

Protection of Personal Information (POPI)

EXTERNAL PRIVACY POLICY

PINOTAGE VILLAS HOME OWNERS ASSOCIATION

INDEX

1. Definitions 1
2. Introduction 3
3. Objective of the Policy 3
4. POPIA Core Principles 3
5. Consent 4
6. Collection, Processing and Sharing 5
7. Storage of Information 5
8. Disposal of Information 6
9. Internet and Cyber Technology 6
10. Third Party Operators 8
11. Banking details 8
12. Information Officer and Duties 9
13. Availability and Revision 10

ANNEXURES

Form 1: Objection to Processing

Form 2: Request for Correction or Deletion

Form 3: Consent of Data Subject

ANNEXURES

Form 1: Objection to Processing 11

Form 2: Request for Correction or Deletion 12

Form 3: Consent of Data Subject 14

1. DEFINITIONS

“biometrics”: means a technique of personal identification that is based on physical, physiological or behavioral

characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

“child”: means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent

person, to take any action or decision in respect of any matter concerning him- or herself;

“Competent person”: means any person who is legally competent to consent to any action or decision being taken in respect

of any matter concerning a child;

“consent”: means any voluntary, specific and informed expression of will in terms of which permission is given for the

processing of personal information;

“Constitution”: means the Constitution of the PVHOA amended from time to time;

“Data subject”: means the person to whom personal information relates and for the purposes of PVHOA, this will include but

not be limited to all members of the PHOA, employees, external service suppliers and all associates of PHOA;

2

“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 of PVHOA, legal services to the

data subject; or b) Requesting the data subject to make a donation of any kind for any reason;

“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,

“Electronic communication”: means any text, voice, sound or image message sent over an electronic communication

network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;

“Filing system”: means any structured set of personal information which in the case of PVHOA consist of physical files kept in

the offices of PVHOA together with the data filed on the various software systems used by PVHOA;

“Information officer”: of PVHOA will mean the person appointed by the Trustees of the PVHOA from time to time;

“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 and in the context of this Policy will mean all third-party operators of

information collected by the PVHOA;

“PVHOA”: means the PINOTAGE VILLAS HOME OWNERS ASSOCIATION constituted of all owners of properties, both freehold and

sectional title in all phases of the development known as KLAPMUTS and which is bound by the provisions of this

Constitution;

“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: Information relating to the education or the medical,

financial, criminal or employment history of the person; Any identifying number, symbol, e-mail address, telephone number,

location information, online identifier or other particular assignment to the person; The biometric information of the person;

The personal opinions, views or preferences of the person; Correspondence sent by the person that would reveal the contents

of the original correspondence if the message is of a personal or confidential nature; The views or opinions of another

individual about the person; and 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. The following information is expressly

excluded from the definition of “personal information” for purposes of the functions fulfilled by the PHOA:

- i) Property descriptions and location of such properties;
 - ii) Resolutions passed at properly constituted meetings of the Trustees;
 - iii) Notices for meetings (special or general) of the Trustees and/or members;
 - iv) Details regarding Proxy appointments at meetings (special or general) since such appointments affect decisions
- and therefore, all members directly or indirectly;

“private body” means—

- (a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
- (b) a partnership which carries or has carried on any trade, business or profession; or
- (c) any former or existing juristic person, but excludes a public body;

“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, organization, 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 (PAIA), 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: I. Writing on 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 another 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; and c) Regardless of when it came into

existence;

“Regulator”: – means the Information Regulator established in terms of Section 39 of the POPIA;

“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;

“restriction”: means to withhold from circulation, use or publication any personal information that forms part of a filing

system, but not to delete or destroy such information;

“Special personal information”: means personal information as referred to in Section 26 of the POPIA which includes

Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, color, sexual

3

orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the

person;

“This Act”: means the Protection of Personal Information Act, No. 4 of 2013.

“Unique identifier”: means any identifier that is assigned to a data subject and is used by a responsible party for the purposes

of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2. INTRODUCTION

The PVHOA is an Association constituted of all owners of property, both freehold and sectional title, within the development

known as Klapmuts.

The PVHOA is managed by the elected Trustees who manage and control the business and affairs of the PVHOA, who determine

what constitutes appropriate standards for residential living, maintenance, repairs, additions and improvements of all

properties in Klapmuts and who may make, enter into and carry out contracts or agreements for any of the purposes of the

PVHOA contained in its Constitution and Resolved by the Trustees from time to time, who may employ and pay agents, servants

and any other service providers, sue and defend actions in the name of the PVHOA and who may appoint legal representatives

for this purpose and exercise the power conferred upon them in terms of the Constitution of the PVHOA.

Since all owners of all properties within Klapmuts are members of the PVHOA, it is inevitable that the PVHOA will collect, process

and in certain instances, share their information in performing its functions.

In performing its business operations most of the PVHOA's communications are done electronically via the internet and on

email. In recognizing the international risk of data breach and also to ensure that lawful conditions exist surrounding its data

subject's information, the PVHOA accepts that all its South African based data subjects' Constitutional Right to Privacy is of

utmost importance. The PVHOA further accepts that its data subjects based in other parts of the world are entitled to equal

rights to privacy in terms of Regulations applicable to such data subjects in the countries in which they are based. As such,

PVHOA is committed to comply with South Africa's POPIA. PVHOA is further committed to the education of its data subjects in

respect of their rights to privacy and will make all operational amendments necessary.

3. OBJECTIVE

The objective of this Policy is to ensure adherence to the provisions within POPIA together with its Regulations aimed at

protecting all the PVHOA's data subjects from harm by protecting their personal information, to ensure that data subjects'

Consent is obtained as provided for in POPIA, to ensure that data subjects' information is not unlawfully shared with third

parties unless Consent for such sharing is obtained, to stop identity fraud and generally to protect privacy. This Policy

constitutes the EXTERNAL SET OF INFORMATION PRIVACY RULES and sets out the standard for suitable protection of personal

information as required by POPIA.

4. POPIA CORE PRINCIPLES

In its quest to ensure the protection of data subjects' privacy, the PVHOA fully commits as follows:

4.1. To continue developing and maintaining reasonable protective measures against the possibility of risks such as loss,

unauthorized access, destruction, use, alteration or revelation of personal information.

4.2. To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with

international standards, that prescribe the minimum threshold requirements for the lawful processing of personal

information;

4.3. To ensure that the requirements of the POPIA legislation are upheld within the PVHOA. In terms of sections 8, 17 and 18

of POPIA, the PVHOA confirms that it adheres to an approach of transparency of operational procedures that controls

collection and processing of personal information and subscribes to a process of accountability and openness

throughout its operations.

4.4. In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPI, the PVHOA undertakes to collect

personal information in a legal and reasonable way, for a specific reason and only if it is necessary for its operations and

to process the personal information obtained from owners, occupiers, visitors and services suppliers only for the purpose for which it was obtained in the first place.

4

4.5. Processing of personal information obtained from owners, occupiers, visitors and service suppliers will not be

undertaken in an insensitive, derogative discriminatory or wrongful way that can intrude on the privacy of the

particular data subject.

4.6. In terms of the provisions contained within sections 23 to 25 of POPIA, all data subjects of PVHOA will be allowed to

request access to certain personal information and may also request correction or deletion of personal information

within the specifications of the POPIA.

4.7. To not request or process information related to race, religion, medical situation, political preference, trade union

membership, sexual certitude or criminal record unless this is lawfully required and unless the data subject has

expressly consented. The PVHOA will also not process information of children unless the specific consent provisions

contained within POPIA have been complied with.

4.8. In terms of the provisions contained within section 16 of POPIA, the PVHOA is committed that data subjects' information

is recorded and retained accurately.

4.9. To not provide any documentation to a third party or service provider without the express consent of the data subject

except where it is necessary for the proper execution of the service as expected by the data subject.

4.10. To keep effective record of personal information and undertakes not to retain information for a period longer than

required.

4.11. In terms of sections 19 to 22 of POPIA, the PVHOA will secure the integrity and confidentiality of personal information in

its possession. PVHOA will provide the necessary security of data and keep it in accordance with prescribed legislation.

5. CONSENT

As provided for in the PVHOA Constitution, owners of properties within the ambit of the PVHOA are obliged to become members

of the PVHOA upon taking transfer of their properties. Membership forms are completed by such owners in which they

complete their requested personal information and supply their Consent to the PVHOA in order to process such information

When data subjects' information is collected, processed or shared by PVHOA for any other reason than the original reason of it

being collected, the specific Consent for such purpose must be obtained from the data subject. In the event that UNIQUE

IDENTIFIERS as defined in section 57 of POPIA are processed by the PVHOA, PRIOR APPROVAL of the Information Regulator will

be obtained in terms of the provisions contained in section 58 of POPIA, before the PVHOA continues with the processing of

such unique identifiers.

If SPECIAL PERSONAL INFORMATION is collected, processed and stored for any reason from any of PVHOA's data subjects,

specific Consent for such collection must first be obtained

The prohibition on collection and processing of special personal information does not apply if: -

5.1. Processing is carried out with the consent of the data subject;

5.2. Processing is necessary for the establishment, exercise or defense of a right or obligation in law;

5.3. Processing is for historical, statistical or research purposes.

PVHOA has amended its standard documentation with references to the Act and will obtain all clients' general Consent in each

transaction.

6. COLLECTION, PROCESSING AND SHARING OF INFORMATION

As mentioned before, the PVHOA collects, processes and where lawful shares personal information from its data subjects for a

variety of reasons and in a variety of ways. The most pertinent reason for data collection and processing results from the

compulsory membership of each owner within Klapmuts to the PVHOA and the need therefore of the PVHOA to continuously

communicate with the owners, their tenants, their visitors and the PVHOA service providers.

In addition to POPIA, various South African laws apply to the collection and processing of information by PVHOA including but

not limited to:

☐ The Community Schemes Ombud Services Act 9 of 2011 read together with Regulations and Directives as amended

from time to time in terms of which several statutory obligations are set out on the part of the PVHOA;

☐ The Electronic Communications Act 36 of 2005

5

The primary way of collection and processing of personal information is electronically. By submitting personal and special

personal information details to PVHOA, all data subjects acknowledge the terms of this Policy.

6.1. Personal information collected by PVHOA will be collected directly from the data subject, unless –

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

6.1.2. The data subject or a competent person;

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

6.1.4. Collection of the information from another source is necessary -

6.1.4.1. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection,

investigation, prosecution and punishment of offences;

6.1.4.2. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

6.1.4.3. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

6.1.4.4. In the interest of national security;

6.1.4.5. To maintain the legitimate interests of PVHOA or of a third party to whom the information is supplied;

6.1.4.6. Compliance would prejudice a lawful purpose of the collection;

6.1.4.7. Compliance is not reasonably practicable in the circumstances of the particular case.

6.1.5. Personal information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of

PVHOA;

6.2. Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.

6.3. PVHOA will take reasonably practicable steps to ensure that the personal information is complete, accurate, not

misleading and updated where necessary, having regard to the purpose for which the personal information is collected

and further processed.

6.4. Where personal information is collected from a data subject directly, the PVHOA will take reasonably practicable steps to

ensure that the data subject is aware of: -

6.4.1. The nature of the information being collected and where the information is not collected from the data subject, the

source from which it is collected;

6.4.2. The name and address of PVHOA;

6.4.3. The purpose for which the information is being collected;

6.4.4. Whether or not the supply of the information by the data subject is voluntary or mandatory;

6.4.5. The consequences of failure to provide the information;

6.4.6. Any particular law authorizing or requiring the collection of the information.

7. STORAGE OF INFORMATION

The PVHOA acknowledges the risks facing data subjects with the storage of personal and special personal information on the

PVHOA's software systems as well as filing copies of the physical information sheets containing personal information physically

in an office. To ensure that its best attempts are made to minimize data subjects from suffering loss of personal information,

misuse or unauthorized alteration of information, unauthorized access or disclosure of personal information generally, it will:

7.1. Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and

confidentiality of your information.

7.2. Constantly monitor the latest internet developments to ensure that the systems evolve as required.

PVHOA tests its

systems regularly to ensure that our security mechanisms are up to date.

7.3. Continue to review its internal policies and third-party agreements where necessary to ensure that these are also

complying with the POPIA and Regulations in line with PVHOA's Policy rules.

8. DISPOSAL OF DATA SUBJECTS' INFORMATION

The PVHOA is responsible to ensure that necessary records and documents of their data subjects are adequately protected and

maintained to ensure that records that are no longer needed or if no value are disposed of at the proper time or on request by

the data subject.

In the event that a data subject wishes to request a correction or deletion of their personal information from the PVHOA

database, he/she will complete the FORM 2 hereto attached and submit same to the Information Officer of the PVHOA.

These rules apply to all documents which are collected, processed or stored by the PVHOA and include but are not limited to

documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

Secure disposal maintains data security and supports compliance with this PVHOA policy. The PVHOA acknowledges that

electronic devices and media can hold vast amounts of information, some of which can linger indefinitely.

6

8.1. Under no circumstances will paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or

confidential information be simply binned or deposited in refuse tips.

8.2. The PVHOA undertakes to ensure that all electrical waste, electronic equipment and data on disk drives be physically

removed and destroyed in such a way that the data will by no means be able to be virtually retrievable.

8.3. The PVHOA will ensure that all paper documents that should be disposed of, be shredded locally and then be recycled.

8.4. In the event that a third party is used for data destruction purposes, the Information Officer will ensure that such third

party will also comply with this policy and any other applicable legislation.

8.5. The PVHOA may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation,

audits, government investigations or similar proceedings. The PVHOA undertakes to notify employees of applicable

documents where the destruction has been suspended to which they have access to.

8.6. In the event that a document and/or information is no longer required to be stored in accordance with this policy and

relevant legislation, it should be deleted and destroyed.

8.7. The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a

document and/or information.

9. INTERNET AND CYBER TECHNOLOGY

9.1. Acceptable use of the PVHOA's Internet Facilities & standard Anti-Virus rules

The repercussions of misuse of the PVHOA systems can be severe. Potential damage includes, but is not limited to, malware

infection (e.g., computer viruses), legal and financial penalties for data leakage and lost productivity resulting from network

downtime.

In order to ensure that the PVHOA's IT systems are not misused, everyone who uses or has access to the PVHOA's systems will

have received training and internal guidelines in order to meet the following five high-level IT Security requirements:

9.1.1. That information will be protected against any unauthorized access as far as possible;

9.1.2. That confidentiality of information will be assured as far as possible;

9.1.3. That integrity of information will be preserved as far as possible;

9.1.4. That availability of information for business processes will be maintained;

9.1.5. That compliance with applicable laws and regulations to which PVHOA is subject will be ensured by the Information

Officer as far as possible.

Every user of PVHOA's IT systems will have received training in respect of the IT Security requirements and will be responsible

for exercising good judgment regarding reasonable personal use.

9.2. IT Access Control

The PVHOA undertakes to ensure that logging into the IT system and software packages is password controlled and shall

exercise all caution in allowing unauthorized access to the password. It is a further undertaking that the password/s shall be

reviewable from time to time but in particular where GOOGLE based products are used and linked (such as Facebook,

WhatsApp and GMAIL based domains).

9.3. PVHOA's Email Rules

The PVHOA acknowledges that most of its communications are conducted via email and instant messaging (IM). Given that

email and IM may contain extremely sensitive and confidential information, the information involved must be appropriately

protected. In addition, email and IM are potentially sources of spam, social engineering attacks and malware, so the PVHOA

must be protected as completely as possible from these threats. The misuse of email and IM can post many legal, privacy and

security risks, so it is important for users to be aware of the appropriate use of electronic communications.

It is of use to note that all users of PVHOA's email system are prohibited from using email to:

9.3.1. Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race,

religion, color, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

9.3.2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.

9.3.3. Spread gossip, rumors, or innuendos about employees, clients, suppliers, or other outside parties.

9.3.4. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.

9.3.5. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or

adult-oriented language.

7

9.3.6. Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass

PVHOA negatively impact productivity, or harm morale.

The purpose of the Email and IM rules is to ensure that information sent or received via these PVHOA's IT systems is

appropriately protected, that these systems do not introduce undue security risks to PVHOA and that users are made aware of

what PVHOA deems as acceptable and unacceptable use of its email and IM.

9.4. PVHOA's Rules related to handheld devices

Many users do not recognize that mobile devices represent a threat to IT and data security. As a result, they often do not

apply the same level of security and data protection as they would on other devices such as desktop or laptop computers. This

policy outlines PVHOA's requirements for safeguarding the physical and data security of mobile devices such as smartphones,

tablets, and other mobile devices that PC's and Notebooks.

9.4.1. PVHOA's users of handheld devices are expected to diligently protect their devices from loss and disclosure of

private information belonging to or maintained by the PVHOA.

9.4.2. Before connecting a mobile handheld device to the network at the PVHOA, users are expected to ensure it is on

the list of approved devices issued by the IT support where ever necessary.

9.4.3. In the event of a security incident or if suspicion exists that the security of the PVHOA's systems has been

breached, PVHOA shall be obliged to notify the IT support immediately especially when a mobile device may have

been lost or stolen.

9.5. Anti-virus rules

9.5.1. Management of PVHOA is responsible for creating procedures that ensure anti-virus software is run at regular

intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute

malicious programs into PVHOA's programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

9.5.2. It is worth noting that users are discouraged from attempting to remove viruses themselves. If a virus infection is

detected, users are expected to disconnect from PVHOA's networks, stop using the infected computer

immediately and notify the IT support as well as the Information Officer and/or Deputy Information Officer who

will take the necessary steps set out hereunder.

9.5.3. It is further worth noting that PVHOA's users are encouraged to be cautious of e-mail attachments from an

unknown source as viruses is often hidden in attachments. If a virus is suspected the attachment must not be

opened or forwarded and must be deleted immediately.

9.6. Physical access control

9.6.1. All of PVHOA's premises that include computers and other types of information technology resources will be

safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical

threats. This includes but is not limited to; security doors, key entry areas, external doors that are locked from

closing until opening of the building, locked and/or barred windows, security cameras, registration of visitors at

entrances, security guards, and fire protection.

9.7. Usage Data

Usage Data Usage Data is collected automatically when using the internet services of PVHOA. Usage Data may include

information such as data subjects' device's internet protocol address (e.g., IP address), browser type, browser version, details

of the pages of PVHOA'S website that are visited by data subjects, the time and date of the website visit, the time spent on

those pages, unique device identifiers and other diagnostic data. When data subjects access the website services of PVHOA by

or through a mobile device, PVHOA may collect certain information automatically, including, but not limited to, the type of

mobile device used by the data subject, unique ID, the IP address of the mobile device, the mobile operating system, the type

of mobile Internet browser used, unique device identifiers and other diagnostic data. The PVHOA may also collect information

that the user's browser sends whenever PVHOA's website is visited.

9.8. Tracking Technologies and Cookies

Cookies and similar tracking technologies are used to track the activity on PVHOA's website and store certain information.

Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyze the

efficiency of the website. The technologies which may be used to track may include:

9.8.1. Cookies or Browser Cookies. A cookie is a small file which may be placed on a data subject's device. Data subjects can

instruct their browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if this function of

PVHOA's website is not accepted, data subjects may not be able to use some parts of the website. Unless the browser

settings have been adjusted PHOA's website may use Cookies.

9.8.2. Flash Cookies. Certain features of the website may use local stored objects (or Flash Cookies) to collect and store

information about data subjects' preferences or activity on the website. Flash Cookies are not managed by the same

browser settings as those used for Browser Cookies. For more information on how Flash Cookies can be deleted the

following process can be followed: "Where can I change the settings for disabling, or deleting local shared objects?"

available at <https://helpx.adobe.com/flashplayer/kb/disable-local-shared-objects>;

9.8.3. Web Beacons. Certain sections of the website and emails may contain small electronic files known as web beacons

(Also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit PVHOA for example, to count users who have

visited those pages or opened an email and for other related website statistics (for example, recording the popularity

of a certain section and verifying system and server integrity).

9.8.4. Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on data subjects' personal computer or

mobile device even when offline, while Session Cookies are deleted as soon as data subjects' web browsers are

closed.

10. THIRD PARTY OPERATORS

The PVHOA recognizes that, in fulfilling its service offering to its data subjects as stipulated in the Constitution and in order to

operate efficiently, it is necessary at times to share data subjects' personal and special personal information with third parties

for specific reasons related to PVHOA's service delivery. As referenced in clauses 5 and 6 above, the PVHOA will obtain the

necessary and specific Consent where required from the particular data subject.

The PVHOA shall moreover and where possible enter into an OPERATORS' AGREEMENT with the relevant third party with which

PVHOA shares data subjects' information in order to ensure that the third-party operator treats the personal information of

PVHOA's data subjects responsibly and in accordance with the provisions contained in the Act and Regulations thereto. PVHOA

shall, where possible request copies of the third-party operators' POPIA Policy, rules, internet rules and details of the third

party's Information Officer.

11. BANKING DETAILS

It is a known fact that any role player in the property industry faced an increased risk of email interceptions and in particular

the interception of banking details for purposes of payment of funds or levies. The PVHOA's data subjects are open to large

amounts of damages and losses if emails are intercepted and banking details are fraudulently amended without the data

subject's knowledge.

The PVHOA has implemented clear ALERTS within all its correspondences (emails and physical letters) warning data subjects of

the risks of email hacking and interceptions. In the event that banking details are sent to data subjects or received from data

subjects for purposes of payment, the banking details will be confirmed with a telephone call and a follow up WhatsApp were

ever possible.

12. INFORMATION OFFICER

Since the PVHOA is an association, it will elect the Information Officer and Deputy Information Officer from time to time and a

Resolution will be passed in respect thereto. The details of these elected Officers are available at the PVHOA offices:

Office number: 0878213655

12.1. The general responsibilities of PVHOA's Information Officer and Deputy Information Officer where delegated include

the following:

12.1.1. The encouragement of compliance, by PVHOA, with the conditions for the lawful processing of personal information;

12.1.2. Managing requests made to PVHOA pursuant to POPIA;

12.1.3. Working with the Regulator in relation to investigations conducted pursuant to prior authorization required to

process certain information of POPIA in relation to the business.

12.1.4. Continuously perform data backups, store at least weekly backup offsite, and test those backups regularly for data

integrity and reliability.

12.1.5. Review policy rules regularly, document the results, and update the policy as needed.

9

12.1.6. Continuously update information security policies and network diagrams.

12.1.7. Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.

12.1.8. Perform continuous computer vulnerability assessments and audits

12.2. The data breach responsibilities of PVHOA's Information Officer and Deputy Information Officer where delegated

include the following:

12.2.1. Ascertain whether personal data was breached;

12.2.2. Assess the scope and impact by referring to the following:

12.2.2.1. Estimated number of data subjects whose personal data was possibly breached

12.2.2.2. Determine the possible types of personal data that were breached

12.2.2.3. List security measures that were already in place to prevent the breach from happening.

12.2.3. Once the risk of the breach is determined, the following parties need to be notified within 72 hours after being

discovered:

12.2.3.1. The Information Regulator

12.2.3.2. Communication should include the following:

☐ Contact details of Information Officer

☐ Details of the breach,

☐ Likely impact,

☐ Actions already in place, and those being initiated to minimize the impact of the data breach.

☐ Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.

12.2.4. Review and monitor

12.2.4.1. Once the personal data breach has been contained, PVHOA will conduct a review of existing measures in

place, and explore the possible ways in which these measures can be strengthened to prevent a similar breach from reoccurring.

12.2.4.2. All such identified measures should be monitored to ensure that the measures are satisfactorily

implemented.

13. AVAILABILITY AND REVISION

A link to this Policy is made available at the offices of the PVHOA.

This policy will continually be updated to comply with legislation, thereby ensuring that personal information will be secure.

10

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.

4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 2]

Note:

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

A DETAILS OF DATA SUBJECT

Name(s) and

surname/ registered

name of data subject:

Unique Identifier/

Identity Number

Residential, postal or

business address:

Code ()

Contact number(s):

Fax number/E-mail

address:

B DETAILS OF RESPONSIBLE PARTY

Name(s) and surname/

Registered name of

responsible party:

Residential, postal or

business address:

Code ()

Contact number(s):

Fax number/ E-mail

address:

C

REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please

provide detailed reasons for the objection)

Signed at this day of20.....

..... Signature of data subject/designated person

11

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF
RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL
INFORMATION ACT, 2013 (ACT NO.

4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. Affidavits or other documentary evidence as applicable in support of the request may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

Mark the appropriate box with an "x".

Request for:

Correction or deletion of the personal information about the data subject which is in possession or
under the control of the responsible party.

Destroying or deletion of a record of personal information about the data subject which is in possession or
under the control of the responsible party and who is no longer authorized to retain the record of

information.

A DETAILS OF THE DATA SUBJECT

Name(s)and surname/ registered name of data
subject:

Unique identifier/ Identity Number:

Residential, postal or business address:

Code ()

Contact number(s):

Fax number/E-mail address:

B DETAILS OF RESPONSIBLE PARTY

Name(s)and surname/ registered name of
responsible party:

Residential, postal or business address:

Code ()

Contact number(s):

Fax number/ E-mail

address:

C INFORMATION TO BE CORRECTED/DELETED/ DESTRACTED/ DESTROYED

12

D

REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT
THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER
THE CONTROL OF THE RESPONSIBLE PARTY; and or

REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION
ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE
PARTY IS NO LONGER AUTHORISED TO RETAIN.

(Please provide detailed reasons for the request)

Signed at this day of 20.....

.....

Signature of data subject/ designated person

FORM 3

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION
FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL
INFORMATION ACT, 2013 (ACT NO.

4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 6]

TO:

FROM: (Name of data subject)

Contact number(s):

Fax number:

E-mail address:

(Name, address and contact details of responsible party)

Full names and designation of person signing on behalf of responsible party:

.....

Signature of designated person

Date:

PART B

I, (full names of data subject) hereby:

Give my consent.

To receive direct marketing of goods or services to be marketed by means of electronic communication.

SPECIFY GOODS or SERVICES:

SPECIFY METHOD OF COMMUNICATION: FAX:

E - MAIL:

SMS:

OTHERS – SPECIFY:

Signed at this day of20.....

.....Signature of data subject