Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID AFRIKA

Vol. 699 8 September / September 2023 No. 49280

ISSN 1682-5845

9 771682 584003 49280

Contents

DEPARTMENT OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT

NO. 3867 **8 September 2023**

Address: 27 Stiemens Street, 4th Floor
JD House Building, Braamfontein,
Johannesburg, 2017
Tel: 010 023 5214
Fax: 0865003351
E-mail: POPIACompliance@inforegulator.gov.za

25 August 2023

NOTICE IN TERMS OF SECTION 61(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013 (POPIA) CODE OF CONDUCT: THE RESIDENTIAL COMMUNITIES COUNCIL (RCC).

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 Communities Council (RCC) that deals with how personal information will be processed in the Residential Community Industry (RCI).

2. The purpose of the code of conduct is to-
   2.1. promote appropriate practices by members of RCC governing the processing of personal information in terms of POPIA;

   2.2. encourage the establishment of appropriate agreements between members of RCC 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 RCC to be guided in their interpretation of POPIA, but also other laws or practices governing the processing of personal information, allowing for complaints against RCC 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 subjects) by institutions that are members of RCC.

Adv. FDP Tlakula (Chairperson), Adv. LC Stroom Nzama (Full-time Member), Adv. JC Weapond (Full-time Member), Ms AR Tilley (Part-time Member), Mr MV Gwala (Part-time Member)

3.2. where appropriate, agreements that may need to be concluded between members of RCC 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 RCC of the provisions of the code of conduct.

4. A notice will be published in the Government Gazette in compliance with section 61(2) of POPIA. 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 COUNCIL

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 Council

Code Prepared By:	Date & Version	For Whom
John Cato Email: johnc@iact-africa.com Dr Peter Tobin Email: petert@iact-africa.com	24 August 2023 Version 1.0	Residential Communities Council Board of Directors and Members

PART A: INTRODUCTION

1. Background

1.1. The Residential Communities Council (RCC) is a representative body acting for the Residential Community Industry (RCI) in terms of chapter 7 in the Protection of Personal Act of No 4 of 2013 (POPIA) Section 60(3)(d) and Section 61(1)(b) of the Act;

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

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

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

1.5. 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.

2. Purpose

The purpose of this Code of Conduct is to:

2.1. Provide an interpretation of the Protection of Personal Act of 2013 (POPIA) for the Residential Community Industry and RCC members;

2.2. Promote appropriate practices for members of the RCC governing the processing of personal information.

3. Scope

The scope of this Code of Conduct includes governance of the following:

3.1. The processing of personal information by members of the RCC in accordance with POPIA and PAIA;
3.2. The voluntary adherence by members of the RCC of the provisions of this Code of Conduct or evidence of an equivalent POPIA compliance framework;
3.3. Ensuring that members of the RCC accept that their membership is subject to compliance with this Code of Conduct.

4. POPIA Definitions (as defined in the Guideline to Develop Codes of Conduct)

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;

''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 person to whom personal information relates;

''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;

''Person'' means a natural person or a juristic person;

''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.

5. Definitions relating to the Residential Community Industry

"Data subject'' means a homeowner, resident, visitor, employee, director, employee of homeowner or resident, contractor, estate, Homeowners Association, service provider, managing estate.

"Responsible Party" means the organisation or person which makes decisions about the processing of personal information and processes it in accordance with the conditions for Lawful Processing. This is normally the Homeowners Association (HOA).

"Operator" means the organisation or person who processes personal information on behalf of the Responsible Party through a contract or mandate. 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 security companies, solution service providers such as community

portal services, access control, human resources and payroll, accounting firms, law firms and managing agents.

6. Governance of the Code of Conduct

6.1. The Code shall be governed by the Residential Communities Council's Board of Directors in accordance with the structures and terms of reference for governance as may be in place.

6.2. 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

6.3. The RCC Memorandum of Incorporate is provided in Annexure A.

PART B: CONDITIONS FOR LAWFUL PROCESSING OF PROCESSING PERSONAL INFORMATION

Processing of personal information in general

Introduction to Part B

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.

1. Condition 1: Accountability

1.1. Responsible Party to ensure conditions for lawful processing.

1.1.1. The Responsible Party (HOA) shall ensure accountability at all levels e.g. Boards, Estate Management team and a Risk and Compliance committee or equivalent.

1.1.2. The Homeowner's Association (HOA) shall establish an accountability structure for ensuring that measures for complying with the conditions for the lawful processing of personal information as set out in Chapter 3 of POPIA are developed, implemented, monitored and maintained. The accountability structure will include the appointment of the Information Officer and Deputy Information Officer (or as many as are required) as set out in Part B Section 55 in POPIA, the POPIA Act Regulations and Guidelines issued by the Information Regulator South Africa from time to time.

1.1.3. In accordance with generally accepted corporate governance codes of practice such as in the King IV Code™ for Corporate Governance, the Board of Directors or Governing Body, shall ensure the following:

1.2. King IV™ Principle 12: Practice 14

The governing body (Board of Directors) shall exercise ongoing oversight of the management of information and, in particular, oversee that it results in the following:

1.2.1. The leveraging of information to sustain and enhance the organisation's intellectual capital;

1.2.2. An information architecture that supports confidentiality, integrity and availability of information;

1.2.3. The protection of privacy of personal information;

1.2.4. The continual monitoring of security of information.

1.2.5. Members shall include governance mechanisms in one or more of the following committees in order to ensure the monitoring and maintenance of compliance with POPIA:

- Legal, Governance and Compliance
- Finance

- Architecture and Land use
- Security and Emergency
- Estate Infrastructure
- Communications Emergency
- Eco Infrastructure
- Information, Communication and Technology
- Human Resources and Remuneration
- Sports
- Social

In estates where none of the committees above are in place, the Board of Directors will be responsible for ensuring the monitoring and maintenance of compliance with POPIA.

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 estate sector 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 with. It should also not be used for a different purpose other than the purpose for which it was obtained. These are described further in this section.

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 Homeowners' personal information should only be collected and processed for the purpose of administrating their affairs pertaining to the estate and only the items of information for this purpose should be collected.

2.3. 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 estates and Homeowner Associations (HOAs) 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 HOAs 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 HOA (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.

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.

Although these are not defined in POPIA, the following types of consent are important to consider in residential estates:

2.3.3.1. Types of Consent

There are two types of consent which must be considered:

- **Implied Consent.**

Where consent for standard personal information is required, it can be deemed to have been given by a data subject if one or more of the criteria described in section 2 above are met.

- **Explicit Consent.**

Where Special Personal Information such as biometric information is going to be obtained and processed, explicit consent should be obtained as section 27 in POPIA does not include the other criteria referred to in section 2 above. If, however, it is not possible to obtain explicit consent, then the estate should rely on one of the above such as the legitimate interest of the Responsible Party i.e. the HOA. In order to obtain consent, member organisations should include biometric information into their Memorandum of Incorporation, Constitution or Conduct Rules as appropriate i.e. whichever document is signed by homeowners as acceptance of the organisation's rules.

Explicit 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. In practice, this is the legally authorised person such as a parent or legal guardian.

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 only apply to visitors in an estate as the criteria or legal basis for other data subject groups does not require consent.

2.4. Applying Criteria to Groups of Data Subjects in Estates

As part of the HOA's POPIA compliance programme, the HOA team must 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 estate/HOA 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 estate or homeowner. The following points should be considered.

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

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 off personal information in accordance with POPIA and the estate's Privacy Policy should be included into the document which the homeowner's signs.

2.4.2. Residents. Residents such as family members are also required to abide by the HOA'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, explicit consent should be obtained for the processing thereof. It is strongly recommended that explicit consent is obtained for the use of biometric information.

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 HOA. 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 HOA 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 should 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 estates, a condition for entering the estate 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, HOAs should include this practice as being in the legitimate interest of the HOA based on section 11.1(f) in POPIA and Section 2 above.

2.4.4.2. Legitimate interest of the Estate/HOA (Responsible Party). In estates where it is impractical to obtain either implied or explicit consent, the HOA can process personal information based on the processing being in the legitimate interest of the HOA. The main reason for this will be for ensuring safety and security. 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 HOA 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 HOA for security registration. In such cases, the contractor managers should obtain consent from their employees for sharing their personal information with the HOA.

2.4.4.4. Homeowners' and Tenants' Employees. Homeowners and tenants generally employ domestic and gardening staff. In most estates, such employees are registered either by the homeowner or their employer with the HOA. Where homeowners and tenants register their

employees, they should obtain consent for sharing the personal information with the HOA. Where domestic and gardening employees submit their own personal information to the HOA, consent should be obtained. This is typically done using a registration form.

2.4.4.5. HOA Employees. The personal information of HOA employees is required by both the HOA 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 HOA'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).

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.

In the Residential Community Industry, a common source of personal information is from attorneys within the context of a property transfer for a homeowner in an estate. This is legitimate in terms of legislation relating to property transfer and ownership.

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

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 estates, 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 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.

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

Table 1: Example Residential Estate 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 + [to be defined by the estate]. This should not be excessive.
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.

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 shared with the security company (regarded as an Operator).

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.

6. Condition 6: Openness

Condition 6 requires the Responsible Party to:

6.1. A Responsible Party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act.

6.2. Notify data subjects when collecting personal information. If personal information is collected, the Responsible Party must take reasonably practicable steps to ensure that the data subject is aware of:

(a) the information being collected and where the information is not collected from the data subject, the source from which it is collected;

(b) the name and address of the Responsible Party from which it was collected;

(c) the purpose for which the information is being collected;

(d) whether or not the supply of the information by that data subject is voluntary or mandatory;

6.3. In the Residential Estate Sector, the following measures should be implemented:

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 HOA 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. The HOA 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 estates 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 HOA 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 HOA has a duty or a right to disclose personal information in terms of law or industry codes;
- Where the HOA 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.

7. Condition 7: Security Safeguards

The subject of information security is broad and complex in its own right. Condition 7 makes the protection of personal information a legal obligation.

7.1. Condition 7 requires the Responsible Party to protect the personal information under its control to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:

7.1.1. The loss of damage to or unauthorised destruction of personal information; and
7.1.2. The unlawful access to or processing of personal information.

7.2. The Responsible Party must also identify all reasonably foreseeable risks to personal information and establish measures for reducing and managing the identified risks.

7.3. The Responsible Party must verify that the safeguards are effectively implemented. They must also ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

7.4. Residential Community Industry Practices

The following steps shall be followed by RCC members in order to address the requirements listed above:

7.4.1. A personal information risk assessment shall be conducted;

7.4.2. A suitable generally accepted information security practice i.e. one which is based on a standard or framework for information security and cyber security shall be identified and adopted. Examples of these are the NIST Cybersecurity Framework, ISO 27001 and the UK Governments Cybersecurity Scheme;

7.4.3. Appropriate and reasonable technical and organisational measures shall be implemented. These should include:

i) Roles and responsibilities for ensuring the security of personal information;

ii) Polices such as an Information Security Policy, Acceptable Use Policy and an Access Control Policy should be developed and implemented as a minimum in order to ensure that employees are guided in their responsibilities for protecting personal information;

iii) Technical controls including firewalls, antivirus, antimalware, anti-ransomware, strong passwords, and file encryption should be implemented to guard against unauthorised access to personal information.

7.4.4. The effectiveness of security safeguards must be verified to ensure effectiveness;

7.4.5. Security safeguards must be updated to ensure that new risks or deficiencies in previously implemented safeguards are managed.

7.4.6. The Responsible Party must establish a contract with each Operator in which the following duties and rights are defined:

i) Operator duties should include commitments to protecting the personal information which they process on behalf of the Responsible Party (estate in accordance with the Security Safeguards defined in section 19 in POPIA. These are effectively the appropriate and reasonable technical and organisational measures referred to above.

ii) Operator duties should also include an obligation for notifying the estate of any compromises (breaches) or suspected compromises to personal information being processed within the scope of the services provided.

iii) Responsible Party rights should include:

(1) The right to audit or assess the security safeguards which the Operator has in place;

(2) The right to ensure that the Operator makes appropriate security checks on its staff.

7.5. Notification of security compromises

7.5.1. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Responsible Party must notify the following:

- The information Regulator
- The data subject/s, unless the identity of the data subjects cannot be established

7.5.2. The notification referred must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any

measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the Responsible Party's information system.

7.5.3. The Information Regulator has published a document entitled Guidelines on completing a Security Compromise Notification in terms of Section 22 POPIA which provides guidance on reporting a personal information compromise or suspected compromise. A related form called FORM-SCN1-Security-Compromises-Notification-Fillable-Form.pdf has also been published in order to provide a process for reporting a compromise. These are available on the Information Regulator's website at:

https://inforegulator.org.za/wp-content/uploads/2020/07/Guidelines-on-completing-a-Security-Compromise-Notification-ito-Section-22-POPIA.pdf

https://inforegulator.org.za/wp-content/uploads/2020/07/FORM-SCN1-Security-Compromises-Notification-Fillable-Formpdf.pdf

8. Condition 8: Data Subject Participation

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

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.

9. 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) 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.

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.

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.

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

11.2. 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.

11.3. 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.

12. Rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making.

12.1. 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 residential estates 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.

12.2. 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.

Automated Decision Making

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 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.

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 protectionEffectively 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. **Member Obligations 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.

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.

C5. Residential Community Industry Applicability

C5.1. In estates, in particular in Homeowners Associations (HOAs), the Information Officer shall be the Estate Manager/Chief Executive Officer/General Manager as he or she is the Designated Head of the organisation. The information Officer should not be a member of the Board of Directors as they are not employees of the HOA. They should, however, fulfil an oversight role.

C5.2. The Estate Manager/Chief Executive Officer/General Manager may appoint one or more Deputy Information Officers. The Deputy can be appointed through delegation to fulfil the duties and responsibilities of the Information Officer but accountability for establishing and maintaining POPIA and PAIA compliance remains with the Information Officer. The Information Officer still retains the powers relating to the Information Officer role. The designation and delegation of these roles shall be made in writing through an appointment letter which should include the duties and responsibilities set out above and POPI Act and PAIA as well as the POPI Act Regulations.

C5.3. An exception to the above may be required in smaller estates where there is no Homeowners Association. In such situations there would not be any employees. It would, therefore, be necessary to appoint a director while ensuring that the Board of Directors fulfil an oversight role. In small estates such as these, it is common for the role of the Homeowners Association to be fulfilled by a Managing Agent. In these cases, the Director who has been appointed as the Information Officer shall remain accountable for ensuring that the Managing Agent fulfils the responsibilities for establishing and maintaining compliance in terms of an appropriate contract.

C5.4. Where an estate 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.

PART D: 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.

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.

PART E: 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 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 F: ENFORCEMENT PENALTIES CONCERNING NON-COMPLIANCE WITH THE CODE

i. Compliance with this Code of Conduct is a mandatory requirement for membership to the RCC. Members may, alternatively, provide adequate equivalent evidence as their POPIA compliance framework.
ii. The RCC 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 may, depending on the impact of non-compliance on a third party, deal with such non-compliance in accordance with its membership rules.

PART G: REVIEW AND EXPIRY OF THE CODE

i. The RCC 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 H: CONTACT DETAILS

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

RCC Chairman:

Hannes Hendriks

Email: cam@pecanwoodhoa.co.za

RCC Director and Secretary:

Jeff Gilmour

Email: info@rccouncil.co.za

RCC Deputy Chair:

Stephan Vorster

Email: ceo@ebotsehoa.co.za

Annexure A

Memorandum of Incorporation as emended on 12 November 2020.

Annexure B

Resolution passed by the Board members.