Manual in terms of Protection of Personal Information Act 4 of 2013

1. Introduction

The right to privacy is protected in terms of section 14 of the Constitution of South Africa 1996. *Section 14.-*
Everyone has the right to privacy, which includes the right not to have -
a)Their person or home searched,-
b)Their property searched,-
c)Their possessions seized,- or
d)The privacy of their communications infringed.

The Protection of Personal Information Act 4 of 2013 (POPIA) has four main aims:

1. To carry into effect the Constitutional right to privacy through the protection of personal information that may be processed by a responsible party.
2. To provide the minimum requirements for the lawful processing of personal information.
3. To ensure that personal information is not abused by providing rights and remedies.
4. To establish the Information Regulator.

All public and private institutions, companies or organisations processing personal information must ensure compliance with the POPIA by 1 **July 2021.**

2. Definitions

The data subject
Person or Party to whom the personal information relates.

The responsible party

Person or Party that determines the purpose of and means for the processing of the information of the data subject.

Operator
Person or Party who processes personal information on behalf of the Responsible party in terms of a contract under the direct authority of that party.

Processing
Everything that is done with Personal Information including collection, sharing, storage, modification, destruction etc.

Competent Person

A natural or juristic person who is able to give voluntary, specific and informed consent.

Information Officer
A person who is responsible for the overall POPI compliance and lawful processing of personal information within the entity.

Information Regulator

Juristic person or independent body which has jurisdiction throughout South Africa. The information regulator must exercise its powers and perform functions in accordance with the Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA). Some of the information regulator's duties include to provide education, to monitor and enforce compliance, to consult with interested parties, to handle complaints, to conduct research and to facilitate cross-border cooperation.

Personal information
Any and all 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, co|our, 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.

Record

Any recorded information in the possession or control of a Responsible party, regardless of how it came into existence. Some examples of records include:

- Writing on any material;
- Information produces, recorded or stored by means of tape-recorder, computer equipment (hardware, software or both) or any other device;
- Label, marking, other writing, that identifies/describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph of drawing;
- Photograph, film, negative, tape, or any other device one or more visual images are able to be reproduced.

Direct Marketing

To approach a data subject, either in person; by mail or electronic communication for the direct or indirect purpose of promoting/offering to supply any goods or services to the data subject.

Or

Requesting the data subject to make a donation of any kind for any reason.

3. Exclusions

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

- If information relates to personal / household activity,
- If information has been de.-identified and cannot be re.-identified again,
- If information is processed by or on behalf of a public body for purposes that:
  - Involves national security ,
  - Identification of financing of terrorists and related activities ,
  - Defence/public security ,
  - Protection against unlawful activities ,
  - Combating of money laundering activities ,
  - Investigation and proof of offences ,
  - Prosecution of offenders
- If information is needed by Cabinet and its committees or Executive Council of a Province,
- If information is relating to judicial functions of a court , or
- If exemptions have been granted by the Information Regulator.

4. Personal Information may be processed if:

- Voluntary, specific, and informed consent from data subject is acquired.
- Information is necessary in the performance of a contract to which data subject is a party to.
- An obligation imposed by a Responsible Party by law.
- Legitimate interest of data subject exists.
- Legitimate interest of Responsible Party or 3rd party to whom PI was supplied.
- Information is necessary for performance of a public duty by a public body.

5. Lawful Processing

5.1 Accountability

The Responsible party must ensure compliance with the conditions for lawful processing regarding both the usage and protection of personal information. These conditions include appointing an Information Officer and compiling a POPIA Manual.

Appointing an Information Officer:
All public and private institutions, companies or organisations must appoint and register an Information Officer as set out in the Act.

POPIA Manual:
All public and private institutions, companies or organisations must compile a manual detailing information on the collection, usage, storage and destroying of data. The manual must also detail all relevant information for awareness training of all personnel on the Act.

5.2 Processing limitation

Personal Information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

Minimality principle:
Responsible party must only take adequate, relevant and non.-excessive information.

Consent:
Voluntary, specific, and informed consent from data subject to the processing of information.

Justification:
Processing is necessary to carry out actions for contract where data subject is party to, complies with a legal obligation on the Responsible Party, protects a legitimate interest of the data subject, is necessary for proper performance of a public law/duty by public body, and/or is necessary for pursuing legitimate interest of the responsible party.

Objection:

The Data subject may object to the processing of personal information on reasonable grounds. When this occurs, the Responsible party may no longer process the personal information.

Collection
Data must be collected directly from the data subject, except when information is from a public record or was made public by data subject or when the data subject consented to collection of data from another source.

5.3

Purpose specification

Personal information must be collected for a specific, explicitly defined and lawful purpose which must be related to a function/activity of the responsible party. Steps must be taken to ensure the data subject is aware of the purpose of collection of the information or data.

Retention period:

Personal information may not be retained for any longer than necessary for the original purpose for which it was collected, except where a specific law regulates how long the data should be kept. The responsible party must destroy or delete a record of personal information or de-identify as soon as reasonably practical after they are no longer authorized to retain the record.

Further processing limitation

5.4 Personal information or data collected must be in accordance or compatible with purpose for which it was collected. To assess compatibility between information collected and the purpose thereof:

There must be a clear relationship between further processing and

1) the reason data was collected,
2) the nature of information concerned,
3) any consequence of intended further processing ,
4) the manner in which data was collected, and
5) the contractual rights/obligations between the parties.

Further processing is compatible with purpose of collection if:
The data subject consented to further processing,
Information is available from public records, or
Further processing is necessary for the following reasons:

- Legal obligation,
- Court order,
- Interest of national security,
- Prevent serious/imminent threat to public health or safety,
- Research/statistical purposes.

Information quality

5.5 Information must always be as complete and accurate as possible. Information that needs to be updated regularly to be accurate, has to follow the necessary guidelines of updating personal information as set out in the framework.

5.6

Openness

The responsible party must maintain documentation of all processing procedures and must give notice to the data subject when collecting personal information.

The responsible party must take reasonably practical steps to ensure that the data subject is aware of:
The information collected and the source from which the information was collected ,
The purpose of collection of information ,
The responsible party's name and address ,
Is the data collection done in terms of legal obligation ,
Any consequences with the failure to provide information ,
The responsible party intent to use data outside of the Republic of South Africa,
Any other relevant information.

5.7

Security safeguards

Responsible parties must at all times apply appropriate, reasonable, technical and organisational steps to secure integrity and confidentiality of personal information or data in its possession or under its control.

To prevent loss, damage or unauthorised destruction of personal information or unlawful access/processing of personal information, the responsible party must take reasonable steps to:

- Identify reasonably foreseeable internal and external risks,
- Establish and maintain appropriate safeguards against such risks,
- Regularly verify that safeguards are effectively implemented, and
- Ensure safeguards are continually updated against new risks.

Security breach:

In the case of a security breach the responsible party must firstly report the data breach to the Information Regulator and the data subject. The responsible party must also make a report when there is a reasonable belief that a breach occurred or when an unauthorised person has acquired or accessed personal information.

Notification of the breach or possible breach must be made within reasonable period after discovery of the breach. Sufficient information must also be provided to the data subject to allow it to take protective measures as result of the breach.

If breach affects the public, the Information Regulator will direct how the notification must be published.

5.8

Data subject participation

A data subject has the right to access personal information, the right to the correction of personal information and the right to request personal information to be deleted or destroyed.

Furthermore, the data subject is entitled to know what personal information is held by the responsible party, proof of consent to process personal information and to be advised on incorrect personal information that needs to be corrected.

Failure to comply with any condition:

In case of interference with the right to protection the transgressor can be issued with an infringement notice and administrative fine. The fine amount and conditions will be determined by the information regulator.

6. Information Officer

Every organisation processing personal information must appoint an information officer, enrolled at the information regulator.

Duties of Information officer include:

Ensure compliance with conditions of /at/|/]Fu/ *processing* of personal information ,
Ensuring compliance with all other provisions of POPIA ,
Dealing with requests made to company regarding POPIA , and
Working with the Regulator relating to investigations against/by company.

The responsible party must register the information officer with the information regulator before they take up their duties.

7. Enforcements: complaints: penalties

7.1 Enforcements

Interference with protection of personal information of a Data Subject includes:

- Breach of conditions of lawful processing ,
- Non.-compliance , or
- Breach of provisions of a code of conduct issued by the Information Regulator.

7.2 Complaints

Any person may submit a complaint concerning alleged interference of protection of personal information to the Information Regulator. Such complaints must be in writing. Upon receipt of a written complaint, the Information Regulator will either launch a pre-investigation, decide to take action or no further action required, conduct a full investigation or refer the complaint to the Enforcement Committee.

7.3 Offence / Penalties / Administrative fines

Various penalties, imprisonment and fines are prescribed for offences. Administrative fines determined by the Information Regulator. The Magistrate's Court has jurisdiction to impose penalties.