POPIA POLICY MANUAL

[Document subtitle]

Abstract

The Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA) govern the way that businesses collect, store, access and destroy personal client information in a safe and secure manner. The initial deadline for businesses to comply with these Acts was 1 July 2021. Customer and supplier information kept at PCS Global does not only include personal details, but the nature of this may also be extremely sensitive and intimate. All companies, regardless of size, are required to be POPIA and PAIA compliant. All staff are strongly advised to familiarise themselves and to comply with these Acts, as serious consequences may arise if a practice or institution is found guilty of non-compliance.

Sabin Nair
info@pcsglobal.com

CONTENTS

1. SCOPE

- This policy intent to set out principles in relation to POPIA and is applicable across the organization to all employees, including the organization's subsidiaries, consultants, service providers, stakeholders, members of the Board and concessions where the exchange of personal information is warranted.
- The policy also applies to the processing of personal information entered in a record by making use of automated or non-automated means.

2. OBJECTIVE

- To provide guidance on how the organization must comply with the obligations created by the
  protection of Personal Information Act 4 of 2013.
- To set out POPIA conditions and other POPIA compliance requirements and clarify key responsibilities and obligations of the various role players in [insert company name]

3. DEFINITIONS AND ABBREVIATIONS

3.1 DEFINITION

- **Act -** Protection of Personal Information Act 4 of 2013.
- **Conditions** - Conditions of Lawful Processing stipulated in Chapter 3 of the Act.
- **Constitution** - Constitution of the Republic of South Africa 1996.
- **Data Subject** - Means the person to whom the personal information relates. This includes customers, employees, suppliers, contractors, vendors, third parties and stakeholders.
- **De-identification** - Is the process used to prevent a person's identity from being connected with information.
- **Employee** - An officially appointed person to [insert company name], irrespective of the duration or nature of their appointment - permanent or temporary.
- **Information Officer** - The designated employee within the organization responsible for ensuring that the organization complies with POPI Act; the role is prescribed in the Act.
- **Information Regulator** - The Information Regulator (South Africa) is an independent body established in terms of section 39 of the Protection of Personal Information Act 4 of 2013. The Information Regulator is responsible for protecting data subjects against harm and to ensure that their personal information is protected by responsible parties.

- Organization

[insert company name]

- **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.
- **Process** - means any operational activity concerning personal information including the collection, organization, storage, modification, communication, and destruction of information.
- **Personal Information** - means information relating to the identifiable, living, natural person and where it is applicable, and identifiable juristic person, including but not limited to information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic, or social conscience, belief, culture, language and birth of a person. Information relating to the education or the medical, financial, criminal or employment history of the person, any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person. The biometric information of a person, the personal opinions, views or preferences of the person, the views or opinions of another individual about the person, 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 and the name of the person if it appears with other personal information relating thereto.
- **Record -** means any recorded information in whatever form in possession or under the control of.

[insert company name].

3.2 ABBREVIATIONS

Abbreviation Description:

- POPIA - Protection of Personal Information Act
- PAIA - Promotion of Access to Information Act
- PI - Personal Information
- GDPR - General Data Protection Regulation
- IO - Information Officer

4. POLICY GENERAL

- The right of privacy is enshrined in the South African Constitution which expressly states that everyone has the right to privacy. The POPI Act is aimed at facilitating the protection of this important right.
- This policy establishes measures and standards for the protection and lawful processing of personal information within the organization and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.
- The organization shall comply with both the law and good practice, respect individuals' rights to privacy, be open and honest with individuals whose data is held, provide training and support for staff who handle personal data, so that they can act confidently and consistently protect personal information and keeping information securely.

4.1 MAIN PRINCIPLES OF CONDUCT

4.1.1 EIGHT CONDITIONS OF POPIA ACT

- POPIA places a responsibility on the organization to promote the lawful processing of personal Information and its service providers who act on behalf of the organization.
- POPIA consist of eight conditions which are adopted by the organization as principles guiding the organization to comply with the obligations created by the POPIA.

The conditions are as follows:

- **Condition 1 – Accountability**
  The Organization is accountable and responsible for personal information in its possession at an organizational level and shall comply with all the 8 POPIA conditions, including its operators and subsidiaries. Divisions and Departments are accountable and responsible for personal information they process in their respective business units. Each employee is responsible to comply with POPIA, POPIA Policy and POPIA Procedure as they process personal information in their different Divisions.

- **Condition 2 - Processing Limitation**

  The Organization shall ensure that the processing of any personal Information is done in accordance with the relevant legislation without infringing on the data subjects right to privacy. The Organization shall ensure that personal Information is only processed if the reasons given for the processing are adequate, legitimate, relevant and not excessive. Personal information shall be processed for the purpose it was collected for and not for a different purpose unless in accordance with exceptions in the Act.

- **Condition 3 - Specific Purpose**

  The organization shall only collect personal Information for a specific purpose which is explicitly and limit the processing to the specific purpose it was collected for. The Organization must ensure, in collecting the information, that the data subject is aware of the purpose for which the information is being collected.

- **Condition 4 - Further Processing Limitation**

  The further processing of any personal information must be compatible with the purpose for which it was initially collected for.

- **Condition 5 - Information Quality**

  The Organization shall take reasonable steps to ensure that the personal Information it processes, and stores is complete, accurate, not misleading and kept up to date where necessary.

- **Condition 6 - Openness**

  The Organization must maintain the documentation of all processing operations under its responsibility. The purpose of this condition is to ensure transparency and fairness in the processing of personal information. The Organization shall ensure that the data subject is aware of the reasons for which his/her personal Information is processed. The Organization shall inform data subjects of any breaches relating to the Data Subject personal information.

- **Condition 7 - Security Safeguards**

  The organization shall secure the integrity and confidentiality of personal information in its possession through the implementation of appropriate measures to prevent; the loss, damage and unauthorized destruction of personal Information; and unlawful access which leads to processing of personal Information without the consent of the data subject. IT will guide the organization in terms of what are the appropriate IT security technologies to ensure safeguarding and protection of automated personal information and educate employees on protecting and securing automated processing of personal information. Security Enterprise and Infrastructure Asset Management will guide the organization in terms of appropriate security measures and facilities to ensure safeguarding and protection of non-automated personal information. The Organization shall also ensure that it has written agreements with all Operators processing personal Information on its behalf. These agreements will need to outline the Operators measures to ensure the protection of personal Information in their possession. The Organization shall establish and implement processes or mechanisms to notify a data subject and the Information Regulator where there are reasonable grounds to believe that the personal Information of a data subject has been accessed or acquired by any unauthorized person.

- **Condition 8 - Data Subject Participation**

The Organization shall establish mechanisms and processes to provide data subjects with the opportunity to request, correct, delete or destroy their personal information insofar as requests have been done in the prescribed manner and where possible and justifiable.

4.1.2 Personal Information Life Cycle

- Processing includes any activity concerning personal information. When employees, operators, or the Organization Subsidiaries:

- Collects Personal Information
- Use Personal Information
- Share Personal Information
- Transfer Personal Information
- Store Personal Information; and
- Destroy Personal Information

shall do so in accordance with compliance requirements of POPIA Act, Protection of Personal Information (POPIA) Policy – I010 002P and Protection of Personal Information (POPIA) Procedure - I010 002M.

4.1.3 Additional rights and obligation not grouped under the 8 POPIA conditions:

- Processing of special personal information
- Processing of Children's personal information
- Direct Marketing
- Processing subject to prior authorization
- Profiling of data subjects based on the automated processing of PI
- Transfer of PI to other countries
- Notification to the Regulator
- Assessments
- Information Notices
- Enforcement Notices and Administrative fines.

The organization shall take proper measures and controls to ensure compliance with these obligations. The Protection of Personal Information (POPIA) Procedure - I010 002M will provide guidance in terms of how to implement these additional obligations.

4.1.4 Information Officer

- The Organization shall appoint an Information Officer in terms of section 55 of the Act. The Information Officer after the effective date has been announced may only take up her/his duties in terms of the Act after the Organization has registered him /her with the Information Regulator.

4.1.5 Training and Awareness

- Heads of Divisions shall ensure that all their staff members are trained on how to process personal information in accordance with the Act. The information Officer shall be responsible to provide such training and general awareness. Head of Divisions shall appoint POPIA Champions to assist with implementation of POPIA in the respective divisions.

4.1.6 General Data Protection Regulation

- The Organization must determine, based on its business model, if the Organization activities falls within the ambit of the GDPR. Based on the assessment if the GDPR applies to the Organization, shall identify such activities, its risks and develop and monitor controls to minimize the risks associated with breach of GDPR.

4.2 KEY OUTCOMES OF PRINCIPALS

- Organizational Compliance with the POPIA Act.
- Protection of personal information within the organization.
- Promotion of a privacy culture.
- A cross functional coordinating POPIA Champions
- Enhanced personal information security safeguards.

5. PROCESS FOR MONITORING

- The effective implementation and monitoring of this Protection of Personal Information (POPIA) Policy shall be done through relevant committees. Internal audits shall be conducted accordingly to determine conformance and implementation. This policy shall be reviewed accordingly to reflect the environmental changes or regulation requirement in order to ensure that is relevant and current to the organization.

Note: This policy shall be reviewed in three-years cycle and if there is a need to review the policy before three-years cycle lapses due to any circumstances being legal requirements, changes in the businesses, the need to reflect current practices or activities, the policy shall be unlocked for review accordingly.

6. ACCOUNTABILITIES AND RESPONSIBILITIES

- The overall accountability for development and implementation of this procedure lies with the Chief Executive Officer with the support from Group Executive: Governance & Assurance and Information and Privacy Specialist as the responsible persons for actual development, implementation of this procedure. Internal Auditors have full responsibility to report audit outcomes to audit committee about the affairs of legal department.

7. VERIFICATION

- This policy shall be verified in accordance with Verification Policy Document - Z001 002M.

8. NON-CONFORMANCE REPORTING

- Any deviation from this policy shall be identified and registered with corrective and preventative measures for continual improvement in accordance with internal policies.

9. RELATED LEGISLATION AND STANDARD

- Promotion of Access to Information Act No. 2 of 2000
- Protection of Personal information Act No. 4 of 2013
- Quality Management System ISO 9001