POPIA policy

(Protection of Personal Information Act 4 of 2013)

Thesen Islands Homeowners Association

("the association")

Issued: December 2021

CONTENTS

INTRODUCTION

The Protection of Personal Information Act ("POPIA") was promulgated on 26 November 2013. POPIA is intended to promote the right to privacy in the Constitution, while at the same time protecting the flow of information and advancing the right of access to and protection of information.

POPIA establishes the rights and duties that are designed to safeguard personal data. In terms of POPIA, the legitimate needs of organisations to collect and use personal data for business and other purposes are balanced against the right of individuals to have their right of privacy, in the form of their personal details, respected.

POPIA applies to a particular activity, i.e. the processing of personal data, rather than a particular person or organisation. Therefore, if you process personal data then you must comply with POPIA and you must handle personal data in accordance with POPIA's data protection principles.

The term "processing" in terms of POPIA has a very wide meaning. It is intended to cover any conceivable operation on data, ranging from collecting, recording, and holding, to the subsequent disclosure and eventually destruction of data.

The Act can be summarised as follows:

- It sets out the rules and practices which must be followed when processing information about individuals and juristic persons;
- It grants rights to individuals in respect of their information; and
- It creates an independent regulator to enforce these rules, rights and practices.

Definitions:

1) Data subject means the person to whom personal information relates.

2) Processing means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

b) dissemination by means of transmission, distribution or making available in any other form; or

c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

3) Record means any recorded information-

a) regardless of form or medium, including any of the following;

(i) writing of any material;

(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
(iv) book, map, plan, graph or drawing;
(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
b) in the possession or under the control of a responsible party;
c) whether or not it was created by a responsible party and
d) regardless of when it came into existence.

4) 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) 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, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, 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.

Chapter 1: DATA PROCESSING ACTIVITIES

1.1 IDENTIFICATION OF DATA PROCESSING ACTIVITIES

The company engages in the following data processing activities:

1.1.1 Personal information of employees
1.1.2 Personal information of home owners (individuals and juristic persons)
1.1.3 Personal information of tenants
1.1.4 Personal information of visitors
1.1.5 Personal information of contract workers

1.2 PURPOSE FOR COLLECTING DATA

Personal Information must be collected for a specific, explicitly defined, and lawful purpose related to the function or activity of the responsible party. The data subject must be made aware of the purpose of the collection.

Only adequate and relevant information should be collected, and any excessive information collection should be prevented.

The Responsible Party shall ensure that personal information will not be collected indiscriminately, but by fair and lawful means, and be limited to what is necessary to fulfil the specific purpose for which the Personal Information is being collected.

The association's purpose for collection of personal information of employees is for the association to have the necessary contact details of the employee for interaction, banking details for payment of salaries and next of kin details for emergencies. Personal information such as the employees' tax numbers and addresses are also collected for inclusion on payslips and IRP5's.

Therefore, the personal information is collected for the association to comply with the Basic Conditions of Employment Act (BCEA) section 31 as well as the Income Tax Act.

As per the BCEA, specific records to be maintained by the employer also includes the employee's job description, working hours, leave information, remuneration paid, date on which employment commenced and notice period. The employer must retain such data for three years after termination of employment.

The Unemployment Insurance Contributions Act, together with the Income Tax Act, obliges employers to retain records of remuneration paid, tax which has been deducted and unemployment insurance fund contributions and payments for each employee. The records must be maintained in such form, including any electronic form, as may be prescribed by the revenue authorities. These records should be kept for five years from the date of the last entry and must be available for inspection by the South African Revenue Service and Unemployment Insurance Fund officials.

The association's purpose for collection of personal information of homeowners, is for the association to have the necessary contact details for interaction with homeowners (email and phone numbers etc), and information relating to accounts and levies etc.

The association's purpose for collection of personal information of tenants of homeowners, is for the association to have the necessary contact details for interaction with tenants in case of emergency or if any other form of contact needs to be made.

The association's purpose for collection of personal information of contract workers, is for the association to have knowledge of who entered the premises for security purposes, and also the necessary contact details in case of emergency etc.

The Association is also required to collect information as required by law, for example the entry register needed with temperatures for COVID Tracing etc.

1.3 RIGHTS OF DATA SUBJECTS

Data subjects have the following rights:

- Objection to the use of personal information.
- Notification if information is being used for something other than what was consented for.
- Establishing whether the responsible party holds information.
- Request that information be corrected, destructed or deleted.
- Refuse processing for direct marketing by unsolicited electronic communications.
- Lodge a complaint with the Information Regulator.
- Institute civil proceedings. (Sec 99)

1.4 ACCOUNTABILITY

The Responsible party must ensure that the conditions set out in the Act and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

1.5 PROCESSING LIMITATIONS

The conditions for processing information are as follows:

- Data subjects must consent.
- Data subject may withdraw consent.
- Data subject may object on reasonable grounds.
- Consent is necessary to carry out actions to conclude or perform a contract to which the data subject is a party.
- Processing can continue if it is necessary for the conclusion or performance of a contract to which the data subject is a party;
- Processing can continue if there is a legal obligation to do so;
- Processing can continue if it protects the legitimate interests of the data subject;
- Processing can continue if it is necessary for the pursuit of legitimate interests of the responsible party.

The responsible party must restrict processing of personal information if—

- its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;
- the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;
- the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or
- the data subject requests to transmit the personal data into another automated processing system.

1.6 SOURCE OF DATA COLLECTION

Personal Information must be collected directly from the data subject except if:

- the information is contained in a public record or has deliberately been made public by the data subject.
- the data subject has consented to the collection from another source; or
- collection from another source would not prejudice a legitimate interest of the data subject.

Collection from another source is necessary:

• to maintain law and order.
• to enforce legislation concerning the collection of revenue.
• for the conduct of court or tribunal proceedings.
• in the interests of national security.
• to maintain the legitimate interests of the responsible party.
• compliance would prejudice a lawful purpose of the collection; or
• compliance is not reasonably practicable in the circumstances of the particular case.
• further processing must be compatible with the purpose for which it was collected, unless the data subject gives consent to the further processing

Chapter 2: TRAINING POLICY

2.1 INITIAL TRAINING

Staff are trained for first time adoption of the Act with the approval of this policy. This approved policy will be given to staff in writing and they will confirm in writing to the General Manager that they have read and understood this policy.

2.2 NEW STAFF MEMBERS

Any new staff members will receive training as part of their induction to the company.

2.3 ONGOING TRAINING

Staff will receive ongoing training for any changes in the Act.

Chapter 3: WRITTEN CONTRACTS

3.1 WRITTEN CONTRACTS IN PLACE

Employment contracts are signed with all new employees of the company containing relevant clauses for the use and storage of employee information, or any other action so required, in terms of POPIA.

Every employee currently employed by the association will be required to sign an addendum to the Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA.

The above is also applicable for contracts signed with homeowners, tenants and any other third party.

3.2 CLAUSES IN CONTRACTS

A clause is contained in all written contracts informing the individual as to the way their personal information is used, protected, disclosed and destroyed and also the purpose for which said information will be used.

In addition, the association guarantees its commitment to protect the individuals' privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

Clauses included in contracts with anyone processing personal information on behalf of the company:

- They are to treat the information as confidential and not disclose it unless required by law.
- They are to apply the same security measures as the responsible party.

Chapter 4: SECURITY MEASURES

Security measures are put in place to prevent the unauthorised or unlawful processing of personal data or access to personal data, including accidental loss or destruction or damage to personal data.

4.1 INFORMATION RETENTION PERIODS

Records must not be retained any longer than is necessary for achieving the purpose for which it was collected unless;

- further retention is required by law;
- the responsible party is reasonably required to keep it;
- retention is required by a contract between the parties;
- the data subject consents to the further retention.

Personal information shall be retained as prescribed by laws and regulations applicable. Personal information of employees, homeowners and contract workers will be retained during the duration of their contracts with the association. If an employee leaves the employee of the association, employee personal information will be kept in accordance with the timeframes set out in point 1.2 of this policy (except for information relating to disciplinary action, which will be kept indefinitely). If a homeowner sells their property and cease to be a member of the association, the retention of their personal information will be seven years.

4.2 SECURITY SAFEGUARDS

It is a requirement of POPIA to adequately protect the Personal Information we hold and to avoid unauthorised access and use of your Personal information. We will continuously review our security controls and processes to ensure that your Personal Information is secure.

Security controls over personal information include access control to the server on which electronic documents are stored and access control to hard copy documents in the admin office. (Only relevant authorised employees have access to personal information). Security measures also include the necessary firewalls for electronic information and physical security measures such as burglar bars and an alarm system for hard copy information. Personal information is stored in the Cloud with reputable service providers such as Microsoft whom maintain robust security controls to restrict unauthorised access to any data.

All electronic files or data are backed up by our IT Service Provider who is also responsible for system security which protects third party access and physical threats.

4.3 DESTRUCTION PROCESSES AND PROCEDURES

Personal Information must be destroyed, deleted or de-identified as soon as is reasonably practical. Destruction or deletion must be done in a manner that prevents its reconstruction in an intelligible form.

Once the retention period for personal information has expired, the information is deleted (if electronic) or destroyed (shredded if hard copy).

Chapter 5: CONTINUED COMPLIANCE WITH THE ACT

Processes and procedures are in place to ensure that data is kept up to date and current and accurate at all times.

5.1 INFORMATION QUALITY

Information must be complete, accurate, not misleading and updated where necessary.

5.2 OPENNESS

The association must take reasonably practicable steps to ensure the Data Subject is aware of:

- the information being collected;
- the name and address of the Responsible Party;
- the purpose for which the information is being collected;
- whether or not the supply of the information is voluntary or mandatory;
- the consequences of failure to provide the information;
- any particular law authorising the requiring of the collection;
- the right of access to and the right to rectify the information collected;
- the fact that, where applicable, the responsible party intends to transfer the information to a third country/international organisation and the level of protection afforded by that third country/organisation; and
- the right to object to the processing of the information

A clause referring to the above, are included in the company's engagement letters signed with clients.

Chapter 6: INFORMATION OFFICER RESPONSIBILITIES

• Encourage compliance with the information protection conditions in terms of Section 55 of POPIA;
• Developing, publishing and maintaining a POPIA Policy which addresses all relevant provisions of the POPIA Act;
• Reviewing the POPIA Act and periodic updates as published;
• Ensuring that POPIA Act induction training takes place for all staff;
• Ensuring that periodic communication awareness on POPIA Act responsibilities takes place;
• Handling data subject access requests;
• Approving unusual or controversial disclosures of personal data;
• Ensuring that appropriate policies and controls are in place for ensuring the Information Quality of personal information;
• Ensuring that appropriate Security Safeguards in line with the POPIA Act for personal information are in place;
• Consider requests made pursuant to POPIA;
• Work with the Regulator in relation to investigations conducted pursuant to Chapter 6 against us;
• Identify and govern all privacy related risks
• Create and implement procedures and standards to facilitate customer verification of captured and stored personal information files.
• Monitor and control the privacy requirements and responsibilities of information processing service providers or operators in terms of sections 20 and 21 of POPIA.
• Manage breach and incident investigation processes
• Create standards and procedures to manage any compromise in the security of the stored personal information correctly and appropriately.
• Investigate, analyse and document all privacy related incidents and complaints.
• Apply investigation findings to update standards, processes and systems as an on-going operational improvement routine.