DEPARTMENT OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT

NO. 6216 **23 May 2025**

INFORMATION REGULATOR (SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

JD House, 27 Stiemens Street, Braamfontein,
Johannesburg, 2017, South Africa
P.O Box 31533, Braamfontein, Johannesburg, 2017
Email: enquiries@@inforegulator.org.za
Website: www.inforegulator.org.za
Toll Free: +27 80 001 7160

06 MAY 2025

NOTICE IN TERMS OF SECTION 61(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013 (POPIA) CODE OF CONDUCT: RESIDENTIAL COMMUNITY INDUSTRY (RCI)

1. In terms of the provisions of section 61 (2) of POPIA, the Information Regulator (Regulator) gives notice that the Regulator is in receipt of a proposed code of conduct from the Residential Community Industry (RCI) that deals with how personal information will be processed in the residential community sector.

2. The purpose of the code of conduct is to-

    2.1. promote appropriate practices by members of Residential Communities Council (RCC) and National Association of Managing Agents (NAMA) governing the processing of personal information in terms of POPIA;

    2.2. encourage the establishment of appropriate agreements between members of RCI and third parties, regulating the processing of personal information as required by POPIA and dictated by good business practice; and

    2.3. to establish procedures for members of RCI to be guided in their interpretation of principally POPIA, but also other laws or practices governing the processing of personal information, allowing for complaints against residential communities to be considered and remedial action, where appropriate, to be taken.

3. The code of conduct governs-

    3.1. the processing of personal information (including personal information of data

3.2. where appropriate, agreements that may need to be concluded between members of RCI and third parties promoting, and to the extent possible ensuring that personal information is processed in compliance with POPIA; and

3.3. the enforcement by RCI of the provisions of the code of conduct.

4. Affected persons are invited to submit written comments to the Regulator (email address: POPIACompliance@inforegulator.org.za.) within fourteen (14) days after publication of the notice in the Government Gazette. A copy of the code of conduct will be made available on the Regulator's website, alternatively, a request for a copy of the code may be made by addressing correspondence to email address: POPIACompliance@inforegulator.org.za.

RESIDENTIAL COMMUNITIES INDUSTRY

POPIA CODE OF CONDUCT (DRAFT)

Lawful Processing of Personal Information for the Residential Community Industry

Code of Conduct governing the Conditions for Lawful Processing of Personal Information by members of the Residential Communities Industry

Incorporating:

Residential Communities Council (RCC)

National Association of Managing Agents (NAMA)

Members and Associated Parties of RCC and NAMA

Table of Contents

Code Prepared By:	Date & Version	For Whom
John Cato Email: johnc@iact-africa.com Dr Peter Tobin Email: petert@iact-africa.com	2 April 2025 Version 1.0	Residential Communities Council (RCC) Board of Directors and Members; National Association of Managing Agents (NAMA) Board of Directors and Members

PART A: INTRODUCTION

1. Background

1.1. The Residential Communities Industry (RCI) processes large amounts of personal information and needs to place a strong focus on processing personal information in a lawful manner.

1.2. The need for a standard approach for processing personal information has been recognised by the Residential Communities Council (RCC) and the national Association of managing Agents (NAMA). These associations have entered in a collaboration for establishing a Code of Conduct for the processing personal information by their members and their own organisations in accordance with the Protection of Personal Information Act of 2013 (POPIA).

1.3. The Residential Community Industry (RCI) includes approximately 3,000 Homeowner Associations and 56,000 Sectional Title Schemes in South Africa. Source: Association of Residential Communities (ARC).

1.4. The RCC currently has 188 members and NAMA has 391 members. In combination they constitute significant representation in the Residential Communities Industry (RCI).

2. Background to RCC

2.1. The Residential Communities Council (RCC) is an association acting for Residential Community Council members. Members are residential community schemes, the majority of which are Homeowners Associations.

2.2. The Residential Communities Council (RCC) is a non-profit company (NPC) registered in terms of the Companies Act 71 of 2008.

2.3. The RCC is a registered Public Benefit Organisation in terms of section 30 of the Income Tax Act, 58 of 1962.

2.4. The RCC serves its members by advocating the Residential Community Industry to self-govern itself;

2.5. The objective of the RCC is to formulate, deliberate and express the united voice, and be the representative of the RCI, including aspects with regard to the interaction between the industry and government (whether national, provincial or local), or any other statutory bodies, as well as interaction with any other public or private individual, entity or institution with regards to matters which may be of concern or interest to RCC Members.

3. Background to NAMA

3.1. The Board of Directors and Members (NAMA) is a non-profit company (NPC) registered in terms of the Companies Act 71 of 2008.

3.2. The primary objectives of NAMA are to:

- Promote and advance the interests of Community Scheme Administration and Management in the Republic of South Africa;
- Promote and advance the common interest of persons and entities engaged in the business of Community Scheme Management.

3.3. NAMA is a voluntary, Non-Profit organisation that promotes and advances the interest of Managing Agents and Community Scheme Management in South Africa.

3.4. NAMA's members are grouped into three categories:

- Corporate Members (Managing Agents)
- These are Managing Agents and have been admitted as members due to the fact that they exclusively render services as a Managing Agent and is duly registered with the Property Practitioners Regulatory Authority (PPRA) and have been issued with a valid Fidelity Fund Certificate (FFC).
- Regional Service Providers
- These are Service Providers to the industry [Attorneys, Plumbers, Accounting, etc.].
- National Service Providers
- These are Service Providers who wish to be represented Nationally.

4. Purpose

The purpose of this Code of Conduct is to:

4.1. Promote appropriate practices for the RCC, NAMA, their members and associated parties for complying with the Protection of Personal Information (POPIA).

4.2. Provide practices for developing, implementing, monitoring and maintaining a compliance framework for POPIA by the RCC, NAMA and their members.

4.3. Promote transparency for the relevant bodies on how personal information should be processed and to provide guidance on the effective application of POPIA.

4.4. The enforcement by the RCC and NAMA of the provisions of this Code of Conduct by members.

4.5. The RCC and NAMA shall ensure that their members accept that their membership is subject to compliance with this Code of Conduct.

5. Scope

The scope of this Code of Conduct includes the following:

5.1. The processing of personal information by the RCC and NAMA of its members in accordance with POPIA and PAIA to provide services to them.

5.2. The adherence by members of the RCC and NAMA of the provisions of this Code of Conduct.

5.3. The processing of personal information relating to homeowners, residents, visitors, employees, contractors and other stakeholders by members of the RCC and NAMA for the purposes of administration and delivery of services to them in compliance with the

Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA) as defined in section 6: POPIA Definitions.

5.4. The inclusion of the RCC, NAMA, Homeowners Associations, Managing Agents, Bodies Corporate and Service Providers associated with these parties.

5.5. Provision of transparency to all stakeholders through the practices contained in this Conduct of Conduct.

6. POPIA Definitions (as defined in the Guideline to Develop Codes of Conduct and the Residential Community Industry)

Any term used in these guidelines would bear the same meaning as in POPIA unless the contrary is indicated in this Code of Conduct.

"Annually" means calendar year which runs from the date on which the code was issued;

''Automated means'' for the purposes of these guidelines, means any equipment capable of operating automatically in response to instructions given for the purpose of processing information;

''Body'' means public or private body as defined in POPIA;

"Body Corporate" means a legal entity that manages and regulates a sectional title scheme in terms of the Sectional Title Schemes Management Act (STSMA).

''Code of conduct'' means a code of conduct issued in terms of Chapter 7 of POPIA;

''Constitution'' means the Constitution of the Republic of South Africa, 1996;

"Data subject'' means the natural person or where applicable to a juristic person to whom personal information relates. It means the person to whom personal information relates;

"Executive Committee" means the executive committee is made up of people who are elected by the community scheme's members. The committee is responsible for making decisions about the scheme, such as approving budgets and maintenance projects. The committee must act in the best interests of the owners and adhere to a code of conduct.

"Governing Body" means the body which serves as the focal point and custodian of governance in the organisation. The governing body should ensure that in its composition, it comprises a balance of the skills, experience, diversity, independence and knowledge needed to discharge its role and responsibilities. Source: King IV Report on Corporate Governance for South Africa

''Information matching programme'' means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action regarding an identifiable data subject.

"Managing Agent" means any person who provides scheme management services to a body corporate for reward, whether monetary or otherwise, including any person who is employed to render such services.

"Memorandum of Incorporation (MOI)" means the rules of a scheme which serve as a contract with homeowners and residents in a scheme

"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, including, but not limited to–

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, 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 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.

''Prescribed'' means prescribed by regulation or by a code of conduct.

''Regulator'' means the Information Regulator established in terms of section 39 of POPIA. ;

''Regulations'' means Regulations made in terms of Section 112(2) of POPIA.

''Relevant body/bodies'' refers to any specified body or class of bodies, or any specified industry, profession, or vocation or class of industries, professions, or vocations that in the opinion of the Regulator which has sufficient representation.

''Relevant stakeholders'' means stakeholders, affected stakeholders or a body representing such stakeholders.

''Republic'' means the Republic of South Africa; and

''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.

'Scheme" means living arrangements where there is shared use of and responsibility for land/buildings such as sectional title, homeowners' associations, retirement housing schemes, share block companies and housing cooperatives. Source: Community Schemes Ombud Services (CSOS).

"Trustee" means person or corporation that holds the legal title to money, property, or an estate.

7. Definitions relating to the Residential Community Industry

"Data subject'' means a homeowner, resident, tenant, visitor, employee, director, employee of homeowner or resident, contractor, estate, Homeowners Association, body corporate and managing agent.

"Responsible Party" means the organisation or person which alone or in conjunction with others, determines the purpose and means of processing personal information, In practice, it is the body that determines the purpose and lawful basis of processing personal information in accordance with the conditions for Lawful Processing and ensures that personal information is processed in accordance with the Conditions for Lawfulness processing contained in POPIA Chapter 3. This is normally the scheme's management team or Governing Body. A Responsible Party may also be an organisation which provides services to the Residential Communities Industry but not to a scheme in terms of a contract or mandate with a scheme.

"Operator" means the organisation or person who processes personal information on behalf of the Responsible Party through a contract or mandate. Operators These are service providers who provide services which include the processing of personal information for which the Responsible Party is responsible. These include but are not limited to managing agents, security companies, solution service providers such as community portal services, access control, human resources and payroll, accounting firms, IT services companies and law firms.

8. Governance of the Code of Conduct

8.1. The Code shall be governed by the Residential Communities Council's Board of Directors for its members.

8.2. The Code shall also be governed by the National Association of Managing Agents' Board of Directors for its members.

8.3. The RCC Memorandum of Incorporation and governance committees will ensure the effective governance of the code in terms of the principal business and objects of the RCC

8.4. The RCC Memorandum of Incorporation is provided in Annexure C.

8.5. The NAMA Memorandum of Incorporation is provided in Annexure D.

8.6. A Personal Information Governance Charter and Terms of Reference which includes the monitoring of compliance with the COC will be established in order to ensure the effective governance of this Code of Conduct. Note to RCC and NAMA Boards: It is recommended that Governance Charter and Terms of Reference is established as it is important for the Information Regulator to have a view of how the CoC will be governed and for relevant parties to ensure a common approach, without a charter, governance may be disjointed across the RCC and NAMA.

PART B: CONDITIONS FOR LAWFUL PROCESSING OF PROCESSING PERSONAL INFORMATION

Processing of personal information in general

Introduction to Part B

This Code of Conduct is applicable to the RCC, NAMA and their members within the Republic of South Africa. It does not apply outside South Africa except where Transborder Information Flows apply.

Chapter 7 of POPIA and the Guidelines to Develop Codes of Conduct issued by the Information Regulator state that Codes of Conduct must incorporate the Conditions for the Lawful Processing of Personal Information as set out in Chapter 3 of POPIA or it should set out obligations that provide a functional equivalent to the obligations established in the conditions. Part 2 in this Code of Conduct provides a functional equivalent of the Conditions for the Lawful Processing of Personal Information and is an interpretation for the Residential Community Industry.

Personal Information Processed in Residential Schemes

The definition of personal information contained in POPIA is generic and does not provide contexts for specific industries. A list of necessary and commonly used items of personal information in the Residential Community Industry is provided below:

Homeowner / resident Information

- Name and surname
- Family members' names including children
- Identify numbers of the above
- Stand number and/or physical address details
- Email address
- Telephone/cell number
- Vehicle/s registration
- Your bank account details
- Biometric information including but not limited to fingerprints, hand/palm information, facial information (regarded as Special Personal Information)

Visitor information

- Name and surname
- Identity number
- Drivers licence number and information
- Vehicle registration number.

Employee Information

- Name and surname
- Next of kin names including children
- Identify numbers of the above
- Physical address details
- Email address
- Telephone/cell number
- Your bank account details
- Health information (regarded as Special Personal Information)
- Biometric information including but not limited to fingerprints, hand/palm information, facial information (regarded as Special Personal Information)

Third party information

Supplier information including Operators (they are juristic persons)

- Company information
- Director and management details:
- Name and surname
- Identity number
- Drivers licence number and information
- Vehicle registration number.

Contractor information

- Company information
- Director and management details:
- Name and surname
- Identity number
- Drivers licence number and information
- Vehicle registration number
- Biometric information including but not limited to fingerprints, hand/palm information, facial information (regarded as Special Personal Information)

It is important to note that POPIA does not provide guidance on high-risk information. Responsible parties are required to identify all reasonably foreseeable risks to personal information and to manage them. In terms of the RCI, it is important to identify and manage high-risk information as a higher priority than lower risk information.

In the absence of guidance in POPIA, the following items of personal information are regarded as high-risk items:

- Special Personal Information defined in section 26, in particular:
- Medical information of data subjects e.g. employees and contractors
- Biometric information of all data subjects whose biometric information processed
- Bank account details of homeowners, residents and employees

1. Condition 1: Accountability

1.1. Responsible Party to ensure conditions for lawful processing.

The Responsible Party shall ensure that the conditions for lawful processing and additional sections provided in Part B of this code are compiled and given effect at the time of the determination of the purpose and during the processing of personal information.

The Responsible Party shall be the following:

- The scheme shall be the Responsible Party in majority of cases.
- Organisations which process personal information for the Residential Community Industry rather than a specific scheme shall also be Responsible Parties. These include but are not limited to the RCC, NAMA and service providers which provide services directly to data subjects in the Residential Community Industry.

This code has been provided primarily for schemes as these entities process most of the personal information in the Residential Community Industry and who conduct a range of personal information processing activities.

Part C in this code provides information regarding the appointment of an Information Officer in the different types of schemes. The Information Officer is responsible for establishing and maintain compliance in accordance with Part B in this code. Boards of Directors and Trustees are accountable for ensuring that compliance with this code is implemented and maintained.

The Responsible Party shall ensure that the conditions for lawful processing and additional sections provided in Part B of this code are complied with and given effect at the time of the determination of the purpose and during the processing of personal information.

2. Condition 2: Processing Limitation

Condition 2 includes the following:

- Lawfulness of processing
- Minimality
- Consent, justification, and objection
- Criteria for processing personal information

These are described within the context of the residential community industry below.

2.1. Lawfulness of Processing

2.1.1. Personal information will be processed lawfully and in a reasonable manner that does not infringe the right of privacy of data subjects.

2.1.2. In practice, this means that personal information should not be processed in a manner in which the data subject would feel that their privacy has been infringed. As an example, it should not be obtained without the data subject's knowledge or from a source with which they would not be in agreement. It should also not be used for a different purpose other than

the purpose for which it was obtained. These are described further in section 2.3. in the Code of Conduct.

2.2. Minimality

2.2.1 Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant, and not excessive.

2.2.2 In practice, personal information collected from a data subject should only be sufficient to satisfy the intended purpose and should not be excessive for that purpose. An example of this is that schemes should only collect and process personal information for the purpose of administering their affairs pertaining to the scheme and only the items of information for this purpose should be collected. A list of necessary and commonly used items of personal information is provided in the Introduction to Part B in this code. No other personal information shall be processed.

IRSA says that the code should include a PIA in terms of an assessment of minimality. POPIA does not say this. The only reference to a PIA is in the POPIA Regulations 4 (1) (b):

> A personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

Consent, justification and objection

Consent, justification, and objection are defined in sections 11 and 12 in POPIA. They are described within the context of residential community schemes as follows:

2.3.1. Criteria for Processing Personal Information

Processing Limitation in POPIA includes six criteria for obtaining personal information directly from the data subject (people or legal entities). In principle there are four criteria which apply in schemes for 'standard' personal information; they are listed below:

1. Personal information may be obtained in order to perform a contract (section 11.1 (b));
2. Personal information may be processed if it is in the legitimate interest of the data subject (section 11.1 (d));
3. Personal information may be processed if it is in the legitimate interest of the SCHEME (section 11.1 (f));
4. Personal information may be processed if consent for processing is obtained (from the data subject for a competent person (parent or legal guardian) if the data subject is a child (section 11.1 (a).

2.3.2. Categories of Personal Information

Before considering the criteria listed above, it is important to consider the categories of personal information. There are 3 categories as shown below:

- Standard Personal Information: Items such as name, address, phone number, physical address, email address, any identifying number, etc.;
- Special Personal Information: items such as race, health information, biometric information, etc.
- Personal Information of Children: Personal information of persons under the age of 18.

These are outlined further below:

2.3.2.1. 'Standard' Personal Information consists of:

first name, surname, email address, office phone, cell phone, fax number, postal address, ID Number, Skype ID, LinkedIn Id, Twitter ID, Facebook Id, physical address, GPS location of address, billing address shipment address, user name, user id, account name, account number, sex (Male/Female), marital status, nationality, age, language, birth, education, financial history, employment history, personal opinions, view or preferences, private, correspondence sent by the person, views or opinions of another person, name with other personal information, name leads to other information.

Cognisance must also be taken of the items of the commonly used personal information in the Residential Community Industry as described I the introduction in Part B in this code.

2.3.2.2 Special Personal Information consists of:

Race, pregnancy status, ethnic origin, colour, sexual orientation, physical health, mental health, well-being, disability, religion, conscience, belief, culture, medical history, criminal history, biometric information.

2.3.2.2. Personal Information of Children consists of:

- Personal information of persons under the age of 18 years.

2.3.3 Consent

Consent is defined in POPIA as:

- ''consent'' means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
- Consent must be freely given and should be based on a clear and unambiguous purpose.

Consent must be contained from data subject for Special Personal Information unless it is required by a law.

Consent must also be obtained where it is necessary to process the personal information of a child or children under the age of 18. POPIA requires the consent of a competent person to be obtained unless it is required by a law. In practice, this is the legally authorised person such as a parent or legal guardian.

2.3.3.1. Records of Consent

Records of consent shall be kept as proof for the data subject's or competent person's consent as referred to in POPIA 11 (2) (a).

2.3.3.2. Withdrawal of Consent

The data subject or competent person may withdraw his or her consent at any time provided that the lawfulness of the processing of personal information before such withdrawal of the processing of personal information will not be affected prior to the withdrawal. In reality, this will normally only apply to visitors in an estate as the criteria or legal basis for other data subject groups does not normally require consent.

2.3.3.3. Objection

The data subject may object, at any time, object to the processing of personal information on reasonable grounds relating to their particular situation unless the processing is required by law. If a

data subject has objected to the processing of personal information, the responsible party may no longer process the personal information of the data subject.

2.4. Applying Criteria to Groups of Data Subjects in Estates

As part of the scheme's POPIA compliance programme, the scheme shall assess the groups of data subjects below in conjunction with the criteria for processing personal information as they apply to these groups of data subjects:

2.4.1. Homeowners. The constitution, conduct rules, etc. are in fact a contract between the scheme and the homeowner. Section 11.1 (b) therefore applies and represents legal grounds for processing the standard personal information of the homeowner. It overrides the need for obtaining consent or for justifying that it is in the legitimate interest of the scheme or homeowner. The following points should be considered.

2.4.1.1. If the scheme uses biometric information for identity and access management, then it is necessary to obtain consent for processing biometric information and to retain records of consent.

2.4.1.2. New homeowners normally sign documents such as sale agreements when they purchase a property. These documents usually refer to the MOI, constitution rules, etc. A contract is, therefore, established at this point. A reference to the processing of personal information in accordance with POPIA and the scheme's Privacy Policy should be included into the document which the residents sign and accept as the rules for living in the scheme.

2.4.2. Residents. Residents such as family members are also required to abide by the scheme's rules but they do not normally sign the MOI, constitution rules, etc. Consent should therefore be obtained from them. If the estate uses biometric information for identity and access control, consent should be obtained for the processing thereof.

2.4.3. Tenants. Tenants normally sign a lease agreement with the homeowner rather than the estate. They also sign their acceptance of the constitution and rules which means that they are entering into a contract with the scheme. Consent for processing is, therefore, not required unless biometric information is processed for identify and access control in which case it must be obtained.

2.4.4. Visitors. Since there is no contract between the estate and the visitor, one of the other legal grounds should be applied. These are:

2.4.4.1. Obtain consent. Obtaining consent from visitors varies depending on how access is controlled. If a manual system is used such as a form or register which the visitor signs, the form or register can be changed to include consent. If a Visitor Management System is in use, a Privacy Notice/Policy should be made available via a link in the Visitor Management System so that visitors are able to read it prior to visiting the estate through the message they receive. The scheme should also amend their signage at the gate to highlight the fact that personal information is being processed in accordance with the estate's Privacy Notice and POPIA.

As already mentioned, if biometric information is being processed, consent for this shall be obtained from the visitor.

It should be made clear that withholding consent has the consequence of the right of refusal of access for visitors.

In many schemes, a condition for entering the premises is the scanning for driver's licences and licence discs for safety and security purposes. While this is not a legal requirement in terms of a specific law, schemes should include this practice as being in the legitimate interest of the schemes based on section 11.1(f) in POPIA and Section 2 above.

2.4.4.2. Legitimate interest of the Estate/Scheme (Responsible Party). In schemes where it is impractical to obtain consent, the scheme can process personal information based on the processing being in the legitimate interest of the scheme. If this basis for processing personal information is to be used, it must be clearly stated in the Privacy Notice/Policy.

2.4.4.3. Contractors. Contractors normally have an agreement with homeowners rather than the scheme which means that they should be regarded as visitors to the estate. Contractors often bring employees to the estate. They need to be registered as visitors as well. In some estates, contractors send details of their employees to the SCHEME for security registration. In such cases, the contractor managers should obtain consent from their employees for sharing their personal information with the Scheme.

2.4.4.4. Homeowners' and Tenants' Employees. Homeowners and tenants generally employ domestic and gardening staff. In most schemes, such employees are registered either by the homeowner or their employer with the scheme. Where homeowners and tenants register their employees, they should obtain consent for sharing the personal information with the scheme. Where domestic and gardening employees submit their own personal information to the scheme, consent should be obtained. This is typically done using a registration form.

2.4.4.5. Scheme Employees. The personal information of scheme employees is required by both the scheme from an employee records perspective and in order to comply with the Basic Conditions of Employment Act. In view of this, 2 of the criteria for processing are being met with the need to obtain consent. It is, however, recommended that SCHEME's obtain consent for their personal information be shared with organisations such as medical aid and provident schemes if such sharing is conducted. Consent for processing biometric information should also be obtained if it is being processed.

2.5. Collection directly from data subject

Section 12 (1) states that personal information must be collected directly from the data subject, except as otherwise provided for in subsection (2).

Examples of collection of Personal Information in Residential Schemes

Collection directly from the data subject

- Registration of a homeowner or resident
- Registration of a visitor
- Registration of a contractor
- Registration of a supplier
- Registration of a new employee

Collection from another party

- Collection from an attorney for the transfer of property
- Collection from an estate agent regarding the rental of property to a tenant
- Collection from a homeowner regarding the rental of property to a tenant
- Collection from an Operator such as a security service provider for a visitor
- Collection of a public record or from a source where the data subject has deliberately made their personal information available.
- Collection of a child's personal information where a competent person such as the parent or legal guardian has provided consent for it to be processed

The content from Section 12 (1) Subsection 2 relating to the collection of personal described above is provided below for clarity.

Subsection (2) states that is not necessary to comply with subsection (1) if —

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

2.5.2. 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;

2.5.3. collection of the information from another source would not prejudice a legitimate interest of the data subject;

2.5.4. collection of the information from another source is necessary —
(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act;
(iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
(iv) in the interests of national security; or
(v) to maintain the legitimate interests of the Responsible Party or of a third party to whom the information is supplied;
(e) compliance would prejudice a lawful purpose of the collection or;
(f) compliance is not reasonably practicable in the circumstances of the particular case.

Responsible parties shall process personal information in accordance with sections 2.1 to 2.5 in this code.

3. Condition 3: Purpose Specification

Condition 3 includes the following:

- Collection for specific purpose
- Retention and Restriction of Records

3.1. Collection for specific purpose

POPIA requires that personal information shall be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Responsible Party, It shall not be used for any other purpose by the scheme.

Examples of Purposes for Processing Personal Information in Residential Schemes

Examples of Purposes for Processing Personal Information in Residential Schemes are provided below:

- For managing the affairs of residents relating to their residency in the scheme including but not limited the processing of levy payments
- For providing services to residents
- For managing the safety and security of residents residing in a scheme
- For managing the safety and security of visitors and other non-residents such as contractors to the scheme

The scheme shall ensure that the data subject is aware of the purpose of the collection of their personal information. This can be done in a Privacy Policy or Notice and the scheme's constitution or rules.

The content from Section 13 (1) 2 relating to the purposes for processing personal information described above is provide below for clarity.

3.1.1. POPIA requires that personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Responsible Party.
3.1.2. POPIA also requires that steps must be taken in accordance with section 18 (1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of section 18 (4) are applicable.
3.1.3. In schemes, the purposes for the various data subject groups are clear but they need to be stated when personal information is collected. In other words, the criteria for processing personal information lawfully as described in section 2 in this document must be based on a specific, clear and relevant purpose.

3.2 Retention and Restriction of Records

Section 14 on POPIA states that personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

3.2.1. the retention of the record is required or authorised by law i.e. another law;
3.2.2. the Responsible Party reasonably requires the record for lawful purposes related to its functions or activities;
3.2.3. retention of the record is required by a contract between the parties thereto; or
3.2.4. the data subject or a competent person where the data subject is a child has consented to the retention of the record.

Schemes shall, therefore, only retain personal information records for as long as they required to comply with 3.2.1, 3.2.2, 3.2.3., and 3.2.4. above. Schemes shall destroy personal information records in accordance the retention periods provided in table 1. The destruction shall be conduct in a secure manner and in a manner which prevents personal information from being constructed.

Table 1 below provides an example of the common personal information categories processed in the Residential Community Industry.

Table 1: Scheme Records Retention Management Schedule

Table 1 below provides a list of common personal information types as well as recommended retention periods and where appropriate, the law which requires retention period shown.

Table 1: Scheme Records Retention Management Schedule

Record Type	**Retention Period (Years)**
Financial Records	7 (required by Companies Act)
Employee Records	EXP + 5 (required by Basic Conditions of Employment Act)
Company Records	7 (required by Companies Act)
Homeowners, Resident Records	USE + 6 (required by the Sectional Titles Schemes Management Act - STSMA). This is used as a guide in the absence of any other law relating to the Residential Community Industry.
Visitor Records	USE +30 days is recommended. There is no law which defines the retention period requirements for visitors
Security and CCTV Event Information	USE + 30 days. CCTV footage for security events should be extracted into a separate storage in case they become incidents and are required for criminal investigation purposes. These should be retained until the investigation or legal proceeding has been completed.
Contracts/agreements	EXP + 7 (required by Companies Act)
Information Technology Records (Backups, Logs, etc.)	To be defined in terms of practical requirements and backup schedules
Compliance records (including Consent records)	EXP + 2
Communication Records (Newsletters and Publications)	USE + 6 (required by the Sectional Schemes Management Act)

Abbreviation of Legend:

USE: As long as information is used + 1

EXP: Expiration or termination date, including the expiration date of a contract, patent, permit or warranty; the expiration of a confidentiality obligation; the date on which a lawsuit or dispute is concluded by a final court judgement or settlement; the date of an asset disposition; the date when a document is superseded; the termination of active employment; the abandonment of a trademark; Confirmation Date by Master of final trustee's account.

Responsible parties shall process personal information in accordance with sections 3.1 and 3.2. in this code. They shall also provide instructions to Operators for managing the retention of records.

3.3. Restriction of Records

The Responsible Party shall restrict the processing of personal information if:

3.3.1. Its accuracy is contested by the data subject.
3.3.2. The responsible party no longer needs the personal information for its intended purpose but needs to be maintained for purposes of proof or evidence.
3.3.3. The processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead.

Processing may be resumed once matters described in 3.3.1 and 3.3.2 have been resolved. The responsible party shall, however, inform the data subject before lifting the restriction on processing.

Responsible parties shall restrict the processing personal information in accordance with sections 3.3.1, 3.3.2 and 3.3.3. above and shall inform the data subject before lifting the restriction on processing.

4. Condition 4: Further Processing Limitation

Further processing to be compatible with purpose of collection.

4.1. Condition 4 allows the Responsible Party to extend the purpose for which personal information is being processed provided it is in accordance with or compatible with the purpose for which it was obtained.
4.2. An example of further processing is the processing of resident information with a security services company. Many estates appoint security companies to provide security services and in order to do so, the personal information needs to be
4.3. shared with the security company (regarded as an Operator).

Responsible Parties shall ensure that any further processing of personal information is compatible with the intended purpose as described in 4 above. Where personal information is shared with an Operator, a written contracts between the Responsible Party and Operator shall be established to ensure that adequate security safeguards are in place. Section 5.7 provides additional information about contracts.

5. Condition 5: Information Quality

Quality of information

5.1. Condition 5 requires the Responsible Party to take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

5,2. The reason for this requirement is to prevent the Responsible Party from making incorrect decisions which may negatively affect data subjects.

5.3. Practical steps for ensuring that personal information is accurate and not misleading are to implement processes for inviting data subjects (homeowners, residents, employees, etc.) to check the accuracy of their personal information periodically.

Responsibilities Parties shall implement processes for ensuring that personal information is complete, accurate and not misleading as described in 5.3 above.

Condition 6: Openness

Condition 6 requires the Responsible Party (normally Schemes) to notify data subjects when personal information is collected and to publish a document describing the processing operations for personal information under its control by developing and publishing a PAIA Manual.

Schemes shall therefore:

6.1. Notify data subjects when personal information is collected and inform them of the purpose for which it was collected. If it was not collected directly from the data subject, the fata subject should be notified of the source, purpose and whether the supply was voluntary or mandatory.

6.2. Develop and publish a Promotion of Access to Information Act (PAIA) Manual in which the processing operations for personal information. It should be published o the scheme's website and in paper format in the scheme's office.

6.3. In the Residential Community Industry, schemes shall implement the following measures:

6.3.1. A PAIA Manual which includes all processing operations i.e., a list of personal information record categories should be developed and published;

6.3.2. The scheme should inform new homeowners, residents, employees, visitors and contractors that their personal information has been obtained and the purpose thereof. It is common practice for the personal information of new homeowners to be obtained from transferring attorneys. Schemes should inform new homeowners of the receipt of their information.

6.3.3. A Privacy Policy or Notice should be developed in order to inform data subjects about the personal information they collect. The policy should include the following:

- Details of personal information being processed. In schemes the commonly processed items are:
    - Name and surname
    - Names and surnames of family members including children
    - Stand number and/or physical address details
    - Email address
    - Telephone/cell number

- Vehicle/s identification
- Bank details
- Biometric information (where such technology is used)

- The purpose/s for which personal information is being processed. In estates the common processing purposes are:
  - To confirm and verify a person's identity or to verify that you are a homeowner, resident, worker, contractor or visitor for security purposes.
  - To carry out obligations arising from any contracts entered into between the scheme and data subjects.
  - To notify data subjects about changes to our services.
  - For the detection and prevention of fraud, crime, or other malpractice.
  - To conduct members satisfaction research or for statistical analysis.
  - For audit and record keeping purposes.
  - In connection with legal proceedings.
  - We will also use Personal Information to comply with legal and regulatory requirements or industry codes to which we subscribe, or which apply to us, or when it is otherwise allowed by law.
  - Parties to whom personal may information be disclosed.
  - In estates the common recipients of personal information are:
  - Service providers who are involved in the delivery of products or services to you. Agreements must be established with them to ensure that they comply with the duties of an Operator;
  - Where the scheme has a duty or a right to disclose personal information in terms of law or industry codes;
  - Where the scheme believes it is necessary to protect their rights.
  - A summary of how personal information is secured. Common security practice areas in estates are:
    - Physical security;
    - Computer and network security;
    - Access to personal information;
    - Secure communications
    - Security in contracting out activities or functions;
  - Retention and disposal of personal information; acceptable usage of personal information;
  - Governance and regulatory issues;

- Investigating and reacting to security and estate management incidents.

Responsible Parties shall implement processes and documents described in 6.1, 6.2. and 6.3 above to ensure that appropriate measures for openness are established.

7. Condition 7: Security Safeguards

The subject of information security is broad and complex in its own right. Condition 7 in POPIA makes the protection of personal information a legal obligation for all parties. Security Safeguard requirements for securing personal information are contained in Condition 7 Section 19, 20 and 21 and are described below.

It is important to consider that personal information includes but is not limited to paper, electronic, verbal, multi-media such as security camera footage information.

In order to address the requirements contained in sections 19, 20 and 21, schemes, as the Responsible Party, shall establish and maintain the following practices:

Responsible Parties

7.1. The confidentiality and integrity of personal information should be protected by implementing and maintaining appropriate, reasonable technical and organisational measures to prevent the loss, damage or unauthorised destruction of personal information as well as to prevent the unlawful access to or processing of personal information. Annexure A provides guidance for appropriate, reasonable technical and organisational measures.

7.2. All reasonably foreseeable risks to personal information shall be identified and appropriate measures should be established to ensure that identified risks are reduced and managed. Identified risks and measures should be taken into account when implementing the measures referred to in 7.1 above. Annexure B provides guidelines for assessing and managing risks to personal information.

7.3. Measures implemented must be verified to ensure their effectiveness and must be continuously updated to address new risks and any deficiencies in the measures implemented.

7.4. Consider industry practices for information security such as standards or frameworks and align with security measures with one of these. Commonly used standards and frameworks are ISO 27001, NIST Cybersecurity Framework and the UK ICO Cybersecurity Scheme.

7.5. Written contracts with Operators must be established which include commitments and clauses for the protection of personal information which Operators process on behalf of the Responsible Paty (Scheme).

7.6. Notify the Information Regulator and affected data subjects (if they can be identified) of security compromises or suspected compromises (also referred to as security breaches) using the Guidelines-on-completing-a-Security-Compromise-Notification-ito-Section-22-POPIA and associated FORM-SCN1-Security-Compromises-Notification-Fillable-Formpdf provided by the Information Regulator at https://inforegulator.org.za/

Responsible Parties shall implement practices for ensuring that the confidentiality and integrity of personal information is secured by implementing measures as described in 7.1, 7.2., 7.3., 7.4, 7.5 and 7.6 above.

Operators

Operators such as managing agents, security companies, IT service and solution providers, accounting firms and law firms who provide services which include the processing of personal information to schemes to schemes shall:

7.7. Process personal information only with the knowledge or authorisation of the responsible party.

7.8. Treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

7.9. Comply with the clauses contained in the contract with the Responsible Party (Scheme) relating to the protection and processing of personal information as well as the requirements for security safeguards described 7.1 to 7.4 (these are contained in section 19 in POPIA).

7.10. Notify the responsible party immediately where there are reasonable grounds to believe that a compromise (or breach) or suspected compromise has occurred.

7.11. Permit the Responsible Party to audit the Operator in terms of their compliance with Sections 19 to 21 (Security Safeguards) of the Act

7.12. Comply with requests by the Responsible Party which relate to requests for access to the relevant personal information following the receipt of a valid and approved data subject request.

7.13. The Operator shall not sub-contract any of the processing of the data supplied by the Responsible Party without first ensuring the sub-contractor (sub-operator) will be compliant with the requirements of Sections 19 to 21 of the Act

Operators shall implement practices for ensuring that the confidentiality and integrity of personal information is secured by implementing measures as described in 7.7, 7.8., 7.9, 7.10, 7.11, 7.12, and 7.13.

7.14. Personal Information Risk Assessment and Management

The following steps shall be followed by Responsible Parties to identify and mage risks to personal information:

7.14.1. A personal information risk assessment shall be conducted.

There are several risk management standards and methodologies which can be used, including ISO 22301 and ISO 27005, the international standards which describe how to conduct an information security risk assessment

The standards referred to above may too complex for small schemes, in which case the approach below and table 2 in Annexure B provides an example of a practical approach to personal information risk assessment and management. Key aspects of the approach included in the example are:

- Risk name: Name of the risk
- Risk description: A description of the risk
- Probability of risk occurring: High, Medium or Low probability
- Impact if risk does occur: High, Medium or Low impact
- Overall risk assessment: High, Medium or Low risk based on a balance of the points above
- Possible risk treatment action: Action for treating and managing the risk
- Risk owner and Review date: The name of the person responsible for managing the risk and the next review date of the status of the risk.

Responsible Parties shall assess and manage all reasonably foreseeable risks to personal information as described in 7.15.1 and Annexure B (or similar) in this code.

8. Condition 8: Data Subject Participation

Condition 8 gives effect to data subjects' rights regarding the privacy of their personal information.

In order to provide data subjects with a view of information processed but the Responsible Party and to enable them to exercise their right of access to personal information, the Responsible Part shall publish a PAIA Manual with the request form called REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION published by the Information Regulator. This is also covered in Condition 6: Openness in this code.

The PAIA Manual should contain the following:

- Information required under section 51(1) (a) of the act
- Description of guide referred to in section
- Records available in terms of other legislation
- Records automatically available
- Subjects and categories of records held by [organisation name]
- Purpose of processing of personal information
- Data subject categories and their personal information
- Planned recipients of personal information
- Planned trans-border flows of personal information
- Security measures to protect personal information
- Detail on how to make a request for access
- Availability of the manual
- Availability of the manual
- Fees in respect of private bodies

A PAIA Manual template is available from the Information Regulator at https://inforegulator.org.za/wp-content/uploads/2020/07/PAIA-Manual-Template-Private-Body.pdf

Condition 8 includes the following:

8.1. Access to personal information

8.1.1. A data subject, having provided adequate proof of identity, has the right to:

8.1.1.2. Raise a request to ascertain whether or not the Responsible Party holds personal information about them.

8.1.1.3. Raise a request with a Responsible Party for the personal information record or a description of the personal information about the data subject held by the Responsible Party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information. The request should be raised using the form InfoRegSA-PAIA-Form02-Reg7 available at https://inforegulator.org.za/paia-forms/ or a substantially similar form made available by the Responsible Party. The request shall be responded to by the Responsible Party:

i) within a reasonable time;
ii) at a prescribed fee, if any;
iii) in a reasonable manner and format; and
iv) in a form that is generally understandable

8.1.2. A data subject has the right to request the correction of any incorrect personal information held by the Responsible Party.

8.1.3. If a data subject is required by a Responsible Party to pay a fee for services provided to the data subject, the Responsible Party shall:

i) Give the applicant a written estimate of the fee before providing the services;
ii) Request the applicant to pay a deposit for all or part of the fee.

8.1.4. The Responsible Party may or must refuse, as the case may be, to disclose any information requested in terms of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act (PAIA). Grounds for refusal are:

63. Mandatory protection of privacy of third party who is natural person

64. Mandatory protection of commercial information of third party

65. Mandatory protection of certain confidential information of third party

66. Mandatory protection of safety of individuals, and protection of property

67. Mandatory protection of records privileged from production in legal proceedings

68. Commercial information of private body

69. Mandatory protection of research information of third party, and protection of research information of private body

70. Mandatory disclosure in public interest

8.2. Correction of personal information

8.2.1. A data subject has the right to request a Responsible Party to:

(i) Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(ii) Destroy or delete a record of personal information about the data subject that the Responsible Party is no longer authorised to retain in terms of section 14.

8.2.2. On receipt of a request in terms of subsection (1) a Responsible Party must, as soon as reasonably practicable:

(i) Correct the information;

(ii) Destroy or delete the information;

(iii) Provide the data subject, to his or her satisfaction, with credible evidence in support of the information;

Form 2: Request for Correction or Deletion of Personal Information or Destroying or Deletion of Record of Personal Information available at https://inforegulator.org.za/popia-forms/ or a substantially similar form made available by the Responsible Party should be used to raise a request.

8.3. Manner of access

8.3.1. The provisions of sections 18 and 53 of the Promotion of Access to Information Act apply to requests made in terms of section 23 of this Act.

8.3.2. In practical terms this means that information relating to a request can be provided to the data subject in the following manner:

8.3.2.1. Printed copy of record (including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form);

1) Postal services to postal address;
2) Postal services to street address;
3) Courier service to street address;
4) Facsimile of information in written or printed format (including transcriptions);
5) E-mail of information (including soundtracks if possible);
6) Cloud share/file transfer;
7) Preferred language (Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available).

Responsible Parties shall implement measures for making their PAIA Manual available with the request forms published by the Information Regulator and will implement processes for handling requests for the deletion and correction of personal information. Request forms can be downloaded from https://inforegulator.org.za/popia/ . Responsible Parties shall also publish the PAIA Guide in at least 2 official languages. These alare also available on the Information Regulator's website.

ADDITIONAL SECTIONS CONTAINED IN POPIA CHAPTER 3

In addition to the 8 Conditions for Lawful Processing, these additional sections must also be given due consideration in order to establish appropriate measure for compliance.

The additional sections described in this section are:

- Processing of special personal information;
- Processing of personal information of children;
- Prior authorisation;
- Rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making.

In principle, the processing of the personal information listed above is prohibited unless appropriate measures are implemented and carried out. Processing of special personal information

9.1. Prohibition on processing of special personal information

Section 26 in POPIA states that the processing of special personal information is prohibited unless the following criteria are met:

9.1.1. Consent is obtained from the data subject or where the data subject is a child (under 18 years of age), consent must be obtained from a competent person. In practice, this is the legally authorised person such as a parent or legal guardian. In situations where the legal authorised person is not available, an adult who has a genuine concern for the wellbeing of the child may provide consent.

9.1.2. If the criminal behaviour of a data subject is required to the extent that such information relates to—

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

9.2. General authorisation concerning special personal information.

The prohibition of processing of special personal information as stated in Section 26 does not apply in the following situations:

9.2.1. Where consent has been given by the data subject or a competent person where the data subject is a child;

9.2.2. Where the special personal information is required in order to meet the requirements of another law. An example of this would be processing the information concerning the race of an employee in order to comply with the Basic Conditions of Employment Act 75 of 1997 and the Employment Equity Act 55 of 1998.

9.2.3. Where processing is necessary to comply with an obligation of international public law. An example of this would be the obligation for the estate to comply with the EU General Data Protection Regulation where an EU resident owns property in in South Africa;

9.2.4. Where processing is necessary for historical, statistical or research purposes to the extent that—

9.2.5. Where the purpose serves a public interest, and the processing is necessary for the purpose concerned; or

9.2.6. Where it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent. *An* example of this in the Residential Community Industry is the processing of biometric information. While section 26 requires consent for processing biometric information, it may not always be possible to obtain consent. The implementation of appropriate measures such as a Privacy Policy and amendments to the estate's Governing documents (MOI / Constitution), Conduct Rules (or equivalent) and signage will constitute a suitable alternative for consent.

Sections 28 to 33 cover the following items regarding the processing of special personal information:

- Section 28: Authorisation concerning data subject's religious or philosophical beliefs
- Section 29: Authorisation concerning data subject's race or ethnic origin
- Section 30: Authorisation concerning data subject's trade union membership
- Section 31: Authorisation concerning data subject's political persuasion
- Section 32: Authorisation concerning data subject's health or sex life
- Section 33: Authorisation concerning data subject's criminal behaviour or biometric information

In principle each of these sections make provision for organisations which are based on these subject areas to process personal information without having to comply with section 26 i.e. obtaining consent. The exception is section 33 i.e. criminal behaviour or biometric information which requires consent unless it is required in order to comply with a local or international law or for a legal proceeding.

Responsible Parties shall obtain written consent for processing special personal information of data subjects unless it is required by a South African law or an international public law as described in 9.2.1, 9.2.3 and 9.2.4. Where it is not possible to obtain consent, schemes shall provide sufficient guarantees that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

10. Processing of personal information of children

Prohibition on processing personal information of children

Section 35 in POPIA states that the processing of the personal information of a child is prohibited unless the following criteria are met:

10.1. Prior consent has been obtained from a competent person (parent or legal guardian);
10.2. It is necessary for the establishment, exercise or defence of a right or obligation in law;
10.3. It is necessary to comply with an obligation of international public law;
10.4. For historical, statistical or research purposes to the extent that—

(i) the purpose serves a public interest, and the processing is necessary for the purpose concerned; or

(ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or

10.5. If personal information which has deliberately been made public by the child with the consent of a competent person.

10.5.1. The Regulator may, notwithstanding the prohibition referred to in section 34, but subject to subsection (3), upon application by a Responsible Party and by notice in the Gazette, authorise a Responsible Party to process the personal information of children if it is in the public interest and if appropriate safeguards are in place.

10.5.2. The Regulator may impose reasonable conditions in respect of any authorisation granted under section 35 (2), including conditions with regard to how a Responsible Party must— upon request of a competent person provide a reasonable means for that person to—

(i) review the personal information processed; and

(ii) refuse to permit its further processing;

(b) provide notice—

(i) regarding the nature of the personal information of children that is processed;

(ii) how such information is processed; and

(iii) regarding any further processing practices;

- refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and
- establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

Responsible Parties shall obtain written consent for processing the personal information of children from a competent person as described in 10.1. unless it is required by a South African law or an international public law as described in 10.2. and 10.3. Where it is not possible to obtain consent, schemes shall provide sufficient guarantees that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

11. Prior authorisation

Please note that Section 57 and 58 are provided for information purposes only. They will not be applicable once the Code of Conduct has been approved by the Information Regulator.

The RCC and NAMA will, however, submit a Request for Prior Authorisation of subject to discussion regarding the processing of personal information described in a) to e) below.

Section 57: Processing subject to prior authorisation

Section 57(1) of POPIA requires the Responsible Party to obtain prior authorisation from the Information Regulator under certain situations. These are:

a) If the Responsible Party intends using unique identifiers for purposes other than the purpose at the time of the collection.
b) If the Responsible Party plans to link the information together with information processed by other responsible parties.

c) If the scheme plans to process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;
d) If the estate plans to process information for the purposes of credit reporting
e) If the Responsible Party plans to transfer special personal information, as referred to in section 26, or the personal information of children as referred to in section 34, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information
f) The Regulator may apply the provision of subsection 1 above to other types of information processing by law or regulation if such processing carries a particular risk for the legitimate interests of the data subject;
g) The provisions of section 57 and section 58 are not applicable if a code of conduct has been issued and has come into force in terms of Chapter 7 in a specific sector or sectors of society
h) The Responsible Party is only required to obtain prior authorisation as referred to in subsection (1) only once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised in accordance with the provisions of subsection (1.)

11.1. Section 58: Responsible Party to notify Regulator if processing is subject to prior authorisation

Section 58 subsection 1 requires the Responsible Party to notify the Information Regulator of any processing set out in Section 57 above.

Section 58 subsection 2 places an obligation on the Responsible Party to suspend processing of such information until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

Section 58 subsection 3 states the Information Regulator must inform the Responsible Party in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation.

Section 58 subsections 4 to 6 contain the Information Regulator's obligations regarding more detailed assessments and providing a statement on the lawfulness of the processing within 13 weeks.

Section 58 subsection 7 states that where a Responsible Party has suspended processing of the personal information being assessed and has not received a response from the Information Regulator within 13 weeks, they may presume a decision in its favour and continue with its processing.

11.2. Section 59: Failure to notify processing subject to prior authorisation.

Section 59 states that if section 58 is contravened, the Responsible Party is guilty of an offence and liable to a penalty.

The RCC and NAMA shall ensure that processing requiring prior authorization will not be conducted.

12. Rights of Data Subjects regarding Direct Marketing.

POPIA includes rights for protection data subjects against unsolicited electronic communications i.e. being spammed.

Direct marketing by means of unsolicited electronic communications.

Chapter 8 gives data subjects rights in terms of unsolicited direct marketing by electronic means such as sms, email, automated voice messages, social media and other electronic means. This effectively gives data subjects rights to their privacy in terms of spamming practices.

Note: It is uncommon for schemes to conduct direct marketing practices although service providers and Operators may do so. They may place advertisements in various online publications but since these are not aimed at individuals, it would not be regarded as being direct marketing.

The legal basis for conducting electronic direct marketing is the establishment of measures relating to Condition 2: Processing Limitation and Condition 3: Purpose Specification. In practice this is prohibited unless:

- The Responsible Party (direct marketing organisation) obtains consent from the data subject for the purpose of direct marketing.
- The data subject is a customer of the Responsible Party

In addition to the above:

- The Responsible Party may only approach a data subject for consent once.
- The Responsible Party may not approach a data subject who has previously withheld or declined to give their consent.
- Consent should be requested using the prescribed form: Form 4: Application for the Consent of a Data Subject for the Processing of Personal Information for the Purpose of Direct Marketing available at https://inforegulator.org.za/popia-forms/ or a substantially similar form and process.

The Responsible Party may only process the personal information of a data subject who is a customer of the Responsible Party:

- If the Responsible Party has obtained the contact details of the data subject in the context of the sale of a product or service;
- For the purpose of direct marketing of the Responsible Party's own similar products or services; and
- if the data subject has been given a reasonable opportunity to object to the use of their personal information for the purpose of electronic direct marketing;
- Any communication for the purpose of direct marketing must contain sender's details;
- An address or other contact details to which the recipient may send a request that such communications cease must be provided by the Responsible Party.

Responsible Parties and Operators who conduct directing marketing activities shall establish directing marketing practices as described in 12.1. above when conducting directing to recipients in the Residential Community Industry.

12.1. Directories

A data subject who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, must be informed, free of charge and before the information is included in the directory of the following:

- 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 versions of the directory;
- A data subject must be given a reasonable opportunity to object to such use of his, her or its personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use.

The points above do not apply to editions of directories that were produced in print or offline electronic form prior to the commencement of POPIA.

"Subscriber", for purposes of this section, means any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services.

Responsible Parties who publish directories shall establish directory notification practices informing data subjects of the purpose of the directory and further uses thereof as described on 12 above. They shall also give data subjects a reasonable opportunity to object to their inclusion in directories.

12.2. Automated Decision Making

Automated decision-making is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred.

In terms of POPIA section, a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such a person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

The provisions provided above do not apply if the decision:

(a) has been taken in connection with the conclusion or execution of a contract, and;

(i) the request of the data subject in terms of the contract has been met; or

(ii) appropriate measures have been taken to protect the data subject's legitimate interests or;

(b) is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

The appropriate measures, referred to in POPIA subsection (2) (a) (ii), must:

(a) provide an opportunity for a data subject to make representations about a decision referred to in subsection (1); and

(b) require a Responsible Party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of paragraph.

Examples of automated decision making are:

Information Matching Programmes

Information Matching means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject.

Profiling:

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Organisations use profiling to:

- find something out about individuals' preferences;
- predict their behaviour; and/or
- make decisions about them

Your organisation is carrying out profiling if you:

- collect and analyse personal data on a large scale, using algorithms, AI or machine-learning;
- identify associations to build links between different behaviours and attributes;
- create profiles that you apply to individuals; or
- predict individuals' behaviour based on their assigned profiles.

Source: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/

Responsible Parties who conduct automated decisions making practices shall provide an opportunity for a data subject to make representations about a decision. They shall also provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations as described in 12.1 in this code.

13. Transborder information flows

13.1. Transfers of personal information outside Republic

Section 72 states that a Responsible Party may not transfer the personal information of a data subject to a third party or recipient who is in a foreign country unless:

13.1.1. The third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection effectively upholds principles for reasonable processing of the information that are substantially similar to the

conditions for the lawful processing of personal information (the 8 Conditions for Lawful Processing contained in POPIA Chapter 3)

13.1.2. Includes provisions that are substantially similar to this section relating to the further transfer of personal information from the recipient to third parties who are in a foreign country

13.1.3. The data subject consents to the transfer of personal information to a to a third party or recipient who is in a foreign country

13.1.4. The transfer is necessary for the performance of a contract between the data subject and the Responsible Party

13.1.5. 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

13.1.6. The transfer is for the benefit of the data subject, and—

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer and;

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it

13.2. **''binding corporate rules**'' means personal information processing policies, within a group of undertakings (group of companies) which are adhered to by a Responsible Party or operator within that group of undertakings when transferring personal information to a Responsible Party or operator within that same group. Binding corporate rules only apply to international transfers and cannot be used within South Africa.

13.3. **Guidance for Schemes for Transborder Information Flows**.

In practice this means that a Responsible Party (RCC Members) or an Operator must ensure the following:

13.3.1. Ascertain the geographical location jurisdiction of the recipient of the personal information;

13.3.2. Ascertain If there is a law or regulation which is substantially to POPIA, in particular if it contains similar content to the 8 Condition for Lawful Processing;

13.3.3. Establish an agreement similar to the Responsible Party to Operator agreement which should be used for South African Operators. It is essential to ensure that the agreement contains commitments to the security of personal information. A common example is the use of a cloud service in another country.

13.4. Recommendations for the use of a cloud service provider or hosting company includes:

13.4.1. Identify and review their Terms and Conditions or Terms of Use and if available, the Data Processing Agreement Clauses for Data Protection or Personal Data Protection should be present. The names of the parties are likely to be different to those used in POPIA. In particular the Responsible Party will be the Controller and the Operator will be referred to as the Processor. There should be clauses which refer to appropriate and reasonable measures for protecting personal data.

13.4.2. It is also strongly recommended that the service provider provides information about information or cybersecurity certifications such as ISO 27001, NIST, Cloud Security Alliance or the UK Government Cyber Security Scheme.

When planning to send personal information to a recipient outside South Africa, Responsible Parties shall ascertain the geographical location of personal information, ascertain of there is a substantially similar law to POPIA in the recipient jurisdiction and establish an agreement which contains commitments to the security of personal information by the recipient. Guidance for establishing measures is provided in 13.3. above.

PART C: INFORMATION OFFICER: Duties and responsibilities of Information Officer

C1. Introduction.

The Information Officer role is by default that of the Designated Head of a Private Body in terms of the provisions of both the Promotion of Access to Information (PAI) Act, 2000 and the Protection of Personal Information (POPI) Act, 2013. The duties and responsibilities defined in section 4 in the Regulations relating to the Protection of Personal Information, 2018 are also included below.

The responsibilities defined for these roles in a private body in terms of the POPI Act (POPIA) and PAI Act (PAIA), are:

C2. POPI Act Section 55 (1): An information officer's responsibilities include:

(a) the encouragement of compliance, by the body, with the conditions for the lawful processing of personal information;

(b) dealing with requests made to the body pursuant to this Act;

(c) working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body;

(d) otherwise ensuring compliance by the body with the provisions of this Act; and

(e) as may be prescribed. Regulations relating to the POPI Act, 2018: Responsibilities of Information Officers

POPI Act Regulations

Section 4 In the POPI Act Regulations relating to the Protection of Personal Information Act requires the following:

An information officer must, in addition to the responsibilities referred to in section 55(1) of the Act, ensure that-

(a) a compliance framework is developed, implemented, monitored and maintained;

(b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

(c) a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

(d) internal measures are developed together with adequate systems to process requests for information or access thereto; and

(e) internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

(2) The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

C3. POPI Act, 2013 Part B: Designation and delegation of deputy information officers

POPI Act Section 56 states that:

Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of:

(a) such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of this Act; and

(b) any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of that public or private body.

Examples of specific duties for the information officer which could be included in an appointment letter are:

- Complete initial and ongoing compliance assessments;
- Developing, publishing and maintaining a POPI Policy which addresses all relevant provisions of the POPI Act;
- Reviewing the POPI Act and periodic updates as published;
- Ensuring that POPI Act induction training takes place for all staff;
- Ensuring that periodic communication awareness on POPI Act responsibilities takes place;
- Ensuring that Privacy Notices for internal and external purposes are developed and published;
- Handling data subject access requests;
- Approving unusual or controversial disclosures of personal data;
- Approving contracts with operators as defined in the POPI Act;
- Ensuring that appropriate policies and controls are in place for ensuring the acceptable quality of personal information in line with the POPI Act are in place;
- Ensuring that appropriate security safeguards in line with the POPI Act for personal information are in place;
- Handling all aspects of relationship with the Information Regulator as foreseen in the POPI Act;
- Provide direction to any Deputy Information Officer if and when appointed.

C4. PAI Act (PAIA) Information Officer / Deputy Role Responsibilities:

a) Developing, publishing and maintaining a PAIA Manual which addresses all relevant provisions of the PAIA Act, including but not limited to the following;
b) Meets the requirements for contents of the Manual;
c) Establishing processes for information requests;
d) Handling requests for information;

e) Provide direction to any Deputy Information Officer if and when appointed.

Schemes shall appoint an Information Officer and where required, one or more, Deputy Information Officers. The appointments shall be made through an appointment letter containing the duties and responsibilities described n C1, C2, C3 and C4 above.

C5. Residential Community Industry Applicability

In schemes the Information Officer shall be the head of the organisation as defined in POPIA and PAIA. The head of the organisation depends on the type of scheme. These are described below:

C5.1. Homeowners Association (HOA) registered as a Non-Profit Company:

In terms of PAIA, the head of the HOA and, therefore, the Information Officer, NPC-based HOA is the Estate Manager/Chief Executive Officer/General Manager. He or she may appoint another person as the information Officer but they retain accountability for compliance with POPIA and PAIA. The appointments shall be made in writing by the Chairman of the Board through an appointment letter which should include the duties and responsibilities set out in Part C in this code.

Note: The information Officer should not be a member of the Board of Directors in an NPC as they are not employees of the scheme. They should, however, fulfil an oversight role.

C5.2. Homeowners Association (HOA) defined by the Nonprofit Organisations Act (NPO Act).

The NPO Act incudes Voluntary Associations, Non-profit trusts and Public Benefit Organisations. In terms of the Nonprofit Organisations Act**,** the head of the scheme is the Chairman. Where an Estate Manager is employed in a NPO based scheme, he or she will be the Information Officer. In schemes where there is no Estate Manager, the Chairman shall be the Information Officer.

The appointments shall be made in writing by the Chairman of the Board through an appointment letter which should include the duties and responsibilities set out in Part C in this code.

C5.3. Sectional Title Scheme registered in terms of the Sectional Title Schemes Management Act (STSMA).

The STSMA requires a Chairman and at least 2 Directors to be appointed in schemes such as Bodies Corporate. In these schemes, the Chairman is the head and, therefore, the Information Officer. The appointments shall be made in writing by the Chairman through an appointment letter which should include the duties and responsibilities set out in Part C in this code.

C5.4. Managing Agent registered as a company in terms of the Companies Act. The head of the is the Chief Executive Officer or equivalent such as the Managing Director. The appointments shall be made in writing by Board through an appointment letter which should include the duties and responsibilities set out in Part C in this code.

C5.5. Outsourcing of Information Officer Role.

It is common practice in very small schemes for the Information Officer role to be outsourced to a Managing Agent or other service provider. In terms of C5.1, C5.2, C5.3 and C5.4 above, the responsibility for conducting the required duties may be outsourced, but accountability shall not be outsourced by the head of the scheme to an external party.

Where a scheme plans to appoint an external Information Officer, such an appointment must be established with a natural person and not a juristic person. A written contract in which the duties and responsibilities of the Information Officer as detailed in Part C in this Code of Conduct are defined must be established. Management of the performance of the external Information Officer must be conducted by the Board of Directors in conjunction with the governance practices defined in section 1: Condition 1: Accountability contained in this Code of Conduct. Appropriate metrics for performance measurement shall be incorporated into the contract.

C5.6. Appointment of Deputy Information Officers.

The information Officer may appoint one or more Deputy information Officers. They should be persons who fulfil a management or supervisory role and should have good knowledge of the organisation.

The appointments shall be made in writing by the Board through an appointment letter which should include the duties and responsibilities set out in Part C in this code.

It must be noted only employee(s) of a body can be designated as a Deputy Information Officer. Please refer to section 7.2. in the Guidance Note on Information Officers and Deputy Information Officers published by the Information Regulator.

C5.7. Monitoring and Maintenance of Compliance by Schemes

Section 4 (1) (a) in the POPIA act Regulations requires the Information Officer to develop, implement, monitor and maintain a compliance framework for POPIA.

Information Officers in schemes shall ensure that compliance is monitored and maintained. This should include the monitoring and maintenance of the 8 Conditions described in Part B in this code.

PART D: MONITORING OF COMPLIANCE WITH THIS CODE OF CONDUCT

The RCC and NAMA shall conduct annual questionnaires which will include responses by members about their compliance measures in terms of Part B of this code.

The RCC and NAMA shall submit an annual report to the Information Regulator including the following:

Information on how compliance has been monitored with the code by members such as an annual questionnaire and reported on is provide below:

- Aggregated information from monitoring activities.
- The number of complaints in relation to the code received annually
- The average time taken to resolve the complaints.
- Statistical information about the nature of the complaints
- Statistical information about the outcomes of the complaints
- Information about the remedies awarded in resolving the complaint.

PART E: COMPLAINTS HANDLING PROCESS

D1. Introduction.

Data subjects have the right to submit a complaint regarding the alleged unlawfulness of processing or interference with the protection of their personal information. This section is intended to provide a framework for handling complaints by the RCC and NAMA.

D2. Complaints Handling Process

The Information Regulator has published a complaint form and a process for the submission of complaints to them directly. An instruction has, however, been defined in the Guideline to Develop Codes of Conduct section 26.1.6 which states that complaints must first be submitted to the Responsible Party that has allegedly compromised their personal information. In view of this, member estates shall implement their own Complaints Handling Processes based on the guidelines set out below.

i. Develop a Complaint Form substantially similar to *Form 5: Complaint regarding Interference with the Protection of Personal Information* published by the Information Regulator;
ii. Publish the Complaint Form in a manner which is accessible to all data subjects;
iii. Accept all complaints submitted from data subjects which are based on the estate's Complaint Form;
iv. Reject the complaint if it has not been submitted using the RCC's or estate's Complaint Form and request correct submission to be made;
v. Log the date and content of the complaint in the Complaints Register;
vi. Check the following:
    a. Does it contain the name and an address for correspondence?
    b. Has the requester used a pseudonym?
    c. Does it describe the complaint adequately?
vii. Check if there is enough information to be sure of the requester's identity? (Yes: Proceed; No: Ask the requester for any evidence you reasonably need to confirm their identity);
viii. Acknowledge receipt of the complaint in writing within 3 days of receipt;
ix. Provide the name, contact details and detail of the complainant to the applicable department or Operator;
x. Investigate the complaint to ascertain whether it can be resolved immediately;
xi. Assess the validity and basis of the complaint;
xii. Inform the complainant of the decision and course of action that will be taken in order to resolve the matter relating to the complaint;
xiii. Provide the complainant the opportunity to accept or reject the response;
xiv. If the complainant accepts the response, close the complaint. If the complainant does not accept the response, inform them that they should submit a complaint to the Information Regulator.

D3. Complaint Submission Process

Members may submit a complaint to the RCC, NAMA and any other Responsible Party by contacting the appropriate Information Officer or by following their compliant process made available by the Responsible Party. Contact details for RCC and ARC are provided in Part I in this code.

The RCC, NAMA and other Responsible Parties shall implement a Complaint Handling process as described in D1 and D2 in this code. They stall also publish the contact details and guidance for complaints to be submitted.

PART F: INDEPENDENT ADJUDICATOR

Section 63 in POIA makes provision for an independent adjudicator to be appointed in conjunction the complaints Handling process as defined below:

i. The RCC and NAMA may appoint an independent adjudicator to hear the complaint and adjudicate thereon.

ii. The adjudicator must apply the principles stipulated in section 44 of POPIA in determining any decisions to the unlawful processing of personal information.

iii. The adjudicator will utilise a process that is impartial, accessible, flexible, and efficient and must also observe the principles of natural justice and procedural fairness.

iv. On completion of the investigation, the independent adjudicator must send a report containing its determination, together with reasons for the determination, to the RCC and the relevant member.

v. The adjudicator's determination will continue to have effect unless and until the Regulator makes a determination under Chapter 10 of POPIA relating to the complaint or unless the Regulator determines otherwise.

vi. The adjudicator must prepare and submit a report, in a form satisfactory to the Regulator, within five (5) months of the end of a financial year of the Regulator on the operation of a code during that financial year. The financial year end of the Regulator is the 31st of March of each year.

PART G: ENFORCEMENT PENALTIES CONCERNING NON-COMPLIANCE WITH THE CODE

i. Compliance with this Code of Conduct is a mandatory requirement for membership to the RCC and NAMA. Members may, alternatively, provide adequate equivalent evidence as their POPIA compliance framework.
ii. The RCC and NAMA may, following a complaint, review or appoint an assessor to review a member's compliance with this Code. An Independent Adjudicator may also be appointed where necessary.
iii. The RCC and NAMA may, depending on the impact of non-compliance on a third party, deal with such non-compliance in accordance with its membership rules.

PART H: REVIEW AND EXPIRY OF THE CODE

i. The RCC and NAMA will review this Code annually and apply for approval by the Regulator for any variations that may result from such a review.
ii. If the Regulator has provided its approval, we will publish the revised Code on our website within 14 (fourteen) days from the date of publication of the varied Code in a Government Gazette
iii. The Regulator may review the operation of an approved code within a 5 (five) year period or as and when deemed necessary. We will consult with the Regulator during such a review process and inform you of the outcome.
iv. This Code shall in any event expire within a minimum period of 5 (five) years. The RCC shall take such steps as may be necessary to apply for the approval of a new Code before the expiry of the current Code.

PART I: CONTACT DETAILS

Contact details for queries about this Code of Conduct may be directed to:

RCC Contacts

RCC Chairman:

Hannes Hendriks

Email: cam@pecanwoodScheme.co.za

RCC Director and Secretary:

Jeff Gilmour

Email: info@rccouncil.co.za

RCC Deputy Chair:

Stephan Vorster

Email: ceo@ebotseScheme.co.za

NAMA Contacts

Lizbe Venter

General Manager

Email: gm@nama.org.za

Annexure A: Security Safeguards Guidance

Securing Personal Information in line with POPIA Condition 7: Security Safeguards

Table of Contents

1. Introduction

There is often a perception that the purpose and scope of information and cyber security is purely to keep external hackers away from an organisation's systems and information. While this an essential part of the subject, it is also essential that the management of people and processes relating to the security of information is conducted as internal risks to information also exist in organisations.

The Protection of Personal Information Act of 2013 (POPIA or the POPIA Act) requires all organisation, both Responsible Parties and Operators, to comply with Condition 7: Security Safeguards, in particular sections 19, 20 and 21.

In practical terms this means that they should implement and maintain appropriate organisational and technical measures for securing personal information. POPIA also requires that organisations consider generally accepted practices for Information Security when implementing appropriate and reasonable measures. Several security standards and frameworks exist but these can be too complex for small to medium sized organisations to adopt.

2. UK Cyber Essentials Framework

The recommended measures provided below are based on the UK Cyber Essentials Framework found in the UK ICO SME Toolkit. Source:: https://www.ncsc.gov.uk/cyberessentials/overview

This provides practical guidance for implementing and managing information security in small to medium sized organisations. The scheme is based on 20 sub-categories described below:

2.1. Risk Management

Your organisation should ensure that information security risks are assessed and appropriately managed. These should include a strong focus on risks to personal information in terms of POPIA requirements.

2.2. Information security policy

Your organisation should implement an information security policy that covers all aspects of information security within your organisation. Sub-policies should also be implemented, Annexure A provides a recommended list of information security policies

2.3. Information security responsibility

Your organisation should identify a person or department and assign day-to-day responsibility for information security. Annexure B contains a sample appointment letter for an Information Security Officer.

2.4. Outsourcing / Operators

Your organisation should establish written agreements with third party service providers who process personal information that include appropriate information security clauses and obligations. POPIA regards these as Operators and includes a legal requirement for the establishing and monitoring of written agreements with these parties.

You should also establish protocols to allow periodic security reviews of the security arrangements in place to provide assurances of compliance to contracts/agreements.

Section 3 below provides guidance for establishing practical organisational and technical measures

2.5. Incident management

Personal information security breaches may arise from a theft, an attack on your systems, the unauthorised use of personal information by a member of staff, or from accidental loss or equipment failure. However a breach occurs, it is important that you deal with it effectively and learn lessons from it.

If the breach (also know a security compromise) involves personal information, you should report it to the Information Regulator using FORM-SCN1-Security-Compromises-Notification as soon possible. This is available on the Information Regulator's website at https://inforegulator.org.za/ under POPIA/Forms.

2.6. Education and awareness

Your organisation should brief all staff on their security responsibilities, including the appropriate use of business systems and ICT equipment.

You should also train your staff to recognise common threats such as phishing emails and malware infection, and how to recognise and report personal information security breaches.

You should ensure staff are trained on or shortly after appointment with updates at regular intervals thereafter or when required.

2.7. Secure areas

- Your organisation should establish entry controls to restrict access to premises and equipment on a need-to-know basis. Your organisation prevents unauthorised physical access, damage and interference to personal data.

- You should lock away paper records and mobile computing devices when not in use.

- Implementing a 'clear desk' policy and introducing compliance checking mechanisms within your organisation will be a valuable measure for information security in the workplace.

2.8. Secure storage

Your organisation should establish secure storage arrangements to protect records and equipment to prevents loss, damage, theft or compromise of personal data.

2.9. Secure disposal

My organisation has established a process to securely dispose of records and equipment when no longer required. This should include paper records and electronic records.

It is important to ensure that electronic data stored on devices such has PCs and laptops is removed using techniques such as formatting the drive or using an external service provider for the destruction. It is also important to ensure that paper records are destroyed using a fine cut shredder or by using a reputable shredding service provider.

2.10. Home and mobile working procedures**.**

Your organisation should establish a home and mobile working policy. You should also ensure the security of mobile working and the use of mobile computing devices.

2.11. Secure configuration

The default installation of ICT equipment can include vulnerabilities such as unnecessary guest or administrative accounts, default passwords that are well known to attackers, and pre-installed but unnecessary software. These vulnerabilities can provide attackers with opportunities to gain unauthorised access to personal information held in business systems. Your organisation should, therefore, establish a process to configure new and existing hardware to reduce vulnerabilities and provide only the functionality and services required.

2.12. Removable media

Your organisation should establish controls to manage the use of removable media. These should prevent unauthorised disclosure, modification, removal or destruction of personal data stored on media.

2.13. User access controls

Your organisation should establish a process to assign user accounts to authorised individuals, and to manage user accounts effectively to provide the minimum access to information. You should limit access to personal data held in information systems.

2.14. System password security

Your organisation should enforce regular password changes as well as the user of strong passwords. You should also limit the number of failed login attempts. Usernames and passwords are valuable to hackers and should be managed effectively.

2.15. Antivirus and Malware protection

Computers can be infected with malware (for example, viruses, worms, Trojans, spyware) via email attachments, websites and removable media. This can result in the loss or corruption of personal information. Your organisation should:

- install antivirus, malware protection and file encryption software to regularly scan your computer network in order to detect and prevent threats and vulnerabilities;
- Make sure the software is kept up-to-date; and
- Educate users about common threats.

2.16. Back up and restoration

Your organisation should establish a process to routinely back-up electronic information, including personal information, to help restore information in the event of disaster. Data stored in cloud services should also be backed up to a separate cloud service. You should also test the restoration of backups regularly to check the effectiveness of the back-up process.

2.17. Monitoring

Your organisation should establish a process to log and monitor user and system activity to identify and help prevent data breaches. Your organisation should record events and generate evidence.

Monitoring should also include intrusion attempts through cloud services and operators; they should be instructed to provide regular reports to you.

2.18. Patch management

Your organisation should establish a process to ensure that software is kept up-to-date and the latest security patches are applied. This will help to prevent the exploitation of technical vulnerabilities.

2.19. Boundary firewalls

Your organisation should establish boundary firewalls to protect computers from external attack and exploitation. Firewalls should aim to ensure the protection of personal data in networks.

3. Practical Measures based on the UK Cyber Essentials Framework

Practical organisational and technical measures found in the UK Cyber Essentials Framework described above are provided below. The implementation and maintenance of these will satisfy the requirements contained on POPIA Condition 7: Security Safeguards. They will also represent a coherent but simple information security management system.

3.1. Organisational Measures

Organisational Measures should include the UK Cyber Essentials Framework listed below as a minimum:

- The appointment of an Information Security officer or manager to manage the security of information. This is normally a company-wide role.
- Identification of reasonably foreseeable risks to personal information.
- Ensuring that identified risks are managed effectively.
- Implementation of an Information Security Policy which covers the management of information security.
- Implementation of sub-policies for guiding employees in their responsibilities for information security. Annexure A provides a recommended list of information security policies.
- The management of access rights to systems involved ensuring a 'least privilege' principle is implemented. This means that a user or user profile should only have access to the specific data, resources and applications needed to complete a required task.
- Employee training covering the basics of information security, highlighting the importance and responsibility for ensuring the confidentiality of information, especially of personal information.
- Obtaining an undertaking from all employees to the protection of company information, including personal information.
- Establishment and management of operator contracts including cloud service providers if appropriate.
- Conduct an annual review of your organisation's security posture, consider using the services of an external service provider to conduct the assessment.

3.2. **Technical Measures**

Technical Measures should include the following as a minimum:

- Implementing a perimeter firewall.
- Ensuring strong passwords on all devices involved in the service being provided.
- Implementing and maintaining endpoint security technology including antivirus, antimalware, anti-ransomware and data encryption on all front-end and back-end devices.
- Ensure that the security measures listed above are effective and that they address the identified risks in the risk assessment described in 2.1.
- Monitoring attempted intrusions into the environment which may result in a compromise or breach of personal information. This should include services provided by operators
- Establish a process to routinely back-up electronic information, including personal information and cloud service information. You should also test the restoration of backups regularly to check the effectiveness of the back-up process.
- If your organisation uses Microsoft 365, it is important to ensure that your O365 system is secure as Microsoft will not accept responsibility for the loss or compromise of your data without such measures being in place. Annexure C provides a list of questions to help you assess this.

Annexure A.1. Recommended list of information security policies

- Information Security Policy (overarching policy)
- Clean Desk Policy
- Acceptable Use Policy
- Access Control Policy
- Information Security Incident Management Policy
- Information Technology Equipment Disposal Policy
- Personal Information Backup Policy
- POPIA Staff Notice & Consent Form template
- POPIA Employee compliance commitment undertaking

Annexure A.2: Microsoft 365 Cloud Security Checklist

- Are Office 365 Backups taken?
- Is Multi-Factor Authentication in use?
- Are App Passwords in use e.g. SharePoint?
- Is File Encryption in use in the Cloud?
- Is Malware and Ransomware protection ins use in the Cloud?
- Is Encryption for data in transit in use e.g. SSL/TLS?
- Is Microsoft Online Exchange Protection (OEP) or similar solution is use?
- Are Automated intruder alerts raised e.g. failed login in use?
- Is real-time threat detection in use?
- Are Data Loss Prevention Processes/solutions in place?
- Are Role Based Access Control (RBAC) policies and practices in place?
- External Support company in use? If so, you have a written contract in place?

Annexure B: Personal Information Risk Assessment and Management

Table 2 below provides an example of a practical approach which can be used to assess and manage risks to personal information.

Key aspects of the approach included in the example are:

- Risk name: Name of the risk
- Risk description: A description of the risk
- Probability of risk occurring: High, Medium or Low probability
- Impact if risk does occur: High, Medium or Low impact
- Overall risk assessment: High, Medium or Low risk based on a balance of the points above
- Possible risk treatment action: Action for treating and managing the risk
- Risk owner and Review date: The name of the person responsible for managing the risk and the next review date of the status of the risk.

Table 2: Personal Information Risk Management Tool

Risk name	Risk description	Probability of risk occurring (High, Medium or Low)	Impact if risk does occur (High, Medium or Low)	Impact of risk occurring (High, Medium or Low)	Overall risk assessment (High, Medium or Low)	Possible risk treatment action	Risk owner and Review date
Physical Risks to Personal Information							
Office Park Access	Unauthorised persons could access the office park and enter unsecured buildings	Medium	High	High	Medium	• Visitor authentication. • Strong physical security at main gate	Security manager: End of Q1
Building access	Unauthorised persons could access areas within estate office	Medium	High	High	Medium	• Visitor authentication. • Strong physical security at estate building entrance	• Security manager: • End of Q1
Visitor access	Unauthorised visitor access to estate or building	Medium	High	High	Medium	• Visitor authentication. • Strong physical security at estate	• Security manager: • End of Q1

						building entrance	
Non-Physical Personal Information Risks							
Information Security risk	Loss of information through people (staff), also known as the Insider Threat	Medium	High	High	Medium	Security Policies and training	• Information Security Officer • End of each month
Insecure PCs, Mobile devices (hacks, breaches, loss)	Potential loss of resident and other stakeholders' personal information	High	High	High	High	Strong endpoint security suite	• Information Security Officer • End of each month
Third Party / Operator Risk	Operator risks - inadequate contractual clauses and security practices	High	High	High	High	Contracts and periodic Operator security reviews	• Information Security Officer • End of each month

Acknowledgements: Mr Glen Lambert and Dr Peter Tobin

Annexure C: RCC MOI and Resolution

Memorandum of Incorporation as emended on 12 November 2020.

Resolution passed by the Board members.

Annexure D: NAMA MOI

Memorandum of Incorporation