POPIA Readiness Checklist

Protection of Personal Information Act 4 of 2013. What a South African business has to have in place.

POPIA applies to every responsible party domiciled in South Africa that processes personal information. There is no exemption based on headcount or turnover. This checklist sets out the 22 things the Act and the Information Regulator expect you to be able to show.

1. Accountability and roles

Condition 1 of the eight conditions for lawful processing is Accountability, section 8. Sections 55 and 56 deal with the Information Officer. Regulation 4, as amended on 17 April 2025, sets out that officer's responsibilities.

- [ ] **1. Confirm who your Information Officer is**
  In a private body the Information Officer is the chief executive officer, the owner or the partner by default. That person may authorise someone else in writing, but the head of the body stays accountable.
  POPIA s1 read with s55

- [ ] **2. Register the Information Officer with the Regulator**
  An Information Officer takes up duties only after registration with the Information Regulator, done on the eServices portal.
  POPIA s55(2)

- [ ] **3. Designate deputy Information Officers**
  One or more deputies keep the organisation reachable for data subjects and requesters. The Regulator expects deputies to sit at management level.
  PAIA s17

- [ ] **4. Develop and continually improve a compliance framework**
  The framework must be developed, implemented, monitored, maintained and continually improved. A document written once in 2021 no longer meets the wording.
  Regulation 4(1)(a), amended 17 April 2025

- [ ] **5. Publish and maintain a PAIA manual**
  Every private body must have a manual, on its website, at its principal place of business, on request, and to the Regulator. The small-body exemption lapsed on 31 December 2021.
  PAIA s51

2. Lawful processing and transparency

Conditions 2 to 6 cover processing limitation (s9 to s12), purpose specification (s13 and s14), further processing (s15), information quality (s16) and openness (s17 and s18).

- [ ] **6. Map the personal information you hold**
  List what you collect, why, where it sits, who can see it and who you share it with. Without this you cannot evidence a lawful basis, a retention period or a control.
  POPIA s17

- [ ] **7. Confirm a lawful justification for each purpose**
  The grounds are consent, contract necessity, a legal obligation, protecting the data subject's legitimate interest, a public law duty, or legitimate interests. Consent is one option, not the default.
  POPIA s11

- [ ] **8. Give a collection notice to data subjects**
  At collection, tell the person what you are collecting, who you are, why, whether supply is voluntary, the consequences of not supplying, and their rights.
  POPIA s18

- [ ] **9. Handle special personal information with care**
  Religion, race, trade union membership, political persuasion, health, sex life, biometrics and criminal behaviour are prohibited unless a listed ground applies.
  POPIA s26 to s33

- [ ] **10. Check whether prior authorisation applies**
  Prior authorisation is needed for defined processing, including credit reporting and certain cross-border transfers of special or children's information.
  POPIA s57

- [ ] **11. Set and apply retention and deletion rules**
  Records may not be kept longer than necessary for the purpose, and must be destroyed, deleted or de-identified as soon as reasonably practicable once retention is no longer authorised.
  POPIA s14 and s14(4)

3. Security safeguards and third parties

Condition 7 is Security safeguards, sections 19 to 22. Section 72 governs transfers outside South Africa.

- [ ] **12. Implement reasonable technical and organisational measures**
  Identify foreseeable internal and external risks, put safeguards in place, verify regularly that they work, and update them as risks change. The Regulator's first fine concerned expired security licences.
  POPIA s19

- [ ] **13. Put written operator contracts in place**
  Payroll bureaus, cloud providers, IT support, recruiters and marketing agencies are operators. Each needs a written contract obliging them to maintain your security measures.
  POPIA s21

- [ ] **14. Check transfers outside South Africa**
  Foreign hosted email, cloud storage and software as a service must be assessed against the listed transfer grounds before you rely on them.
  POPIA s72

4. Data subject rights, complaints and direct marketing

Condition 8 is Data subject participation, sections 23 to 25. Section 69 governs unsolicited electronic direct marketing.

- [ ] **15. Build a data subject request process**
  People may ask what you hold and request correction or deletion of information that is inaccurate, excessive, out of date, misleading or unlawfully obtained.
  POPIA s23 to s25

- [ ] **16. Accept objections free of charge on multiple channels**
  Since April 2025 an objection may come by hand, post, email, SMS, WhatsApp or telephone, free of charge. Telephonic objections must be recorded.
  Regulation 2, amended 17 April 2025

- [ ] **17. Get direct marketing consent right**
  Unsolicited electronic direct marketing needs consent, and you may approach a person for that consent once only. Existing customers may be marketed similar products with an opt-out in every message.
  POPIA s69

- [ ] **18. Register on the National Opt-Out Registry if you direct market**
  From 15 April 2026 direct marketers must register with the National Consumer Commission and cleanse their databases monthly against the registry. POPIA consent duties continue to apply alongside this.
  CPA Amendment Regulations, 2026

- [ ] **19. Run a documented complaints process**
  Complaints may be lodged on the prescribed form or one substantially similar, and must be acknowledged. A complaints register is useful evidence.
  Regulation 7, amended 2025

5. Breach response and enforcement readiness

Section 22 governs security compromise notification. Chapter 10 governs enforcement, and sections 107 to 109 the penalties.

- [ ] **20. Report security compromises through the eServices portal**
  Where there are reasonable grounds to believe personal information was accessed by an unauthorised person, notify the Regulator and the affected people as soon as reasonably possible. Since 1 April 2025 reporting is through the portal, not email.
  POPIA s22

- [ ] **21. Prepare a breach playbook and keep records**
  The Regulator's August 2025 fact sheet states there is no minimum threshold, so all security compromises are reportable, and that you report before the investigation is finished.
  Regulator fact sheet, 19 August 2025

- [ ] **22. Be ready for a compliance monitoring request**
  Since late 2025 the Regulator has been selecting organisations and requiring a POPIA compliance report with supporting documents within 14 business days.
  POPIA s89

What non-compliance costs

- Administrative fine: up to R10 million by infringement notice, section 109. Fines issued to date include R5 million twice, R500 000 and R100 000 twice.
- Criminal: a fine set by the court, or imprisonment of up to 10 years for the more serious offences and up to 12 months for the rest, section 107. The often-quoted 'R10 million or 10 years' conflates two different provisions.
- Civil: a data subject may claim damages whether or not there was intent or negligence, section 99. There is no stated cap.
- Pattern to note: every administrative fine so far followed a failure to comply with an enforcement notice, not the underlying contravention on its own.