selekane
ASSET CONSULTANTS

POPIA
INFORMATION GOVERNANCE MANUAL

Ground Floor | Lansdown House | Hampton Park | 20 Georgian Crescent | Bryanston | 2152 | Post Net Suite 344| Private Bag X75
Bryanston |2021| Tel: 011 514 0018 | Fax: 011 463 4659 | www.selekane.co.za | Authorised Financial Services Provider (FSP: 29848)

LEGISLATIVE & COMPLIANCE FRAMEWORKS WITH INTERNAL POLICIES FOR THE PROTECTION OF PERSONAL INFORMATION

This framework outlines the processes and related policies and procedures in the pursuit of compliance within the Protection of Personal Information Act of 2013 (POPIA).

This POPIA Framework must be read with the legislative framework already provided as background and it must be seen as one document.

The purpose of this framework is to enable Selekane Asset Consultants (Selekane) to:

- To ensure compliance with all applicable legislation regarding the protection of personal information of identifiable individuals (employees, clients and other third parties).
- Follow the principles of good practice and treating clients fairly.
- Protect Selekane and the individuals on whose behalf data is collected, processed, distributed, disclosed, and stored.
- Protect Selekane from the consequences of a breach and related fines and penalties.

Personal Information: This framework applies to the protection of personal information (note definition of personal information in legislative framework) relating to identifiable individuals, both natural and juristic.

Framework (Policy) Statement: Selekane will:

- Endeavor to comply with the legal requirements of POPIA and the relevant Regulations as well as the principles of good practise and treating clients fairly.
- Respect individuals' rights to privacy and the protection of their personal information (data) which is collected, processed, distributed, disclosed, and held by Selekane.
- Be open and honest with the relevant individuals whose personal information (data) is collected, processed, distributed, disclosed, and held.
- Provide training and support to all employees who deals with personal information so that they can act confidently and consistently.

Selekane recognises that it is the first priority of POPIA to avoid causing harm to individuals. Therefor it will endeavour to:

- Keep information (data) securely in the right hands; and
- Retain good quality information (data).

The scope of framework applies to all the operations and business practices of Selekane wherever it is conducted but based at the registered offices and branches. It applies to all employees as per the effective date.

As the Key Individuals of Selekane, we hereby confirm the adoption of this policy as part of Selekane's internal control structure and procedures.

Mxolisi Mbekwa

Lindi Moabi

Date: 25 June 2025

1. DOCUMENT DETAILS

1.1 Background:

This POPIA Manual provides a compliance framework and internal policies and procedures for meeting the legislative requirements in terms of the protection of personal information and to manage the associated compliance risks effectively and efficiently. The framework will ensure the appropriateness and consistency of approach between the external compliance requirements and internal policies and procedures. It is used to establish a structured approach to continuously improve the many technical and complex requirements of the Protection of Personal Information Act.

1.2 Purpose & Objective:

A POPIA compliance framework provides a monitoring capability to manage compliance with the obligations of the Protection of Personal Information Act to ensure compliance with the conditions for the lawful processing of personal information.
The Information Regulator has extended the duties and responsibilities to ensure a suitable compliance framework is implemented. Responsible parties will have to demonstrate compliance to a wide range of legal obligations that include:

- Keeping documentation that can be used later to demonstrate accountability.
- Clarifying the roles, responsibilities and accountability obligations of responsible parties using risk-based approaches to data protection and the implementation of protective measures which correspond to the level of risk of processing personal data so that the fundamental rights and freedoms of data subjects are protected.
- Supporting information officers and their efforts to achieve strong data protection compliance and establish effective privacy programmes.
- Providing effective governance of processors and third parties operating under the authority of the responsible party.
- Pro-actively identifying and tracking procedural or training weaknesses in an effort to preclude regulatory violations.

2. LEGISLATIVE FRAMEWORK

2.1 What is POPIA:

The intention of the Protection of Personal Information Act (POPIA) is to bring South Africa in line with international standards of protection of personal information and will radically change the way in which both government and business deal with individuals' private information. POPIA sets conditions for what companies and individuals must and may do with personal information about their employees, clients and other third parties.

2.2 Personal Information:

The definition of personal information is all encompassing and includes biometric information. Basically, if information can identify someone, it is deemed personal. In the financial services industry, Financial Service Providers and their staff receive (as an example) application forms, claims and premiums data that contain a host of information such as names, identity numbers, staff numbers, addresses, tax numbers, banking details, health information etc. All of this is personal information, so POPIA is applicable to all Financial Services Providers.

2.3 Important Definitions:

- **Biometrics:** means a technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.
- **Consent:** means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.
- **Data Subject:** means the person to whom personal information relates.
- **De-identify:** means to delete all information that identifies the data subject.
- **Information Officer:** in relation to a private body means the head of a private body or any person duly authorised by that person.
- **Operator:** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
- **Personal Information:** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.
- **Person:** a natural or juristic person.
- **Processing:** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal Information.
- **Public Record:** means a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
- **Regulator:** means the Information Regulator.
- **Re-identify:** means to resurrect any information that has been de-identified, that identifies the data subject.
- **Record:** means any recorded information regardless of form or medium.
- **Responsible Party:** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
- **Special Personal Information:** the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject. The prohibition on processing special personal information does not apply if the processing is carried out with the consent of a data subject or if processing is necessary for the establishment, exercise, or defence of a right or obligation in law or information has deliberately been made public by the data subject.

2.4 Rights of Data Subjects:

A Data Subject has the right to -

- Have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information including the right to be notified that personal information about him, her or it is being collected; and his, her or its personal information has been accessed or acquired by an unauthorised person.
- Establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information.
- Request, where necessary, the correction, destruction, or deletion of his, her or its personal information.
- Object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information.
- Object to the processing of his, her or its personal information at any time for purposes of direct marketing.

2.5 Conditions for Data Collection:

Condition 1: Accountability:

Selekane aims to ensure that all principles and measures of the Act are complied with during the collection and processing of personal information.

Condition 2: Processing limitation:

Processing must be done lawfully and not infringe the privacy of the individual. Processing of personal information must be adequate, relevant, not excessive, given the purpose for which it is to be used.

Personal information may only be processed:

- If the data subject or a competent person where the data subject is a child consent to the processing.
- Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party.

The responsible party bears the burden of proof for the data subject's or competent person's consent. The data subject or competent person may withdraw his, her or its consent at any time or object to the processing of personal information and the responsible party may then no longer process the personal Information.

Personal information must be collected directly from the data subject unless:

- The information is contained in or derived from a public record or has deliberately been made public by the data subject.

- The data subject or a competent person where the data subject is a child has consented to the collection of the information from another source.

Condition 3: Purpose Specification:

Personal information must only be collected for a specific purpose, and the individuals must be aware of this. Records must not be kept for longer than necessary to achieve the purpose for which it was collected. Legislative requirements (FICA & FAIS) must be adhered to. A responsible party must destroy or delete a record of personal information as soon as reasonably practicable after the responsible party is no longer authorised to retain the record. It must be done in a manner that prevents its reconstruction in an intelligible form.

Condition 4: Further Processing Limitation:

Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in the first place.

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 data subject.
- The manner in which the information has been collected.
- Any contractual rights and obligations between the parties.

Condition 5: Information Quality:

We must take reasonable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary, always considering `the purpose for which the information was initially collected or further processed.

Condition 6: Openness:

We maintain the documentation of all processing operations under its responsibility. We take reasonably practicable steps to ensure that the data subject is aware of:
- The information being collected or 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 is voluntary or mandatory.
- The consequences of failure to provide the information.
- Any particular law authorising or requiring the collection of the information.
- The fact that, where applicable, 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.

Conditions 7: Security Safeguards:

We secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent:

- Loss of, damage to or unauthorised destruction of personal information, as set out in our **Business Continuity and Disaster Recovery Plan**.
- Unlawful access to or processing of personal information. An operator or anyone processing personal information on behalf of a responsible party or an operator, must process such information only with the knowledge or authorisation of the responsible party. Our IT Appropriate Use standard is set out in our **IT Governance and Security Policy (Par 6).**

Condition 8: Data Subject Participation:

The data subject can request whether an organisation holds their private or personal information, and what information is held. They may also request a responsible party to correct or delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully. The responsible party must adhere to the request of the data subject as soon as possible and inform the data subject of the action taken as a result of the request.

2.6 Special Personal Information:

The following information may not be processed without consent of the data subject or unless allowed by law:

1. Religious or philosophical beliefs
2. Race or ethnic origin
3. Trade union membership
4. Political persuasion
5. Health or sex life
6. Biometric information
7. Criminal behaviour relating to alleged offences.

2.7 Children:

No personal information of a child (under 18) may be processed without consent of a competent person or unless allowed by law.

2.8 Information Regulator and Information Officer:

The information regulator's powers, duties and functions in terms of POPIA are:

(a) to educate
(b) to monitor and enforce compliance
(c) to consult
(d) to handle complaints
(e) to conduct research and report to parliament
(f) to issue codes of conduct
(g) to facilitate cross-border co-operation
(h) other general duties for example matters relating to the access of information as provided by PAIA.

In light of the duties imposed by POPIA we have appointed an information officer (and deputy information officer where appropriate). Registration of Information Officers with the Regulator is a prerequisite for Information Officer to take up their duties in terms of POPIA and PAIA.

Our information officer's responsibilities and duties include:

- The encouragement of compliance with the conditions for the lawful processing of personal information.
- Dealing with requests made pursuant to this Act.
- Working with the Regulator in relation to investigations.
- Ensuring compliance with the provisions of this Act.
- Develop, implement, and monitor a compliance framework.
- Ensure that adequate measures and standards exist.
- Conduct preliminary assessments.
- Develop a manual for the purpose of the Promotion of Access to information Act and the POPl Act.
- Develop internal measures and adequate systems to process requests for access to information.
- Conduct awareness sessions.

Information officers must take up their duties after the responsible party has registered them with the Regulator. The POPIA information officer would be –

- In the case of a sole practitioner - the sole practitioner or any person duly authorised by the sole practitioner.
- In the case of a partnership - any partner of the partnership or any person duly authorised by the partnership.
- In the case of an incorporated practice - the chief executive officer or a person duly authorised by the chief executive officer.

One of the primary functions of the information officer is the receipt, processing and determining whether access to information held by the private body should be granted.

A Deputy Information Officer(s) should have a reasonable understanding of the business operations and processes of a body.

2.9 Prior Authorization:

Prior authorisation is necessary where the responsible party plans to process information:

- Which contains any unique identifiers of data subjects for a purpose other than the one specifically intended at collection and with the aim of linking the information being processed with information processed by other responsible parties.
- In respect of criminal, unlawful or objectionable conduct.
- For the purpose of credit reporting.
- That is defined as special personal information or is the information of a child which is being transferred to a foreign country that does not provide an adequate level of protection in its law.

The Regulator may require prior authorisation if the processing carries a risk to the legitimate interests of the data subject. The authorisation only must be obtained once for a particular category of processing but if the manner of processing changes, then a further application to the Regulator for authorisation will be necessary.

2.10 Consequences of Infringement:

POPIA makes provision for enforcement notices to be served on those infringing the data protection principles or the direct marketing provisions of POPI. Failure to comply with an enforcement notice is an offence, and on conviction may lead to a fine of not more than R10 million, or up to 10 years in prison, or both.

2.11 Direct Marketing:

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of - promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or requesting the data subject to make a donation of any kind for any reason.

We do not provide any direct marketing, as per our FAIS licensing conditions.

2.12 Cross-border Information Flow:

Section 72 of POPIA requires that in order for cross-border transfers of personal information to be permissible, one of the following must be present:

Adequate legal protection:

The recipient of the personal information must be subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that effectively upholds the principles for reasonable processing, and that include provisions that are substantially similar

to the conditions for the lawful processing of personal information and for the further transfer of personal information.

Consent:

The data subject consents to the transfer.

Necessary for the performance of a contract:

The transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request.
Interests of the data subject: The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.

Benefit of the data subject:

The transfer is for the benefit of the data subject in circumstances where it is not reasonably practicable to obtain the consent of the data subject for the transfer, and the data subject would be likely to give consent had it been obtained.
These are not cumulative requirements, and only one of the above would need to be present in order for the cross-border data transfer to pass muster.

2.12 Staff Training and Acceptance of Responsibilities:

Employees will be required to attend training; disciplinary actions will be taken against employees who do not comply with the provisions of the Act.

3 KEY RISKS

We have identified the following potential key risks, which this framework is designed to address:

- External breach of privacy and confidentiality with subsequent loss to the individual and Selekane via for example hacking etc.
- Internal breach of privacy and confidentiality with subsequent loss to the individual and Selekane via for example unauthorised access or unauthorised disclosure etc.
- Consent process followed with individuals not meeting all requirements in terms of collecting, processing, distribution, disclosure, and storage of personal information with subsequent complaints received.
- Other non-compliance issues leading to Regulatory action with subsequent fines and penalties.

- Legal and compliance documentation such as employment contracts, service level agreements, application forms etc not brought in line with POPIA with subsequent accountability and responsibility issues.
- Keeping Client information past the recommended period of 5 years.

Selekane will endeavour to comply with all relevant conditions of POPIA and related Regulations. To oversee Selekane's compliance in this regard an Information Officer is appointed and registered with the Information Regulator.

4 IMPACT ASSESSMENT

Selekane may apply an impact assessment on the business focussing on the following areas:

ACCOUNTABILITY. Roles and responsibilities must be clearly set out both internally and when information is shared with third parties. Senior management must oversee information gathering process and should delegate responsibilities to appropriate individuals (information custodians). Standards and procedures must be put in place to ensure that the level of information gathering can be audited.

STANDARDISATION. Business processes and activities must be well-defined and documented in an open and verifiable way. The documentation must be available to employees and appropriate third parties.

INTEGRITY. The right processes are in place to guarantee that the institutional information we use or manage is comprehensible, clear, consistent, and reliable.

SECURITY. Confidential and personal information must be protected from unauthorised destruction, modification, or access.

COMPLIANCE. Good information governance promotes and facilitates compliance with internal policies, applicable legislation, or other binding rules.

AVAILABILITY. Information must be available to the appropriate people at the appropriate time.

RECORDS MANAGEMENT. Information will be retained for an appropriate time only, taking into account legal, regulatory, fiscal, operational, and historical requirements. Once the retention periods have passed, information is disposed of securely.

EMPOWERMENT. The Business' employees must be empowered through training to work responsibly with information and to protect it. In the process, they will empower their staff to protect their own privacy.

5 Contact Information

If you have questions and/or comments about our privacy policy or need to protect any of your rights set out in this policy, please contact our information officer on email address info@selekane.africa or telephone number 011 514 0018.

Our physical address is:

Ground Floor, Lansdown House
Hampton Park
20 Georgian Crescent
Bryanston
2152

If you would like to lodge a complaint, please contact the Information Regulator on email address complaints.IR@justice.gov.za