COMPLIANCE MANUAL

PREPARED IN ACCORDANCE WITH SECTION 51 OF THE PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000, INCORPORATING THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

FOR

ZA PROP ZA (PTY) LTD

Registration number 2024/183941/07

Residential & Commercial Property Sales and Rentals

99 True North Road

Mulbarton

2091

0861 927 767

info@zaprop.co.za

www.zaprop.co.za

Version 1 - 10/06/2025
Version 2 - 05/08/2025

INDEX

1. INTRODUCTION

This manual has been prepared in accordance with Section 51 of the Promotion of Access to Information Act (PAIA) 2 of 2000 and incorporates the Protection of Personal Information Act (POPIA) 4 of 2013.
The Protection of Personal Information Act is intended to balance two competing interests. These are:

- Our individual constitutional rights to privacy (which requires our personal information to be protected); and
- The needs of our society to have access to and to process (work with) our personal information for legitimate purposes, including the purpose of doing business.

This Compliance Manual sets out the framework for our company's compliance with POPI.
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 information is collected, up to the time that the information is destroyed, regardless of whether the information is worked with manually, or by automated systems.

Clients who require guidance in exercising their rights under PAIA are encouraged to contact the Information Regulator:
Website: https://inforegulator.org.gov.za/paia-guidelines
Tel: 010 023 5200
Email: complaints.IR@justice.gov.za

2. CATEGORIES OF RECORDS HELD

Records are grouped into the following categories:

- Employee Personnel Records
- Client Records (Mandates, Sales, Rentals)
- Supplier and Contractor Records
- Internal Company Records (E.G Company Policies and Procedures, Operational Data)
- Statutory Records (E.G Compliance and Governance Documents)
- Financial Records
- Communication Records
- Third-Party Records

3. APPLICABLE LEGISLATION

TheCompanyissubject to various legislation including, but not limited to:

- Promotion of Access to Information Act, 2 of 2000
- Protection of Personal Information Act, 4 of 2013
- Property Practitioners Act, 22 of 2019
- Companies Act, 71 of 2008
- Skills Development Act, 97 of 1998
- Basic Conditions of Employment Act, 75 of 1997
- Employment Equity Act, 55 of 1998
- Unemployment Insurance Act, 63 of 2001
- Income Tax Act, 58 of 1962
- Competition Act, 89 of 1998
- Labour Relations Act, 66 of 1995
- Value Added Tax Act, 89 of 1991
- Occupational Health and Safety Act, 85 of 1993
- Trademarks Act, 194 of 1993
- Compensation for Occupational Injuries & Disease Act, 130 of 1993

4. PURPOSE OF PROCESSING PERSONAL INFORMATION

Personal information is processed for legitimate business purposes such as:

- Employment administration and HR functions
- Client onboarding and service delivery to our clients
- Contract and supplier management
- Legal compliance and reporting
- Internal audits and security measures

5. OUR UNDERTAKING TO OUR CLIENTS

1. We undertake to follow POPI at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of our clients.
2. We undertake to process information only for the purpose for which it is intended, to enable us to do our work, as agreed with our clients.
3. Whenever necessary, we will obtain consent to process personal information.
4. Where we do not seek consent, the processing of our client's personal information will be following a legal obligation placed upon us, or to protect a legitimate interest that requires protection.
5. We will stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.
6. We will collect personal information directly from the client whose information we require, unless:
   - 6.1. the information is of public record, or
   - 6.2. the client consented to the collection of their personal information from another source, or
   - 6.3. the collection of the information from another source does not prejudice the client, or
   - 6.4. the information to be collected is necessary for the maintenance of law and order or national security, or
   - 6.5. the information is being collected to comply with a legal obligation, including an obligation to SARS, or
   - 6.6. the information collected is required for the conduct of proceedings in any court or tribunal, where these proceedings have commenced or are reasonably contemplated; or
   - 6.7. the information is required to maintain our legitimate interests; or
   - 6.8. where requesting consent would prejudice the purpose of the collection of the information; or
   - 6.9. where requesting consent is not reasonably practical in the circumstances.
7. We will advise our clients of the purpose of the collection of the personal information.
8. We will retain records of the personal information we have collected for the minimum period as required by law unless the client has furnished their consent or instructed us to retain the records for a longer period.
9. We will destroy or delete records of the personal information (so as to de-identify the client) as soon as reasonably possible after the time period for which we are entitled to hold the records have expired.
10. We will restrict the processing of personal information:
    - 10.1 where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information.
    - 10.2 where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for the purposes of proof;
    - 10.3 where the client requests that the personal information is not destroyed or deleted, but rather retained; or
    - 10.4 where the client requests that the personal information be transmitted to another automated data processing system.
11. The further processing of personal information will only be undertaken:
    - 11.1 if the requirements of paragraphs 3; 6.1; 6.4; 6.5 or 6.6 above have been met.
    - 11.2 where the further processing is necessary because of a threat to public health or public safety or to the life or health of the client, or a third person;
    - 11.3 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or
    - 11.4 where this is required by the Information Regulator appointed in terms of POPI.

12. We undertake to ensure that the personal information which we collect, and process is complete, accurate, not misleading and up to date.
13. We undertake to retain the physical file, and the electronic data related to the processing of the personal information.
14. We undertake to take special care with our client's bank account details, and we are not entitled to obtain or disclose or procure the disclosure of such banking details unless we have the client's specific consent.
15. **Annexure 1** referred to in **Section 19** below is readily available should same be requested.

6. OUR CLIENT'S RIGHTS

- In cases where the client's consent is required to process their personal information, this consent may be withdrawn.
- In cases where we process personal information without consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the client has the right to object to such processing.
- All clients are entitled to lodge a complaint regarding our application of POPI with the Information Regulator.
- **Annexure 2** referred to in **Section 19**, must be completed by each client when we accept a mandate (sale or rental), offer on a property or when finding a suitable tenant, to obtain the client's consent to process their personal information while we do our work for them, unless this consent has been obtained within another document signed by the client.
- Client's personal information will not be sold.

7. SECURITY SAFEGUARDS

- In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, we implemented the following security safeguards:
  - Our business premises where records are kept protected by access control, burglar alarms and armed response.
  - Archived files are stored behind locked doors and access to these storage facilities are strictly controlled.
  - All laptops on our internal computer network and our servers are protected by passwords which is changed on a regular basis.
  - Our email infrastructure complies with basic industry standard security safeguards.
  - Vulnerability assessments are carried out on our digital infrastructure on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place.
  - We use an internationally recognised security software AVG Antivirus Internet Security as well as Microsoft Office with double factor authentication to protect the data on our local servers and laptops. AVG is set to run in the background and update itself. Our laptops and servers are set to automatically download the latest Microsoft patches which is checked and installed regularly.
  - Our laptops have been upgraded to run on Windows 10 / 11 systems which also has built in anti-virus protection.
  - Our staff have been trained to carry out their duties in compliance with POPI, and this training is ongoing.
  - It is a term of the contract with every staff member that they maintain full confidentiality in respect of all of our clients' affairs, including our clients' personal information.
  - Employment contracts for staff whose duty it is to process a client's personal information, includes an obligation on the staff member (1) to maintain the Company's security measures, and (2) to notify their manager/supervisor immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person. See **Annexure 6** referred to in **Section 19** for an example of the relevant addendum/clause to be used in these contracts.
  - The processing of the personal information of our staff members takes place in accordance with the rules contained in the relevant labour legislation.
  - The digital work profiles and privileges of staff who have left our employ will be properly terminated.
  - The personal information of clients and staff will be destroyed timeously in a manner that de-identifies the person.
- These security safeguards are verified on a regular basis to ensure effective implementation, and these safeguards are continually updated in response to new risks or deficiencies.

8. SECURITY BREACHES

- Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, we will notify the Information Regulator and the relevant client/s, unless we are no longer able to identify the client/s. This notification will take place as soon as reasonably possible.
- Such notification will be given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the client/s be delayed.
- The notification to the client will be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the client:
  - by mail to the client's last known physical or postal address;
  - by email to the client's last known email address;
  - by publication on our website or in the news media; or
  - as directed by the Information Regulator.
- This notification to the client will give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and will include:
  - a description of the possible consequences of the breach;
  - details of the measures that we intend to take or have taken to address the breach;
  - a recommendation of what the client could do to mitigate the adverse effects of the breach; and
  - if known, the identity of the person who may have accessed, or acquired the personal information.

9. CLIENTS REQUESTING RECORDS

To access records, a requester must complete the prescribed PAIA **Form 2. Annexure 12** under **Section 19** and submit it to the Information Officer. Form 2 is available at https://inforegulator.org.za/forms/ or upon request from the Company,

The following is required:

- Full name and contact details of requester
- Description of the record requested
- Form of access required
- Reason the record is required to exercise or protect a right
- Copy of ID or proof of authority if acting on behalf of another person

- **On production of proof of identity, any person is entitled to request that we confirm, free of charge, whether or not we hold any personal information about that person in our records.**
- If we hold such personal information, on request, and upon payment of a fee of R500-00, we will provide the person with the record, or a description of the personal information, including information about the identity of all third parties or categories of third parties who have or have had access to the information. We will do this within a reasonable period of time, in a reasonable manner and in an understandable form.
- A client requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request will be made on the prescribed application form. See **Annexure 4 (POPIA Form 2)** referred to in **Section 19**.
- In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have discretion as to whether or not to do so.
- In all cases where the disclosure of a record will entail the disclosure of information that is additional to the personal information of the person requesting the record, the written consent of the Information Officer (or his delegate) will be required, and that person will make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.
- If a request for personal information is made and part of the requested information may, or must be refused, every other part must still be disclosed.

10. REFUSAL OF ACCESS TO RECORDS AND REMEDIES OF REFUSAL

Based on POPIA & PAIA and at the discretion of the Information officer, access may be refused, on the following grounds. The Information officer will notify the requester of the outcome by using **PAIA Form 3, Annexure 13** referred to in **Section 19.**

- The information requested involves the unreasonable disclosure of personal or confidential information of a third party who is a
- natural person, including a deceased person.
- The information requested forms part of legally privileged information
- The information could be detrimental or disadvantage the commercial or financial interests of the Company or third parties
- The information requested is protected under legislation or agreements
- The disclosure of information requested would endanger an individual's physical safety or life.
- The information requested would be detrimental or disadvantage an individual in securing a property
- The information requested would be detrimental or disadvantage the protection of the safety of the public
- The information requested is frivolous or vexatious

Should the application be refused, the requester can lodge a complaint with the Information Regulator & Court against the refusal, within 30 days.

11. THE CORRECTION OF PERSONAL INFORMATION

- A client is entitled to require us to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.
- A client is also entitled to require us to destroy or delete records of personal information about the client that we are no longer authorised to retain.
- Any such request will be made on the prescribed form, **POPIA Form 2, Annexure 4**, referred to in **Section 19**.
- Upon receipt of such a lawful request, we will comply as soon as reasonably practicable.
- In the event that a dispute arises regarding the client's rights to have information corrected, and in the event that the client so requires, we will attach to the information, in a way that it will always be read with the information, an indication that the correction of the information was requested but was not made.
- We will notify the client who made a request for their personal information to be corrected or deleted what action(s) we take as a result of such a request.

12. SPECIAL PERSONAL INFORMATION

Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.
We will not process any of this Special Personal Information without the client's consent, or where this is necessary for the establishment, exercise or defence of a right or an obligation in law.
Having regard to the nature of our work, it is unlikely that we will ever have to process special personal information, but should it be necessary the guidance of the Information Officer, or their deputy/delegate, will be sought.

13. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

- We only process the personal information of a child if we have the consent of the child's parent or legal guardian.

14. INFORMATION & DEPUTY INFORMATION OFFICERS

- Our Information Officer is **MARGARET NORRIS** who is our Principal/Director/Owner. Such authorisation shall be made on **Annexure 9** referred to in **Section 19**. Our Information Officer's responsibilities include:
  - Ensuring compliance with POPI.
  - Dealing with requests which we receive in terms of POPI.
  - Working with the Information Regulator in relation to investigations.
  - Our Information Officer's details are:

    Margaret Norris
    Margaret.norris@zaprop.co.za
    082 498 7155
- Our Information Officer has designated in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in paragraph 1 above. Such designation was done by the completion of the prescribed form of which a copy is an annexure to this Compliance Manual, see **Annexure 8** referred to in **Section 19**.
  - Our Deputy Information Officer is MARK NORRIS who is our Director/Owner.
  - Our Deputy Information Officer's details are:
    Mark Norris
    Mark.norris@zaprop.co.za
    082 820 0503
- Our Information Officer and our Deputy Information Officers have registered themselves with the Information Regulator prior to taking up their duties, see **Annexure 7** referred to in **Section 19**.
  In carrying out their duties, our Information Officer or deputies ensured that:
  - this Compliance Manual was implemented;
  - a Personal Information Impact Assessment was done to identify Information and ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
  - that this Compliance Manual was developed and will be monitored, maintained using review register, **Annexure 10** in **Section 19** and made available;
  - that internal measures were developed together with adequate systems to process requests for information or access to information;
  - that internal awareness sessions are conducted using form regarding the provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator; and
  - that copies of this manual are provided to persons at their request, hard copies to be provided upon payment of a fee (to be determined by the Information Regulator).
- Guidance notes on Information Officers have been published by the Information Regulator (on 1 April 2021) and our Information Officer and deputy Information Officers have familiarised themselves with the content of these notes.

15. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

- In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:
  - In the event that we intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;
  - if we are processing information on criminal behaviour or unlawful or objectionable conduct;
  - if we are processing information for the purposes of credit reporting (this will be important if we are making reports to assist with member profiling).
  - if we are transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.
- The Information Regulator will be notified of our intention to process any personal information as set out in paragraph 1.1 above prior to any processing taking place and we will not commence with such processing until the Information Regulator has decided

in our favour.

- The Information Regulator has 4 weeks to make a decision but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator, which may not exceed 13 weeks. If the Information Regulator does not make a decision within the stipulated time periods, we can assume that the decision is in our favour and commence processing the information.

16. DIRECT MARKETING

- We will only carry out direct marketing (using any form of electronic communication) to clients if:
  - they were given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected; and
  - they did not object then or at any time after receiving any such direct marketing communications from us.
- We may only approach clients using their personal information, if we have obtained their personal information in the context of providing services associated with our business to them, and we may then only market such services to them.
- We may only carry out direct marketing (using any form of electronic communication) to other people if we have received their consent to do so.
- We may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent.
- A request for consent to receive direct marketing must be made in the prescribed manner and form. The prescribed form of this request and consent is an annexure to this Compliance Manual, **Annexure 5** referred to in **Section 19**. All direct marketing communications will disclose our identity and contain an address or other contact details to which the client may send a request that the communications cease.

17. TRANSBORDER INFORMATION FLOWS

- We may not transfer a client's personal information to a third party in a foreign country, unless:
  - the client consents to this, or requests it; or
  - such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country; or
  - the transfer of the personal information is required for the performance of the contract between ourselves and the client; or
  - the transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between ourselves and the third party; or
  - the transfer of the personal information is for the benefit of the client and it is not reasonably possible to obtain their consent and that if it were possible the client would be likely to give such consent.

18. OFFENCES AND PENALTIES

- POPI provides for serious penalties for the contravention of its terms.
  For minor offences a guilty party can receive a fine or be imprisoned for up to 12 months.
  For serious offences the period of imprisonment rises to a maximum of 10 years.
  Administrative fines for the company can reach a maximum of R10 million.
- Breaches of this Compliance Manual by staff members will be viewed as a serious disciplinary offence and can lead to dismissal.
- It is therefore imperative that we comply strictly with the terms of this Compliance Manual and protect our client's personal information in the same way as if it was our own.
- Staff have been given the opportunity to read through this manual and have signed the POPIA Manual Staff Confirmation Sheet, **Annexure 11** referred to is **Section 19.**

19. SCHEDULE OF ANNEXURES AND FORMS

1. Initial letter to client
2. Seller, Purchaser, Tenant & Landlord's consent to process personal information
3. Objection to the Processing of Personal Information
4. Request for correction or deletion of personal information
5. Application for consent to direct marketing
6. Addendum to the ZA Prop ZA letter of appointment.
7. Information Officer's registration form
8. Designation and delegation to Deputy Information Officer
9. Authorisation of Information Officer
10. POPIA Manual Review Register
11. POPIA Manual Staff Confirmation Sheets
12. Request to Access Records
13. Outcome of Request & of Fees Payable
14. ZA Prop Exclusive Mandate including POPI act April 2021
15. ZA Prop Dual Mandate including POPI act April 2021
16. ZA Prop Authority to Market (Open Mandate) including POPI act April 2021
17. ZA Prop RMCP Annexures 4.1 Individual & FICA Declaration including POPI act April 2021
18. ZA Prop RMCP Annexures 4.2 Companies & Closed Corporations including POPI act April 2021
19. ZA Prop RMCP Annexures 4.3 Trusts including POPI act April 2021
20. ZA Prop RMCP Annexures 4.4 Partnerships including POPI act April 2021
21. ZA Prop RMCP Annexures 4.5 Alternative Entities including POPI act April 2021
22. ZA Prop RMCP Annexures 4.6 Deceased/ Insolvent Estates including POPI act April 2021