EVERYDAY LEGAL
SOLUTIONS

FREE GUIDE · POPIA & DATA

POPIA compliance checklist for small businesses

POPIA applies to every South African business that processes personal information, with no exemption for small businesses. Compliance comes down to meeting eight conditions for lawful processing, set out in sections 8 to 25 of the Act. In practice, that means 12 concrete steps: know what data you hold, have a lawful reason to hold it, register an Information Officer, publish a privacy notice, secure the data, and be ready to report a breach.

REVIEWED BY THE ELS TEAM

Build on solid legal ground

Published 2 October 2026 · South Africa

everydaylegalsolutions.co.za

AT A GLANCE

- POPIA applies to every business that processes personal information. **There's no small-business exemption.**
- **Register your Information Officer** with the Information Regulator.
- Since **1 April 2025**, breaches must be reported through the Regulator's eServices portal.
- Administrative fines can reach **R10 million**.

Does POPIA apply to your business?

Almost certainly. If you keep client contact details, employee records, supplier contacts, customer orders or a mailing list, you are processing personal information. Under POPIA, personal information also includes information about existing companies and other juristic persons, not just individuals.

The eight conditions behind every step

POPIA's eight conditions for lawful processing are **accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation**. The checklist below turns them into actions.

The 12-step POPIA checklist

1. Map the personal information you hold

List what you collect, from whom, why, where it's stored, who can access it and how long you keep it. Cover clients, customers, employees, job applicants, suppliers and website visitors. Everything else depends on this map.

2. Confirm a lawful reason for each purpose

Consent is only one of the lawful grounds in section 11. You can also process information when it's necessary to perform a contract, to comply with a legal obligation, or to pursue a legitimate interest. Match each purpose on your map to its ground. If consent is your ground, you need proof of it.

3. Appoint and register your Information Officer

The head of your business (owner, managing director or CEO) is the Information Officer by default under section 55. You must register them with the Information Regulator. You can also designate deputy information officers to help.

4. Publish a privacy notice

Section 18 requires you to tell people, when you collect their information, what you're collecting, why, whether it's voluntary or required, who you'll share it with, and what their rights are. Most businesses publish a privacy notice on their website and refer to it in forms, contracts and onboarding.

5. Adopt an internal POPIA policy and train your staff

Accountability means you can show how your business complies. An internal policy sets the rules for collecting, using, sharing, storing and deleting personal information. Train everyone who handles it, including temporary staff.

6. Put reasonable security safeguards in place

Section 19 requires appropriate, reasonable technical and organisational measures to prevent loss, damage and unauthorised access. For a small business, that typically means:

- Strong passwords and multi-factor authentication on email and cloud accounts.
- Access only for people who need it.
- Regular backups.
- Encrypted laptops and phones.
- Locked storage for paper records.
- A process for removing access when someone leaves.

7. Sign operator agreements with your service providers

An “operator” processes personal information on your behalf: your payroll provider, cloud CRM, email marketing tool, IT support or outsourced bookkeeper. Sections 20 and 21 require a written contract that obliges the operator to keep the information confidential and secure.

8. Prepare a breach response plan

If you have reasonable grounds to believe personal information has been accessed or acquired by an unauthorised person, section 22 requires you to notify the Information Regulator and the affected people as soon as reasonably possible.

> **Breaches go through the portal.** Since 1 April 2025, notifications to the Regulator must go through its eServices portal, not email. Decide now who does what, and get your Information Officer registered on the portal before you need it.

9. Get direct marketing right

Under section 69, you generally need consent before sending electronic direct marketing (email, SMS, WhatsApp) to people who aren’t your customers. For existing customers, you may market similar products or services if you gave them a chance to opt out when you collected their details, and every message must include an opt-out.

10. Set retention periods and delete what you don’t need

Keep personal information only as long as you need it for its purpose, or as long as another law requires (for example, tax and employment records). Then destroy or de-identify it securely.

11. Be ready to handle requests from people

People can ask whether you hold their information, request a copy, ask you to correct or delete it, and object to certain processing. Decide who handles these requests and how quickly.

12. Check for special cases

Extra rules apply to:

- **Special personal information,** such as health, religion, race, biometrics and criminal behaviour.
- **Children's information.**
- **Cross-border transfers** (section 72): if your cloud provider stores data outside South Africa, check that the transfer is allowed.

And don't forget your **PAIA manual**, which every business has needed since 1 January 2022. Read our PAIA manual guide.

The checklist mapped to your documents

STEPS	WHAT POPIA REQUIRES	DOCUMENT THAT COVERS IT
1, 2, 5, 6, 10, 11	Accountability, lawful processing, security, retention, data subject requests	POPIA internal policy
4	Openness: telling people how you use their information	POPIA privacy notice
7	Written contracts with operators	POPIA operator undertaking
2, 9	Proof of consent where consent is your lawful ground	POPIA consent form
12	Access-to-information manual	PAIA manual
3, 8	Information Officer registration and breach reporting	Done through the Information Regulator's portal

What happens if you don't comply?

The Information Regulator can investigate complaints, issue enforcement notices and impose administrative fines of up to R10 million. Some offences under POPIA also carry criminal penalties. People whose information is mishandled can claim damages too.

For most small businesses, the more immediate risk is commercial. Larger clients increasingly ask suppliers to show POPIA compliance before they sign, and a data breach without a plan is far more damaging than one you were ready for.

Frequently asked questions

Is there a small-business exemption from POPIA?

No. POPIA applies regardless of size. What scales is the effort: a five-person business needs the same documents as a large one, but simpler processes.

Do I need consent for everything?

No. Consent is one of several lawful grounds. Much routine processing, such as handling a client's details to deliver their order, is justified because it's necessary for the contract.

Who should be our Information Officer?

By default, the head of the business. You can designate deputy information officers, but responsibility stays with the head.

Do we have to report a small breach, like one misdirected email?

The Regulator's guidance says reporting is mandatory where section 22 applies, and responsible parties don't have discretion to skip it. If in doubt, treat it as reportable and get advice.

Get your POPIA documents in one go

The ELS **POPIA Compliance Pack** includes all five documents in the table above: privacy notice, internal policy, operator undertaking, consent form and PAIA manual. Running a website or online store? The **Web & Online Pack** adds your website terms and conditions.

SEE THE POPIA COMPLIANCE PACK

TAKE THE FREE LEGAL HEALTH CHECK

INFORMATION, NOT ADVICE

ELS provides legal information, not legal advice. Nothing in this guide creates an attorney-client relationship. For advice on your specific situation, consult a qualified attorney. The law is stated as at 2 October 2026.

EVERYDAY LEGAL SOLUTIONS

Attorney-drafted legal documents and plain-English legal information for South African businesses. Not sure what your business needs? Take the free Legal Health Check.

Build on solid legal ground.