information Regulator.

All parties must be informed of developments during and as result of an investigation.

If the Information Regulator, after having considered the recommendation of the Enforcement Committee, is satisfied that a responsible party has interfered or is interfering with the protection of personal information of an individual, the Information Regulator may serve the responsible party with an enforcement notice to do either or both of the following:

- To take specified steps within a period specified in the notice.
- To stop processing personal information specified in the notice or to stop processing personal information for a purpose or in a manner specified in the notice within a specified period.

A responsible party on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal may be brought against that notice, apply in writing to the Information Regulator for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the conditions for the lawful processing of personal information.

If the Regulator considers that all or any of the provisions of an enforcement notice need not be complied with to ensure compliance with a condition for the lawful processing of personal information or conditions to which it relates, it may cancel or vary the notice by written notice to the responsible party on whom it was served.

A responsible party on whom an information or enforcement notice has been served may, within 30 days of receiving the notice, appeal to the High Court for the setting aside or variation of the notice.

4.5 Civil Remedies

An individual my institute a civil action for damages in a court against a responsible party for the breach of any provisions of the POPI Act whether there is intent or negligence on the part of the responsible party.

The court may award an amount that is just and equitable, including-

- Payment of damages as compensation for patrimonial and non-patrimonial loss.
- Aggravated damages, in a sum determined in the discretion of the Court.
- Interest.
- Cost of suit on such a scale as may be determined by the Court.

If a client suffers any loss because of a breach in the conditions, the responsible person will be strictly liable for this loss. In other words, it does not matter if the responsible person was negligent or acted intentionally in breaching POPI – if the breach caused loss to the client, the responsible person is liable. Furthermore, the organisation will also suffer considerable reputational damage.

The responsibility is also on the organisation to prove that the information was not compromised in any way.

Be aware: Simple actions like synchronizing your contacts on your phone, sending an email with sensitive content, taking or sharing a video or photo can be considered a breach of the POPI Act!

4.6 Offences and penalties

4.6.1 General offences

Any person who hinders, obstructs or unlawfully influences the Information Regulator or any person acting on behalf of or under the direction of the Information Regulator in the performance of the Information Regulator's duties and functions, is guilty of an offence.

Failure to comply with an enforcement notice is an offence.

A responsible party which in supposed compliance with an information notice make a statement knowing it to be false or recklessly makes a statement which is false is guilty of an offence.

4.6.2 Offences by witnesses

Any person summoned to attend and give evidence or to produce any document or object before the Information Regulator, is guilty of an offence, if the person without sufficient cause fails-

- To attend at the time and place specified in the summons.
- To remain in attendance until conclusion of the proceeding or until excused.
- Having attended, refuses to be sworn or to make an affirmation as witness after he or she as has been required by the Chairperson to do so.
- To answer fully and satisfactorily any question lawfully put to him or her.
- To produce any book, document or object in his or her possession or custody or under his or her control, which he or she has been summoned to produce.

Any person who after having been sworn or having made an affirmation, gives false evidence before the Regulator knowing such evidence to be false is guilty of an offence.

4.7 Unlawful acts by a responsible party regarding an account number

A responsible party who process an account number of an individual unlawfully is guilty of an offence if the contravention is of a serious or persistent nature and is likely to cause substantial damage or distress to the individual.

The responsible party must have known that there was a risk that such contravention would occur, or such contravention would like cause substantial damage or distress. The responsible party must have failed to take reasonable steps to prevent the contravention.

4.8 Unlawful acts by third parties relating to an account number

A person who knowingly or recklessly, without the consent of the responsible party obtains or discloses an account number of an individual is guilty of an offence unless the disclosure was necessary for the prevention, detection, investigation or proof of an offence or is required or authorised in terms of law to disclose the account number.

A person who sells or offer to sell an account number which he or she has obtained is guilty of an offence.

4.9 Administrative fines

If a responsible party is alleged to have committed an offence in terms of the POPI Act, the information Regulator may deliver an infringement notice to that person – referred to as the infringer.

An administrative fine not exceeding R10 million can be imposed. The infringer has 30 days after the notice has been served to pay the fine. The infringer can arrange with the Information Regulator to pay the fine in instalments. Alternatively, the infringer can elect to be tried in court on a charge of having committed the alleged offence.

If an infringer elects to be tried in court on a charge of having committed the alleged offence in terms of the POPI Act, the Information Regulator must hand the matter over to the South African Police Service and inform the infringer accordingly.

If the infringer does not pay the fine within the specified time frame, the Information Regulator may file with the clerk of the court a statement for a writ of execution to be issued.

The Information Regulator may not impose an administrative fine if the responsible party concerned has been charged with an offence in terms of the POPI Act in respect of the same set of facts.

No prosecution may be instituted against a responsible party if the responsible party concerned has paid an administrative fine.

An administrative fine imposed in terms of this section does not constitute a previous conviction as contemplated in Chapter 27 of the Criminal Procedure Act.

Failure to comply can lead to fines of R10 million and imprisonment of 10 years