

MANDE PROPERTIES CC

2004/127508/23



"Registered with the PPRA"

COMPLIANCE FRAMEWORK

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT OF 2013

PAGE	CONTENTS
2	Privacy Notice
2	Contact Details
2	Introduction
3	Specific Words / Phrases
3	Information officer
4	Processing personal information and protecting the right of our clients
6	What personal information do we collect?
6	Who might we share your personal information with?
6	Transborder Information Flows
7	Circumstances requiring prior authorisation
7	Special Personal Information
7	Processing of Personal Information of Children
7	Direct Marketing
8	Data Breach Notification
8	Contravention Of POPIA
8	The SA Information Regulator
9	Forms and clauses

INFORMATION OFFICER: PENELOPE SHELLEY MANDE

PRIVACY NOTICE

We respect and protect the privacy of all individuals (both natural and juristic, such as companies and close corporations) whose personal information we collect, regardless of the form and medium. This includes our guests, owners, clients, consultants, power partners and service providers. These privacy notices explain our personal information handling practices for that particular purpose or service. It explains who we collect personal information from, with your consent, what information we collect, how we use it, how you can access it, and with whom it may be shared. It also explains why we collect it, how we will store it, and how we will dispose of it. All of this is covered under the Protection of Personal Information Act (POPI Act).

Mande Properties CC

CONTACT DETAILS:

Physical Main Business address:	104 Wavecrest, 305 Beach Road, Seapoint 8005 Cape Town. Western Cape. Sout Africa
Telephone number/s:	021 - 4399880
E-mail address:	pennym@eastcoast.co.za

INTRODUCTION

The Protection of Personal Information Act (POPI) is intended to balance the scales legally by protecting a person's constitutional rights to privacy (which requires our personal information to be protected). The needs of businesses to have access to and to process (work with) a person's specific personal information to perform the task they are set out to do.

This Compliance Framework outlines the framework for our company's compliance with the POPI Act, focusing on tasks that must be performed in the property sector.

SPECIFIC WORDS/PHRASES *(used in the act) will be used in this document to make it more straightforward.*

Data Subject

The person to whom the personal information relates. It is a living, identifiable natural person or An existing juristic person. – companies, cc, trust, public entity (Mun), e.g., Owner/Guest/Seller / Buyer

Responsible party

Is the person/s or company who is responsible for the processing of personal information? Whether it is to collect, keep it safe, disseminate or destroy it to perform a specific task. e.g., Principal / Property Practitioner, Business / Trustees / Body corporate.

Operator

Is the party processing personal information on behalf of the responsible party? The accountable party retains accountability., The Property Practitioner Business personnel who is processing the data. Or a third party if the processing is outsourced, e.g., an IT company.

Processing

Where reference is made to the "processing" of personal information, this will include any activity in which the information is worked with, from the time that the data is collected, shared, and kept, up to the time that the information is destroyed, regardless of whether the information is a hard copy, or in electronic format.

INFORMATION OFFICER

Our Information Officer is: Penelope Shelley Mande
(Name and contact details) 104 Wavecrest, 305 Beach Road, Sea Point, 8005. Cape Town.
Western Cape. South Africa
021 - 4399880
pennym@eastcoast.co.za

The Information Officer must:

- Develop the compliance framework and ensure it is implemented in line with the eight (8) conditions (*see below*) for the lawful processing of personal information.
- Do a personal information impact assessment to ensure adequate measures and standards. (*What Personal information do we hold, where do we hold it and for what purpose, and is it necessary*)
- Review the forms our Property Practitioner Business uses to gather information (*for example, reservation documents and other relevant documents*) to determine whether it is necessary to request all the information outlined in those forms and whether the consent clause is included.
- He/she must develop *this* framework and monitor, maintain it, and make it available as prescribed in sections 14 and 51 of the Act.
- Internal measures (*7 forms*) are developed together with adequate systems to process requests for information from data subjects or access thereto, free of charge.
- Ensure internal training/awareness sessions are conducted regarding the provisions of the POPI Act and discuss it weekly in the office meeting.
- Working with the Regulator concerning any investigations conducted under the relevant provisions of the POPI Act. (*When needed*)

PROCESSING PERSONAL INFORMATION AND PROTECTING THE RIGHTS OF OUR GUESTS:

We undertake to implement, monitor, and maintain the **eight (8) conditions for the lawful processing of personal information**, always to follow the POPI Act and to process personal information while protecting the right to privacy of our guests.

1. Accountability (*Form 6*)

The Principals (*responsible party*) must ensure that the conditions and all the measures set out in the Act are followed through in the office.

The Information Officer (Operator) will be responsible for ensuring compliance within our office. This individual will be held liable for non-compliance in certain day-to-day situations.

2. Processing Limitation (*Forms 1, 2, 5, 7*)

Personal information may only be processed fairly and lawfully and only with the consent of the person whose information it is (*data subject*) and for the purpose for which it was collected.

- ✓ The personal information must be obtained directly from the person (*Data Subject*)
- ✓ The person should be aware that we gather their information and consent to its use.
- ✓ If a third party is being used to collect personal data, the person (*Data Subject*) must consent to this information being shared and used by us first.
- ✓ Only information that is required for the specific purpose for which it is gathered may be stored. (*No more than what is necessary*)

3. Purpose Specific (*Forms 1, 2, 3, 5, 7*)

We limit the amount of personal information collected and processed to only what is necessary for the intended purposes.

- ✓ The specific purpose must be documented and adhered to.
- ✓ Data Subject has the right to know what information we have and for what purpose it was gathered.
- ✓ We will need to be able to link all personal information collected to legitimate reasons for its collection.
- ✓ Personal information may only be used for the specific purpose for which it was gathered, and thereafter it must be destroyed.
- ✓ We will be required to account for what information we hold, for what purpose it was gathered and the date that that information must be destroyed.
- ✓ We will destroy Personal Information in a manner that prevents its reconstruction after we are no longer authorised to retain such records.

4. Further Processing Limitation (Forms 1, 2, 3, 5, 7)

Personal information may not be processed for a secondary purpose unless that processing is compatible with the original purpose.

- ✓ We retain personal information only for as long as needed, or longer if required by law.
- ✓ If we retain your personal information for budget or statistical purposes, we ensure that the personal information cannot be used further. *(It will be de-personalised)*
- ✓ Before we use existing personal information for any other purpose, other than what the information was gathered for, consent will be required from the Data Subject again.
- ✓ If he/she refuses, processing will stop.
- ✓ When gathering information, we will inform the Data Subject of the purpose for which the information will be used and the period for which we will retain that information.

5. Information Quality (Forms 1, 3)

While in our possession, with the assistance of the data subject, we strive to maintain the accuracy of personal information.

- ✓ We will obtain information directly from the data source whenever possible to ensure accuracy.
- ✓ When advising Data Subjects of the information we hold and for what purpose we have it, they will be given details of how to check, update their information or withdraw consent.

6. Openness (Form 1, 2, 5, 7)

The data subject whose information we are collecting will be made aware that we are collecting such personal information for what purpose the information will be used, and her/ his rights. *(Even if this is a public record or he/she consented to collection from a third party)*

- ✓ We will gather personal information from Data Subjects which is noted on our client documents and signed by the clients. .
- ✓ The Data Subject will be informed of how the data will be used at the time the information is gathered.
- ✓ The Data Subjects will be given a letter with the details of the principal *(responsible person)* in our Property Practitioner Business and the Information Regulator's contact details.
- ✓ The Data Subject will be advised of his/her rights to complain to the Information Regulator if misuse is suspected. Noted on all clients forms which is signed by the client
- ✓ The Data Subject will always be advised of his/her rights to access his/her information and to object to the processing of said information. (noted on the client documents which the client signs)

7. Security Safeguards (Form 6)

We restrict, secure, and control all our information against unauthorised access, interference, modification, damage, loss, or destruction, whether physical or electronic.

- ✓ We will conduct safety and security risk assessments periodically to ensure compliance with requirements. These assessments will be discussed at our monthly staff meeting, allowing all personnel to provide input.
- ✓ Our staff must be informed and trained to comply with the POPI Act, and this training must be ongoing and up to date.
- ✓ We do everything we can to prevent personal information from falling into unauthorised hands.
- ✓ Our business premises, where records are kept, must remain protected by access control and burglar alarms which is operated through the Concierge services with all personal information locked up safely in cupboards inside a protected area with another locked entrance
- ✓ All our laptops, phones and computer networks are protected by passwords which we change regularly.
- ✓ We utilise Microsoft Business Outlook 365, with multi factor authorisation linked to the cell phones which adheres to industry-standard security safeguards and complies with the General Data Protection Regulation (GDPR), a key requirement in the European Union as well as DMARC for anti spoofing of emails, and Mimecast to stop interception of emails, and Black Fog and DNS filters as well as encrypted hard drives. We have firewalls and use Sentinel 1 anti virus on our laptops.
- ✓ We are a small, husband and wife team Property Practitioner Business, who is doing holiday letting and sales. We do not have any employees. Only we, as the owners, have access to personal information and what information will be accessed.
- ✓ Personal information can only be accessed or modified by us, the owners, with the *passwords* authorising us to do so.
- ✓ If there were a data breach, we would determine the source, neutralise it and prevent the recurrence of such a data breach.
- ✓ When we utilise an external operator, we (the responsible party) will, under a written contract between our Property Practitioner Business and the operator, ensure that the operator establishes and maintains the required security measures.
- ✓ The operator must advise immediately if there is the possibility that personal data has been accessed or acquired by any unauthorised person.
- ✓ The Data Subject will be advised via e-mail or in writing immediately if it is suspected that unauthorised persons have accessed their personal information. Sufficient information will be provided to enable the Data Subject to take measures to safeguard themselves against potential consequences of the security compromise.
- ✓ The Information Regulator will be informed in the event of a security breach where personal information could be compromised. The Responsible Person must ensure this process is followed.

8. Data Subject Participation *(Forms 2, 3, 4)*

Data subjects may request whether their personal information is held, as well as the correction and/or deletion of any personal information held about them.

- ✓ Data Subjects may request information from us on whether we are holding their personal information.
- ✓ This request will not be declined, and we will not incur any charges for it.
- ✓ The Data Subject has the right to correct the personal information that we hold.
- ✓ They also have the right to withdraw consent at any time.

WHAT PERSONAL INFORMATION DO WE COLLECT?

We only collect the minimum amount of information that is relevant to the purpose. If you interact with us online, the personal information we collect depends on whether you visit our website or use our services. When you visit our website, your browser automatically transmits some data, including your browsing times, the data transmitted, and your IP address.

- ✓ If you use our services, personal information is required to fulfil the requirements of that service.
- ✓ We typically collect only the names and contact details of guests and owners, as well as their needs and requirements, when assisting them in letting timeshare units or weeks in the resort.

Generally, we collect the following personal information to complete contracts. If there is any specific personal information to collect, we will indicate as such at the time of collection.

- ✓ Name, surname, and birth name
- ✓ Identification Number/s
- ✓ Married/single status.
- ✓ E-mail address
- ✓ Physical/postal address/ERF number / complex details
- ✓ Telephone number/s
- ✓ Financial & banking details (for deposit refunds to guests or payments to owners)

WHO MIGHT WE SHARE YOUR PERSONAL INFORMATION WITH?

To maintain and improve our services, your personal information may need to be shared with or disclosed to our service providers:

- ✓ homeowner association,
- ✓ trustees,
- ✓ owners
- ✓ sellers

TRANSBORDER INFORMATION FLOWS

Property Practitioner Business is unlikely to process personal information to be sent transborder, but if there is an international component to the work which we are doing for you, and if we are required to share your personal information with an overseas recipient, you are entitled to ask us how your data will be protected in this foreign country, and we will endeavour to assist you.

CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

A Property Practitioner Business is unlikely to process personal information under circumstances requiring authorisation from the regulator; however, if necessary, guidance from the Information Officer will be sought regarding POPIA.

SPECIAL PERSONAL INFORMATION

While we recognise that protecting all personal information is vital in gaining and maintaining your trust, special personal information is often afforded a higher level of protection. A Property Practitioner Business is unlikely to process special personal information; however, if necessary, guidance from the IEASA compliance consultant will be sought regarding POPIA.

THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

A Property Practitioner Business is unlikely to process any personal information of children, except possibly in cases involving young students or where adults place a property in a child's name.

To all students. (Student accommodation)

This is an essential notice that we must share with you and any one of your parents or legal guardians if you are under the age of eighteen. To use our services, we require personal information about you, however only through your parent or legal guardian looking after the student booking.. For example, your name, your email address, and your phone number. It might be so that we cannot use your information unless your parent agrees. We only deal with the parent for student accommodation and this parent is responsible for the student and the booking.

We only require a copy of ID of the student checking into the resort for their booking, from the parent for the capturing of the student on the resort system which is obtained and given to us by the parent. We do not deal with the student. The responsible parent is contacted by the resort management if needed during the student stay in the resort.

To parents / legal guardians. We do not deal with the children or students. Only through the parents and legal guardians of the children or students, who act on their behalf and forward on relevant documents if required by us, on behalf of the children or students, which is normally when we rent or sell on behalf of an owner and the ownership is in the children's name. For this, we are required by law to obtain the consent of a parent or legal guardian and we only deal with the parent or legal guardians.

DIRECT MARKETING *(Form 4)*

Where we, as a Property Practitioner Business, want to contact a person for the first time with marketing communication which was not requested *(unsolicited)*,

- ✓ the Property Practitioner Business must obtain consent before any marketing to individuals.
- ✓ The Property Practitioner Business may approach someone for direct marketing consent once only,
- ✓ and only if they have not withheld consent previously.

We may only conduct direct marketing *(using any form of communication)* **to previous guests if:**

- ✓ The potential guest was given the option to opt out of receiving direct marketing materials from us at the time their personal information was collected.
- ✓ and they did not object at the time.
- ✓ or at any other time, after receiving any such direct marketing communications from us.

We may only approach guests using their personal information,

- ✓ if we have obtained their consent to use their personal information in the context of providing services associated with marketing to them,
- ✓ and we may then only market Property Practitioner Business services to them.

We will stick to permitted contact times.

The prohibited times for marketing are:

- ✓ Sundays or public holidays.
- ✓ Saturdays before 09h00 and after 13h00.
- ✓ and all other days between the hours of 20h00 and 08h00 the following day

We are aware that we are not allowed to use lists purchased from a lead generation business if:

We purchased it from a lead generation business without obtaining confirmation from the list's provider that the records had been obtained and stored in a manner compliant with the Protection of Personal Information Act (POPIA).

The “unsubscribe” option must be on our marketing emails.

All electronic direct marketing communications must contain an “unsubscribe” option.

Similarly, physical postboxes contain a direction that says, “no junk mail”.

We will make use of a bulk email and SMS software that keeps track of “opt-in” and “opt-out” information and automatically includes an automatic “opt-out” on each message sent to existing guests and others that have “opted-in” to receive marketing and to ask people directly if they may be added to the Property Practitioner Business's database.

We will include the sender's details in all emails.

An address or other contact details to which the recipient may reply/send a request that such communications cease.

DATA BREACH NOTIFICATION

Where there are reasonable grounds to believe that a data subject's personal information has been accessed or acquired by an unauthorised person, the Property Practitioner Business *(as responsible party)*, or any third-party, processing personal information, on instruction from the

Property Practitioner Business (*the operator*), must notify the Information Regulator and the data subject in writing as soon as possible.

THE INFORMATION REGULATOR IS RESPONSIBLE FOR THE INVESTIGATION AND ENFORCEMENT OF POPIA.

A person contravenes the provisions of POPIA if he/she it:

- hinders, obstructs, or unlawfully influences the Information Regulator.
- fails to comply with an information or enforcement notice.
- gives false evidence before the Information Regulator on any matter after having been sworn in or having made an affirmation.
- contravenes the conditions.

Knowingly or recklessly, without the consent of the responsible party, obtains, discloses, or procures the disclosure, sells, or offers to sell details of a data subject to another person; and will be guilty of an offence.

CONTRAVENTION OF POPI Act.

This could result in far-reaching sanctions, including the imposition of fines of up to R10 million, imprisonment for a period of 12 months to 10 years and/or damages claimed by the data subject.

THE SA INFORMATION REGULATOR

You have the right to complain to the SA Information Regulator.

The Information Regulator (South Africa)
PO Box 31533, Braamfontein, Johannesburg, 2017
Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg
The Information Regulator (South Africa)

From 1 August 2025, the SA Information Regulator Address: P.O. Box 31533, Braamfontein, Johannesburg, 2017 **or** Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2001

POPIAComplaints@info regulator.org.za

SCHEDULE OF CLAUSES AND FORMS

1. Form 1 CONSENT TO PROCESS (USE) PERSONAL INFORMATION **On all documents which the client signs.**
2. Form 2 OBJECTION TO PROCESS (USE) PERSONAL INFORMATION- **this can be inserted on the documents when the client signs**
3. Form 3 REQUEST TO CORRECT OR DELETE PERSONAL INFORMATION – **noted on the client documents**
4. Form 4a CONSENT TO DIRECT MARKETING- **noted on the client documents which are signed by the client**
5. Form 4b REFUSAL OF DIRECT MARKETING- **noted on the client documents**
6. Form 5 INTRODUCTORY LETTER TO GUEST RE POPIA – **All details on the client forms**
7. Form 6 EMPLOYEE COMPLIANCE WITH POPIA N/A **no employees**
8. Form 7 SHOW HOUSE ATTENDANCE REGISTER **N/A**
9. CLAUSES FOR MANDATES AND CONTRACTS (English)