

**Protection of Personal Information Management Policy**  
**of**  
**WOODLANDS LIFESTYLE HOME OWNERS ASSOCIATION**  
**(HOA)**  
**PROTECTION OF PERSONAL INFORMATION ACT**  
**NO 4 OF 2013**

## 1. INTRODUCTION

Data and personal information security laws mandate that organisation implement adequate safeguards to ensure the protection of the Home Owners Association's personal information.

The POPI Act regulates how Home Owners Association's handle, keep and secure personal information. With the appointment of the Information Regulator and the subsequent formalisation of the legislation, entities need to enhance (or if necessary, upgrade) their information technology security systems.

The development of a standard operating procedure to ensure adequate protection of personal client information which becomes available to the Home Owners Association is of utmost importance for the effective operations and risk management practices of the Home Owners Association. Moreover, internal control mechanisms to constantly review and measure adherence to procedures and processes are important risk management tools. The absence of a personal information risk management plan will expose the Home Owners Association to unnecessary risk and create a burden in respect of financial and other regulatory requirements.

The Home Owners Association subscribes to the principles expressed in the Protection of Personal Information Act and the Constitution of South Africa in respect of:

- 1 The lawful processing of client data by the Home Owners Association;
- 2 The identification and allocation of accountability, where personal data is processed contrary to the prescripts of the Act;
- 3 Follow good practice;
- 4 Protect the Home Owners Association from the consequences of a breach of its responsibilities.

## 2. OBJECTIVES

This personal information policy ensures that the Home Owners Association:

- ❖ Complies with data protection regulation and follows good practice;
- ❖ Protects the rights of members, service providers, tenants and staff;
- ❖ Is open about how it stores and processes member's data;
- ❖ Protects itself from the risks of data breaches.

## 3. SCOPE

This personal information management policy applies to all personal information held by the Home Owners Association relating to identifiable individuals, even if that information technically falls outside of the Protection of Information Act. This can include but not be limited to:

- ❖ Names of individuals;
- ❖ Postal addresses;

- ❖ Email addresses;
- ❖ Telephone numbers;
- ❖ Remuneration;
- ❖ Race and Gender;
- ❖ Information external to the immediately knowledge of an employer;
- ❖ Any other information relating to individuals.

It is understood that personal information may also include sensitive personal information, and thus the Home Owners Association acknowledges the need for increased scrutiny of its safety, protection and security measures.

#### 4. DEFINITIONS

**“Act”** means **the Protection of Personal Information Act No.4 of 2013;**

**Home Owners Association** means a non-profit company with members, established in terms of the Companies Act

**“Data subject”** means the person to whom personal information relates;

**“consent”** means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information;

**“data subject”** means the person to whom personal information relates;

**“de-identify”**, in relation to personal information of a data subject, means to delete any information that –

- (a) Identifies the data subject;
- (b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- (c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject,

**“direct marketing”** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

- (a) Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
- (b) Requesting the data subject to make a donation of any kind for any reason;

**“electronic communication”** means any text, voice, sound, or image message sent over an electronic communications network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;

**“enforcement notice”** means any notice issued in terms of section 95 of the Protection of Personal Information Act No. 4 of 2013;

**“filling system”** means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

**“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 in regard to an identifiable data subject;

**“information officer”** of, or in relation to, a –

- (a) Public body means an information office or deputy information officer as contemplated in terms of section 1 or 1; or
- (b) Private body means the head of a private body as contemplated in section 1 of the Promotion of Access to information Act;

**“Minister”** means the Cabinet member responsible for the administration of justice;

**“operator”** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

**“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 –

- i. 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;
- ii. Information relating to the education or the medical, financial, criminal or employment history of the person;
- iii. Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- iv. The biometric information of the person;
- v. The personal opinions, views or preferences of the person;
- vi. 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;
- vii. The views or opinions of another individual about the person; and
- viii. 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;

**“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;

**“Promotion of Access to Information Act”** means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

**“public record”** means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

**“record”** means any recorded information –

- (a) Regardless of form or medium, including any of the following:
  - ❖ Writing on any material;
  - ❖ 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;
  - ❖ Label, marking or other writing that identifies or describes anything or to which it is attached by any means;
  - ❖ Book, map, plan, graph, or drawing;
  - ❖ 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;

**“Regulator”** means Information Regulator established in terms of section 39;

**“re-identify”**, in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that –

- (a) Identifies the data subject;
- (b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- (c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject;

**“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. RESPONSIBILITIES

Everyone who works for or with the Home Owners Association has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone that handles personal information must ensure that it is handled and processed in line with this policy and data protection principles.

Key areas of responsibility:

- ❖ **Chairperson and Directors** are ultimately responsible and accountable for ensuring that the Home Owners Association meets its legal obligations.
- ❖ **Information Officer Responsibilities**
  - Developing, publishing and maintaining the POPIA Policy which addresses all relevant provision of the POPIA Act.

- Reviewing the POPIA Act and periodic updates as published.
  - Ensuring that periodic communications awareness on POPIA Act responsibilities takes place.
  - Ensuring that Privacy Notices for internal and external purposes are developed and published.
  - Handling of data subject requests.
  - Handling data protection questions from staff and anyone else covered by this policy;
  - Dealing with requests from individuals to see the data that the Home Owners Association holds about them;
  - Approving unusual or controversial disclosures of personal data.
  - Implementing appropriate policies and controls for ensuring the information quality of personal information.
  - Ensuring that appropriate security safeguards are in line with the POPI Act for personal information.
  - Managing the relationship with the Regulator as foreseen in the POPI Act.
- Keeping the Directors update about data protection responsibilities, risks, and issues;
  - Reviewing all personal information protection procedures and related policies;
  - Checking and approving any contracts or agreements with third parties that may handle the Home Owners Association's sensitive data.
  - Ensuring all systems, services and equipment used for storing personal information meet acceptable security standards;
  - Performing regular checks and scans to ensure security hardware and software is functioning properly;

## **6. PROTECTION OF PERSONAL INFORMATION**

The Protection of Personal Information Act No.4 of 2013 describes how organisations including Home Owners Associations must collect, handle and store as well as discard personal information.

The rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with regulatory requirements, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

This policy is underpinned by eight important principles. The principles state that data must:

1. Be processed fairly and lawfully;
2. Be obtained only for specific, lawful purposes;
3. Be adequate, relevant and not excessive;
4. Be accurate and kept up to date;
5. Not be held for any longer than necessary;
6. Processed in accordance with the rights of data subjects or competent persons if the data subject is a child;
7. Be protected in appropriate ways;

8. Not be transferred outside the borders of South Africa unless that country or territory also ensures an adequate level of protection.

The Home Owners Association has an obligation to ensure that its members, tenants, staff members and service providers maintain the same level of security when accessing and processing personal information on the information management system.

## **7. THE PERSONAL INFORMATION RISK MANAGEMENT PROCESS**

### **7.1. Data Protection Risk Identification, Analysis, Assessment and Prioritisation**

This policy helps to protect the Home Owners Association from data security risks. When assessing risk, both inherent and residual risk is considered. Inherent risk considers the “worst case scenario” whilst residual risk measures the current level of risk considering the adequacy and effectiveness of controls and measures already in place thus understanding any remaining risk to which the organisation may be exposed.

Assessment of inherent risk assists in:

- ❖ Understanding of exposure level in the event of a significant control failure;
- ❖ Identifying key controls and considering their effectiveness;
- ❖ Understanding the relationship between risks and their associated responses and controls;
- ❖ Developing effective key risk indicators and controls.

Residual risk is essential to determining the organisation’s current levels of risk and shall always be used. Determining the residual risk requires, as a pre-requisite, considering existing measures and controls that have already been implemented and assessing/ estimating the adequacy and effectiveness thereof.

### **7.2. Data Protection Control Measures**

- ❖ The only people able to access data covered by this policy shall be those who need it for their work in relation to and on behalf of the Home Owners Association as contracted to do so;
- ❖ Data shall not be shared informally. When access to confidential information is required, employees may request it from management;
- ❖ The Home Owners Association will provide training to all Directors/Employees to help them understand their responsibilities when handling data;
- ❖ Directors/Employees shall keep all data secure, by taking sensible precautions and following the guidelines below;
- ❖ In particular, strong passwords must be used and they shall never be shared. Password updates shall become routine;
- ❖ Personal information shall not be disclosed to unauthorised people, either within the Home Owners Association or externally;
- ❖ Data shall be regularly reviewed and updated if it is found to be out of date. If no longer required, it shall be deleted and permanently disposed of; unless is it required in the confines

of the law to be maintained for a fixed period of time, in which case the Home Owners Association shall store such information safely and restricted access rights align with lawful parameters;

- ❖ Employees shall request help from The Board of Directors or the Information Officer if they are unsure about any aspect of data protection;
- ❖ In the event of a breach of security regarding data the Information Officer shall notify the Information Regulator and the affected data subjects (or competent person as the case may be) as soon as reasonably possible, by such means and media as are appropriate in the circumstances to enable them to take steps to protect their interests;
- ❖ The Home Owners Association shall ensure, when requested to transfer data across the borders of South Africa, that this is so done only with the consent of the data subject and thereafter only to a jurisdiction which has rules on the protection of data substantially similar to those contained in this policy and the Protection of Personal Information Act.
- ❖ Information regarding a data subject in respect of the following shall not be processed unless the data subject has authorised such processing or unless otherwise required by law:
  - the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information;
  - the criminal behaviour of a data subject to the extent that such information relates to-
    - the alleged commission by a data subject of any offence; or
    - any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
- ❖ The Home Owners Association shall not process data regarding children unless authorised by such children's guardian or otherwise as required by law.

### **7.3. Data Use Code of Conduct**

Personal data is of no value to the Home Owners Association unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- ❖ When working with personal data, Directors/Employees shall ensure the screens of their computers are always locked when left unattended;
- ❖ Personal data shall not be shared informally;
- ❖ Data must be encrypted before being transferred electronically.
- ❖ Directors/Employees shall not save copies of personal data to their own computers. Always access and update the central copy of any data.

### **7.4. Data Accuracy**

The Home Owners Association has the responsibility to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all Directors who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.



- ❖ Data will be held in as few places as necessary. Directors/Employees shall not create any unnecessary additional data sets;
- ❖ Directors shall take every opportunity to ensure data is updated. For instance, by confirming a member's/residents details when they call;
- ❖ The Home Owners Association will make it easy for data subjects to update the information which the Home Owners Association holds about them. For instance, annual update through means of a personal contact details update form;
- ❖ Data shall be updated as inaccuracies are discovered. For instance, if a member/resident can no longer be reached on their stored telephone number, it shall be removed from the database.

### **7.5. Subject access requests**

All individuals who are the subject of personal data held by the Home Owners Association are entitled to:

- ❖ Ask what information the Home Owners Association holds about them and why;
- ❖ Ask how to gain access to it;
- ❖ Be informed how to keep it up to date;
- ❖ Be informed how the Home Owners Association is meeting its data protection obligations.

If an individual contacts the Home Owners Association requesting this information, this is called "Data Subject Access Request".

Data Subject Access Requests from individuals shall be made by email, addressed to the data controller at info@nudor.co.za. The data controller shall supply a standard request form. The data controller will aim to provide the relevant data within (5 business) days.

The data controller will always verify the identity of anyone making a Data Subject Access Request before handing over any information.

### **7.6. Disclosing data for other reasons**

In certain circumstances, the Protection of Personal Information Act and other legislation which the Home Owners Association is subject to allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Home Owners Association will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Home Owners Association.

### **7.7 Providing information**

The Home Owners Association aims to ensure that individuals are aware that their data is being processed, and that they understand:

- ❖ How the data is being used;
- ❖ How to exercise their rights.

To these ends, the Home Owners Association has a privacy statement, setting out how data relating to individuals is used.

### **7.8 Incident Management**

The Home Owners Association aims to ensure no unauthorised use or access to the personal information of a data subject. However, in the event there is a breach or compromise the “responsible party” i.e. Home Owners Association shall ensure the following:

- ❖ Notify the Information Regulator of the breach;
- ❖ Notify the data subjects who have been the subjects of the breach within 72 hours of the breach having occurred;
- ❖ Investigate the nature of the breach and the causal reasons as to why the breach has occurred;
- ❖ Determine the necessary action(s) that may be necessary to remedy the breach having occurred, and or internal processes and procedures that may have led to contributing to the breach having occurred;
- ❖ Capture the breach on the privacy risk register;
- ❖ Respond to complaints from data subjects who may be seeking compensation as a result of the unauthorised leaking of or access to their personal information;
- ❖ Restore the integrity of systems, processes and procedures through appropriate action to avoid a recurrence of a future breach or compromise of the personal information of data subjects.

### **8. REVIEW OF POLICY**


The contents of the policy will be reviewed by the Board of Directors together with the Information Officer on an annual basis. Compliance with this policy shall be reviewed annually and reported on by the Board of Directors and Information Officer.

### **9. OWNERSHIP AND ACCOUNTABILITY**

This Protection of Personal Information Management Policy of the Home Owners Association is duly registered under the Companies Act.

As the Chairperson, I confirm that this policy is hereby adopted and commit to its successful implementation.

Full Name of Chairperson:

Signature:  \_\_\_\_\_ Date: 4 September 2023