Reg. No.: 2019 / 086104 / 07
Phone: +27 79 885 4543

POPIA COMPLIANCE CHECKLIST (HIGH LEVEL)

1. Formalise your POPIA compliance project

- Identify your relevant stakeholders (clients, suppliers, individuals etc.)
- Identify your project sponsor
- Identify your project manager
- Set high level scope, timescale, budget
- Identify security safeguards applicable to your industry / business

2. Appoint an Information Officer (Legal requirement – Default is highest ranking officer)

- Ensure alignment between your Promotion of Access to Information Act (PAIA) and POPIA Information Officer (IO)
- Decide whether the CEO can fulfil the IO function or needs a Deputy/Deputies (DIO)
- Agree IO/DIO roles and responsibilities
- Complete the formal appointment process

3. Perform a gap analysis versus the ACT (POPIA)

- Set interim and final targets for compliance – Compliance within reasonable practicality.
- Engage with stakeholders in the assessment
- Use an evidence-based approach
- Use the assessments for ongoing compliance monitoring

4. Analyse what and how Personal Information is processed (status quo)

- Use a broad definition of record types as per the POPIA (e.g. CCTV, biometric)
- Identify Special Information (e.g. Biometric data, Gender information etc.)
- Look at various aspects as required by the POPIA (including consent, purpose, source, sharing, destruction)

- Consider user rights and their management
- Think broadly in terms of the types of devices where data is stored – and represents a security compromise risk

5. Review / draft POPIA compliance policies based on findings

- Review existing relevant policies
- Ensure your policies are reasonable and appropriate
- Make sure your policies are enforceable

6. Review your websites & online platforms

- PAIA Manual availability
- Data security notices
- Implement "best practice" such as Cookie notifications
- Develop and implement your remediation plan

7. Update / create your PAIA manual

- Confirm your organisation needs a Promotion of Access to Information Act (PAIA) manual
- Confirm whether you are a Public or Private Body as per the PAIA
- Review the proposed contents of your manual
- Ensure your PAIA manual follows the prescribed layout and includes the necessary details

8. Implement POPIA compliant PI management processes

- Look at the Personal Information lifecycle: including acquisition, processing, retention, and destruction practices
- Develop reasonable and appropriate measures to ensure ongoing compliance (e.g. Procedure document, self-assessments, health-checks, formal audits)
- Develop your dashboard for monitoring

9. Train internal stakeholders on their roles in POPIA compliance

- Design on-going training according to their needs
- Look to special needs such as the IO/DIO roles

10. Adopt POPIA compliance as "Business-As-Usual"

- Recognise that POPIA compliance will be the "new normal" and work that way
- Build compliance into your products, services and processes – adopt "**Privacy By Design**"

11. Information security Safeguards

- Consider generally accepted information security practices and procedures for both local and international data flows
- Consider electronic data protection tools i.e. Cybersecurity against Ransomware
- Consider means for secure data transfer, storage & recovery
- Revise processes for non-electronic data storage / filing
- Agree on safety practices for both operators and processors of data and manage these through contractual agreement where necessary.