POPIA Readiness & Compliance Checklist

A practical checklist for assessing POPIA readiness across information officer duties, data subject rights, and breach management

POPIA · Data Protection · Privacy · Information Officer · Data Subject Rights · Breach Management

POPIA compliance in South Africa depends on an appointed Information Officer, documented processing conditions, and a working process for data subject requests and breaches. This checklist sets out a practical sequence for assessing readiness against the Information Regulator's expectations.

A Information Officer & Governance

- [ ] Appoint an Information Officer and register the appointment with the Information Regulator
- [ ] Appoint deputy information officers for business units or sites where needed
- [ ] Define the Information Officer's responsibilities for POPIA compliance oversight
- [ ] Maintain a POPIA governance structure with clear reporting to management
- [ ] Review Information Officer duties and resourcing on a periodic basis

B Processing Conditions & Lawful Processing

- [ ] Identify and document the lawful justification for each processing activity
- [ ] Confirm personal information is processed only for the purpose it was collected
- [ ] Apply minimality — collect only the personal information reasonably required
- [ ] Obtain consent where consent is the relied-upon justification, and record it
- [ ] Review special personal information and children's information processing for additional safeguards

C Data Subject Rights (PAIA-linked Access)

- [ ] Provide a documented process for data subjects to request access to their personal information
- [ ] Provide a process for correction or deletion of inaccurate or unlawfully held information
- [ ] Verify requester identity before actioning a request
- [ ] Track request timelines from receipt to response and closure
- [ ] Handle objections to processing, including for direct marketing purposes

D Security Safeguards

- [ ] Implement appropriate technical and organisational measures to secure personal information
- [ ] Maintain access controls limiting personal information access to those who need it
- [ ] Assess and document risks to personal information in the organisation's care
- [ ] Review security safeguards when systems, vendors, or processing activities change
- [ ] Maintain an inventory of systems and locations where personal information is held

E Breach (Security Compromise) Management

- [ ] Maintain a documented process for identifying and assessing a security compromise
- [ ] Notify the Information Regulator as soon as reasonably possible once a compromise is confirmed
- [ ] Notify affected data subjects where there are reasonable grounds to believe their information was accessed unlawfully
- [ ] Record breach details, impact assessment, and remedial steps in a breach register
- [ ] Review the cause of each breach and update controls to prevent recurrence

F Third-Party & Operator Agreements

- [ ] Maintain a register of operators processing personal information on the organisation's behalf
- [ ] Confirm written agreements with operators cover confidentiality and security obligations
- [ ] Require operators to notify the organisation promptly of any security compromise
- [ ] Review operator security practices before onboarding and periodically thereafter
- [ ] Assess cross-border transfers of personal information for adequate safeguards

G Cross-Border Transfers

- [ ] Identify all instances where personal information is transferred outside South Africa
- [ ] Confirm the receiving party is subject to comparable data protection obligations
- [ ] Document the legal basis relied on for each cross-border transfer
- [ ] Review cross-border arrangements when providers, contracts, or hosting locations change

H Training & Awareness

- [ ] Deliver POPIA training to employees who handle personal information
- [ ] Ensure the Information Officer and deputies receive role-specific training
- [ ] Track training completion and retain evidence for audit purposes
- [ ] Raise awareness of how to identify and report a suspected security compromise