POPIA Compliance Checklist

Last Updated: 28 February 2026

JACOBS & POTGIETER INCORPORATED

The operative sections of the Protection of Personal Information Act 4 of 2013 (POPIA) came into effect on the 1st of July 2020, with a grace period of one year to ensure that companies comply with the requirements of the new legislation. Companies must ensure that their business practices and dealings with customers, clients, or consumers are compliant with the relevant privacy legislation, and that the collection, storage, and processing of client and even employees' data are compliant with POPIA.

STEP 1:
Information Officer & Governance

- [ ] Appoint an Information Officer and (where necessary) Deputy Information Officers.
- [ ] Register Information Officers with the Information Regulator (https://eservices.inforegulator.org.za)
- [ ] Develop and implement a POPIA compliance framework.
- [ ] Conduct internal POPIA awareness training with all staff.
- [ ] Establish internal monitoring and reporting structures.
- [ ] Ensure PAIA Manual is developed or updated.

STEP 2:
Personal Information Mapping & Risk Assessment

- [ ] Compile an inventory of all personal information processed (client & employee info).
- [ ] Identify special personal information (biometric, health, religion, criminal history).
- [ ] Document processing purposes and legal basis.
- [ ] Conduct Personal Information Impact Assessments.
- [ ] Map data flows across departments and third parties.

www.jacobspotgieterinc.co.za
+27 71 471 5432
+27 82 889 6472
info@jacobspotgieter.co.za

JACOBS & POTGIETER INCORPORATED

STEP 3:
Lawful Processing Compliance

- [ ] Ensure processing is lawful, minimal, and purpose-specific.
- [ ] Obtain valid consent where required.
- [ ] Document alternative legal justifications (contractual necessity, legal obligation).
- [ ] Ensure compatibility for further processing activities.

STEP 4:
Data Subject Notification Requirements

- [ ] Notify data subjects when collecting personal information.
- [ ] Disclose purpose of collection.
- [ ] Provide company and information officer contact details.
- [ ] Disclose third-party sharing.
- [ ] Disclose cross-border transfers.

STEP 5:
Security Safeguards

- [ ] Implement technical safeguards (encryption, firewalls).
- [ ] Implement organisational safeguards (access control, policies).
- [ ] Conduct cybersecurity risk assessments.
- [ ] Maintain breach response plans.

JACOBS & POTGIETER INCORPORATED

STEP 6:
Record Retention & Disposal

- [ ] Define retention periods.
- [ ] Ensure lawful retention justification.
- [ ] Securely delete or de-identify records no longer required.

STEP 7:
Operator & Third-Party Management

- [ ] Execute operator agreements.
- [ ] Ensure third parties maintain POPIA compliance.
- [ ] Monitor vendor security standards.

STEP 8:
Data Subject Access Requests

- [ ] Implement DSAR request procedures.
- [ ] Allow correction, deletion, or objection requests.
- [ ] Maintain response timelines.

STEP 9:
Direct Marketing Compliance

- [ ] Obtain consent for electronic marketing.
- [ ] Maintain opt-out mechanisms.
- [ ] Keep marketing consent records.

www.jacobspotgieterinc.co.za
+27 71 471 5432
+27 82 889 6472
info@jacobspotgieter.co.za

JACOBS & POTGIETER INCORPORATED

STEP 10:
Cross-Border Transfers

- [ ] Assess adequacy of foreign data protections.
- [ ] Obtain consent where required.
- [ ] Execute data transfer agreements.