POPIA COMPLIANCE CHECKLIST

MOBIUS CONSULTING
Actualising change

Several months have passed since POPIA came into full effect. As most organisations have progressed in their Privacy journeys, we have updated our POPIA Checklist from 2021 to take you to the next level and ensure you stay on track with your Privacy compliance goals!

1. ASSIGN ACCOUNTABILITY

Register the Information Officer and Deputy Information Privacy Officer(s) with the Information Regulator and provide adequate training on their responsibilities.

2. EDUCATE EMPLOYEES

Complete annual review of the Privacy awareness and training strategy. This must include targeted training for key staff and refreshers for all staff.

3. UPDATE PRIVACY NOTICES

Ensure Privacy notices are reviewed in alignment with the organisation's information handling practices.

4. IMPROVE CONSENT MANAGEMENT PRACTICES AND FORMS

Drive the implementation of improved consent management practices, including updating consent forms as applicable.

5. MAINTAIN PERSONAL INFORMATION INVENTORIES

Implement mechanisms to manage personal information inventories, including providing targeted training to responsible staff.

6. MONITOR COMPLIANCE WITH PRIVACY POLICIES

Ensure internal Privacy related policies are continuously reviewed for compliance, and communication of these is achieved to obtain relevant staff attestation.

7. MAINTAIN A DATA SUBJECT RIGHTS PROCEDURE

Apply mechanisms to timely manage data subject rights requests and run simulation exercises to test effectiveness of these mechanisms.

8. MAINTAIN A PRIVACY BREACH PROCEDURE

Align Privacy Breach Procedure with the organisation's overall Incident Management Practices and a run periodic breach simulation exercise to test the procedure's effectiveness.

9. MANAGE THIRD PARTY RISKS

Adequately train critical personal information handlers in the Third Party management functions to apply the organisation's Third Party Risk Management Framework.

OTHER KEY CONSIDERATIONS IN LINE WITH IMPROVING PRIVACY MATURITY EFFORTS, THE ORGANISATION:

Adopts a **Privacy Strategy** adaptable to the organisation's changing Privacy needs.

Performs **internal and or external Privacy audits/ reviews** to monitor compliance over Privacy controls and measure effectiveness of these controls.

Aligns record retention and destruction requirements with broader **data governance practices**.

Maintains ongoing internal and or external audit/reviews of **Security Safeguards**.

Takes **proactive** steps to drive **Privacy automation** to ensure the manageability of Privacy controls.

Cape Town: +27 21 201 1120 | Johannesburg: +27 10 590 6111 | Email: info@mobiusconsulting.co.za | Website: mobiusconsulting.co.za