POPIA Compliance Checklist

All 54 requirements of the Protection of Personal Information Act, 4 of 2013 — with the POPIA section behind each one and the evidence an assessor will ask you to produce.

How to use this checklist

1. Score each item Compliant, Partially compliant, Not compliant or Not applicable.
2. Attach the evidence named in the item. If you cannot produce it, the item is not compliant.
3. Score it: compliant counts 1, partial counts 0.5, not-applicable items are excluded from the denominator.
4. Fix the lowest-scoring conditions first — Processing Limitation and Security Safeguards carry the most risk.
5. Re-assess at least annually and after any material change to your systems or vendors.

Run this checklist free with live scoring, evidence uploads and certification at popia.commtac.co/resources/popia-compliance-checklist

Application — does POPIA apply to you?

Sections 3 to 7. Before you do anything else, confirm POPIA applies and record which statutory exclusions you rely on.

Ref	POPIA	Requirement & evidence	Status
A1	s.3	Confirm POPIA applies: the responsible party is domiciled in South Africa, or processing of personal information takes place in South Africa. **Evidence:** Applicability assessment or legal opinion confirming POPIA applies.	
A2	s.6 & s.7	Identify whether any statutory exclusions apply (purely personal or household activity; de-identified information; cabinet or legislative function; judicial functions; journalistic, literary or artistic expression). **Evidence:** Documented exclusion assessment with motivation.	

Condition 1 — Accountability

Section 8. Someone must own POPIA compliance, and the ownership must be documented.

Ref	POPIA	Requirement & evidence	Status
C1.1	s.8	The responsible party has taken accountable steps to ensure all 8 conditions are met when the purpose and means of processing are determined, and throughout processing. **Evidence:** POPIA compliance framework signed off by an accountable executive.	
C1.2	s.8	A POPIA governance structure is in place (Information Officer, deputies, privacy committee) with documented roles and responsibilities. **Evidence:** Governance terms of reference; organogram; appointment letters.	

Condition 2 — Processing Limitation

Sections 9 to 12. This is where most assessments lose points: organisations process data they cannot justify, on a lawful basis they never wrote down.

Ref	POPIA	Requirement & evidence	Status
C2.1	s.9	Personal information is processed lawfully and in a manner that does not unreasonably infringe the data subject's privacy. **Evidence:** Lawful basis register; privacy notice; legitimate interest assessments.	

Ref	POPIA	Requirement & evidence	Status
C2.2	s.10	Minimality: the personal information processed is adequate, relevant and not excessive given the purpose. **Evidence:** Data minimisation review per processing activity; form audit.	
C2.3	s.11(1)	A lawful justification exists for every processing activity: consent, contract, legal obligation, protection of a legitimate interest, public law duty, or legitimate interests of the responsible party or a third party. **Evidence:** Processing activity register with the lawful basis recorded per activity.	
C2.4	s.11(2)	Where consent is the lawful basis, consent is voluntary, specific and informed, you can demonstrate the data subject consented, and there is a mechanism to withdraw consent at any time. **Evidence:** Consent records; consent capture screens; withdrawal procedure.	
C2.5	s.11(3)	Data subjects can object to processing on reasonable grounds (and always for direct marketing) using the prescribed or an equivalent form, and processing stops on a valid objection. **Evidence:** Objection procedure and form; objection register.	
C2.6	s.12	Personal information is collected directly from the data subject unless a listed exception applies and is documented. **Evidence:** Collection source register; documented exceptions.	

Condition 3 — Purpose Specification

Sections 13 to 14. Every purpose must be specific and every record must have an end date.

Ref	POPIA	Requirement & evidence	Status
C3.1	s.13	Each processing activity has a specific, explicitly defined and lawful purpose, and the data subject is made aware of it at the point of collection. **Evidence:** Processing register; privacy notices linked to each collection point.	
C3.2	s.14(1)–(3)	A retention schedule defines maximum retention periods per category of personal information, and records are not kept longer than necessary. **Evidence:** Retention and disposal schedule; records management policy.	
C3.3	s.14(4)–(5)	At the end of the retention period records are destroyed, deleted or de-identified so they cannot be reconstructed in intelligible form. **Evidence:** Destruction or de-identification procedure; destruction certificates.	
C3.4	s.14(6)–(7)	Where processing is restricted (accuracy disputed, no longer needed but required for legal claims), restrictions are applied and the data subject is notified before they are lifted. **Evidence:** Restriction-of-processing procedure; restriction register.	

Condition 4 — Further Processing Limitation

Section 15. New uses of existing data need a compatibility test, not a new privacy policy line.

Ref	POPIA	Requirement & evidence	Status
C4.1	s.15	Any further processing is assessed for compatibility with the original purpose against the section 15(2) factors: relationship, nature of the information, consequences, manner of collection and contractual rights. **Evidence:** Compatibility assessment template; completed assessments for new uses.	

Condition 5 — Information Quality

Section 16. Accuracy is a legal obligation, not a data-hygiene nice-to-have.

Ref	POPIA	Requirement & evidence	Status
C5.1	s.16	Reasonably practical steps are taken to ensure personal information is complete, accurate, not misleading and updated where necessary, taking the purpose into account. **Evidence:** Data quality procedures; periodic data refresh or verification process.	

Condition 6 — Openness

Sections 17 to 18, read with PAIA. If your privacy notice is missing one of the section 18 matters, this condition fails.

Ref	POPIA	Requirement & evidence	Status
C6.1	s.17 (with PAIA s.14/51)	A PAIA manual is maintained and made available, addressing the documentation requirements for processing personal information. **Evidence:** Current PAIA manual published on the website and available at premises.	
C6.2	s.18(1)	Data subjects are notified, before or as soon as reasonably practicable after collection, of every required matter: the information collected, its source, the name and address of the responsible party, the purpose, whether supply is voluntary or mandatory, consequences of not providing it, applicable laws, any intention to transfer abroad, recipients, and rights to access, correct and complain. **Evidence:** Privacy notices; collection-point notifications; just-in-time notices.	
C6.3	s.18(4)	Where exemptions from notification are relied on, the basis is documented. **Evidence:** Documented exemption assessment per section 18(4).	

Condition 7 — Security Safeguards

Sections 19 to 22. This condition carries the breach-notification duty and the operator contract requirement that catches most organisations out.

Ref	POPIA	Requirement & evidence	Status
C7.1	s.19(1)	Appropriate, reasonable technical and organisational measures protect personal information against loss, damage, unauthorised destruction, unlawful access or processing. **Evidence:** Information security policy; ISO 27001 or equivalent ISMS.	
C7.2	s.19(2)	A documented risk assessment identifies all reasonably foreseeable internal and external risks, with safeguards established, regularly verified and updated. **Evidence:** Personal information risk register; periodic risk assessment reports.	
C7.3	s.19(3)	Generally accepted information security practices and procedures, both industry-specific and general, are adopted. **Evidence:** Mapping of controls to ISO 27001, NIST, King IV or sector standards.	
C7.4	s.20	Operators and persons acting under the responsible party's authority process personal information only with knowledge or authorisation and treat it as confidential. **Evidence:** Confidentiality undertakings; access control matrix; authorised-user list.	

Ref	POPIA	Requirement & evidence	Status
C7.5	s.21	A written contract with every operator requires them to establish and maintain section 19 security measures and to notify the responsible party of security compromises immediately. **Evidence:** Operator (DPA) contract register; signed agreements.	
C7.6	s.22	A documented incident response and breach notification procedure exists: notify the Information Regulator and affected data subjects as soon as reasonably possible, with communications meeting the section 22(5) content requirements. **Evidence:** Incident response plan; breach register; notification templates.	

Condition 8 — Data Subject Participation

Sections 23 to 25. People must be able to see, correct and delete what you hold about them.

Ref	POPIA	Requirement & evidence	Status
C8.1	s.23	A process confirms whether personal information about a data subject is held and provides the record or a description within a reasonable time, in a reasonable manner and format, at the prescribed fee. **Evidence:** Subject access request procedure and log; response templates.	
C8.2	s.24	A process lets data subjects request correction, deletion or destruction of information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained. **Evidence:** Correction and deletion request procedure; request register.	
C8.3	s.25	The manner of access aligns with the procedures, forms and fees prescribed under PAIA. **Evidence:** PAIA-aligned request forms; fee schedule.	

Special personal information and children

Sections 26 to 35. Health, biometrics, race, religion, trade union membership, political persuasion, sex life, criminal behaviour and any information about children need a specific statutory authorisation.

Ref	POPIA	Requirement & evidence	Status
SP1	s.26	Identify whether any special personal information is processed: religion or philosophy, race or ethnic origin, trade union membership, political persuasion, health, sex life, biometric information or criminal behaviour. **Evidence:** Special personal information inventory.	
SP2	s.27–33	For each category of special personal information, a lawful authorisation under sections 27 to 33 is documented (consent, established by law, public interest, necessary for a legal claim, or deliberately made public). **Evidence:** Authorisation matrix per category.	
CH1	s.34	Identify whether personal information of children is processed. **Evidence:** Children's personal information inventory; age-gating assessment.	
CH2	s.35	Where children's information is processed, an authorisation under section 35 is in place: consent of a competent person, necessity for law or a legal claim, public interest with safeguards, or information deliberately made public by the child with consent. **Evidence:** Parental or guardian consent records; authorisation rationale.	

Information Officer, exemptions and prior authorisation

Sections 36 to 38 and 55 to 58. Registration is a hard requirement, and some processing may not start at all until the Regulator authorises it.

Ref	POPIA	Requirement & evidence	Status
EX1	s.37 & 38	Where a Regulator-granted or function-based exemption is relied on, the authorisation is documented and current. **Evidence:** Regulator authorisation letter; documented function-based assessment.	
IO1	s.55(1)(a) & Regs	An Information Officer has been designated and registered with the Information Regulator before performing their duties. **Evidence:** Registration confirmation from the Regulator.	
IO2	s.56	Deputy Information Officers are designated in writing to assist the Information Officer, with documented delegations. **Evidence:** Deputy designation letters; registration where required.	
IO3	s.55(1)(b)–(f) & Reg 4	Information Officer duties are actively discharged: encourage compliance, deal with requests, cooperate with the Regulator, develop and implement a compliance framework, conduct impact assessments, maintain the PAIA manual, run internal awareness and training, handle complaints and maintain the section 17 documentation. **Evidence:** Compliance framework; training records; PAIA manual; impact assessment reports.	
PA1	s.57	Determine whether any processing is subject to prior authorisation by the Regulator. **Evidence:** Prior-authorisation assessment register.	
PA2	s.58	Where prior authorisation applies, the Regulator has been notified and processing has not commenced until authorised or the statutory waiting period elapsed without objection. **Evidence:** Notification letter; authorisation or acknowledgement received.	

Direct marketing, directories and automated decisions

Sections 69 to 71. Electronic direct marketing to non-customers is opt-in only.

Ref	POPIA	Requirement & evidence	Status
DM1	s.69(1)–(3)	Electronic direct marketing is only sent with prior opt-in consent, or to an existing customer for similar products and services where opt-out was offered at collection and in every subsequent communication. **Evidence:** Marketing consent register; unsubscribe records; suppression list.	
DM2	s.69(4)	Every direct marketing communication includes the sender's details and a clear opt-out mechanism. **Evidence:** Sample communications showing identification and opt-out.	
DR1	s.70	If directories are published, data subjects are informed free of charge of the purpose before inclusion, and given a free opt-out and the ability to verify, correct or withdraw their data. **Evidence:** Directory inclusion notice and opt-out procedure.	
AD1	s.71	Decisions with legal or substantial effects are not based solely on automated processing unless an exception applies and safeguards such as human review and the ability to make representations are in place. **Evidence:** Automated decision inventory; human review procedures; impact assessment.	

Cross-border transfers, enforcement and account numbers

Sections 72 to 109. Cloud hosting outside South Africa is a cross-border transfer and needs a section 72 basis.

Ref	POPIA	Requirement & evidence	Status
TB1	s.72	Cross-border transfers only occur where at least one section 72 condition is met: adequacy, consent, contract necessity, a contract in the data subject's interest, or benefit to the data subject. **Evidence:** Transfer impact assessments; cross-border data-flow map; transfer agreements such as standard contractual clauses.	
EN1	s.74 & s.5(f)	An internal complaints procedure exists for data subjects, referencing the right to complain to the Regulator. **Evidence:** Complaints procedure; complaints register; published contact details.	
EN2	s.81 & s.89–95	A documented approach exists for cooperating with the Regulator: responding to information notices, assessments and enforcement notices within prescribed time-frames. **Evidence:** Regulator engagement procedure; sample responses.	
OP1	s.105–106	Account numbers (bank, credit, store, customer) are processed only where lawful and necessary, with controls preventing unlawful disclosure, procurement and use. **Evidence:** Account-number handling procedure; access controls; logging.	
OP2	s.107–109	Leadership is aware of the penalty regime, including administrative fines up to R10 million, and there is board-level oversight of POPIA compliance. **Evidence:** Board or Exco reporting cadence; minutes.	

Cross-cutting operational controls

The programme layer. These seven controls are what turn a one-off remediation project into defensible, ongoing compliance.

Ref	POPIA	Requirement & evidence	Status
OC1	Programme	An overall written POPIA or data protection policy is approved, communicated and reviewed at defined intervals. **Evidence:** Version-controlled data protection policy with approval evidence.	
OC2	Programme	A current Records of Processing Activities (RoPA) or personal information inventory and data-flow map is maintained. **Evidence:** RoPA spreadsheet or system entries.	
OC3	Programme	A Personal Information Impact Assessment methodology is in place, and assessments are performed for new or high-risk processing. **Evidence:** Methodology document; completed assessments.	
OC4	Programme	An awareness and training programme covers all employees and contractors handling personal information, refreshed at least annually. **Evidence:** Training plan; attendance records; e-learning completion reports.	
OC5	Programme	A vendor and operator management programme covers due diligence at onboarding, signed data processing agreements and periodic assurance. **Evidence:** Vendor risk assessments; DPA register; assurance reports.	
OC6	Programme	A data subject request register tracks access requests, corrections, deletions, objections and complaints, with response times measured against statutory limits. **Evidence:** Request register or case-management reports.	

Ref	POPIA	Requirement & evidence	Status
OC7	Programme	Periodic internal audit or compliance monitoring of POPIA controls, with findings tracked to closure. **Evidence:** Internal audit reports; management action plans.	