POPIA checklist for estate agencies (South Africa)

A practical list of the things most agencies need to have in place to look after the personal information of buyers, sellers, tenants, landlords and staff. Tick what you have done, and plan the rest.

> This checklist is general information, not legal advice. Check your obligations with a qualified adviser or the Information Regulator. Working through it does not, on its own, make an agency compliant.

1 Information Officer

The head of the business is the Information Officer unless someone else is formally authorised.

- [ ] Decide who your Information Officer is, and appoint any deputies in writing.
- [ ] Register the Information Officer with the Information Regulator, and keep the registration up to date when people change.
- [ ] Make sure staff know who to send privacy questions and complaints to.

2 Know what you hold, and why

- [ ] List the kinds of personal information you hold: buyers, sellers, tenants, landlords, applicants, staff.
- [ ] For each, note why you collect it, where it is kept (CRM, email, spreadsheets, paper files, phones) and who can see it.
- [ ] Collect only what you need for that purpose, and stop collecting what you do not use.
- [ ] Tell people what you collect and why, for example in your mandate forms, lease applications and privacy notice.

3 Consent for marketing

- [ ] Before sending marketing by email, SMS or WhatsApp to people who are not already your clients, get their consent and record when and how it was given.
- [ ] Give an easy way to opt out in every marketing message, and act on opt-outs promptly.
- [ ] Check bought or shared contact lists before using them. If you cannot show consent, do not use them for marketing.

4 Secure client documents

FICA documents, ID copies, bank statements and payslips are among the most sensitive things an agency holds.

- [ ] Limit access: each person sees only what their role needs, and access is removed when someone leaves.
- [ ] Use encryption for laptops, phones and any system that stores client documents.
- [ ] Keep regular backups, store at least one copy separately, and test that you can restore it.
- [ ] Use strong, unique passwords and two-step sign-in for email and your CRM.
- [ ] Lock away paper files and shred copies you no longer need.

5 Operators: your software and service suppliers

- [ ] List the suppliers that process personal information for you: CRM, email, cloud storage, IT support, bookkeepers.
- [ ] Have a written agreement with each that requires them to keep the information confidential and secure, and to use it only on your instruction.
- [ ] Find out where each supplier stores your data. If it is outside South Africa, check that the transfer meets POPIA's conditions.

6 A breach response plan

- [ ] Write down what staff must do if a device is lost, an inbox is compromised or data is sent to the wrong person.
- [ ] Know how to notify the Information Regulator and the people affected, as soon as reasonably possible after a compromise.
- [ ] Keep a record of every incident, what was done, and what was changed afterwards.

7 Retention and deletion

- [ ] Set how long you keep each kind of record, and why. FICA and tax law have their own minimum periods; check which apply to you.
- [ ] Delete or anonymise records once there is no longer a reason to keep them, including old leads and unsuccessful applications.
- [ ] Remember copies in email, downloads folders, WhatsApp chats and old devices.

8 Requests from clients

- [ ] Have a simple process for people who ask what you hold about them, or ask you to correct or delete it.
- [ ] Verify who is asking before you hand over any personal information.
- [ ] Check whether you need a PAIA manual, and how people can request access to records.

9 People and habits

- [ ] Brief every agent and administrator on the basics, and repeat it when someone new joins.
- [ ] Include confidentiality in employment and contractor agreements.
- [ ] Review this checklist at least once a year.