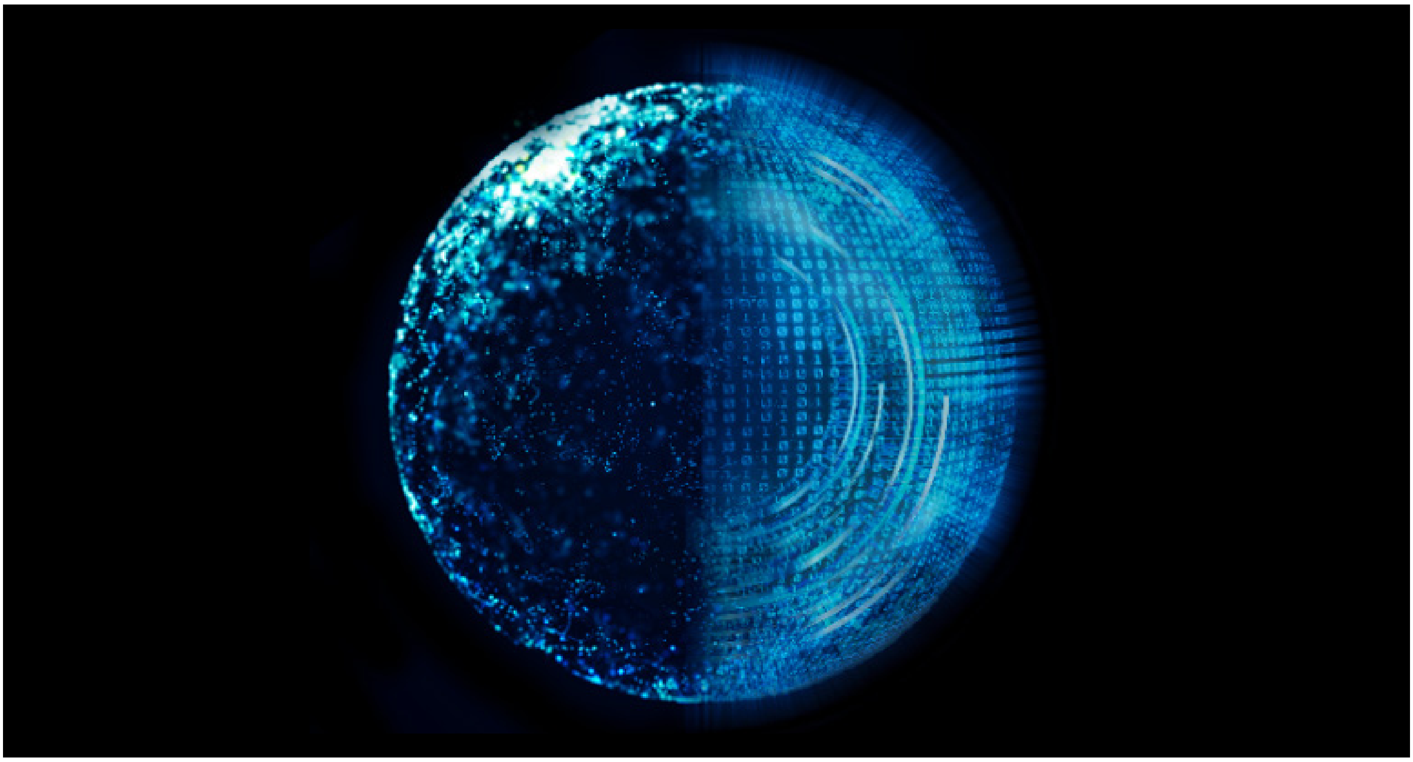
Deloitte.



# What should your organisation be managing in the first 100 days post POPIA compliance

With the Protection of Personal Information Act (POPIA) effective date on 1 July 2021 fast approaching, it is important to identify the key activities and tasks an organisation should be preparing to execute on in order to operationalise an enterprise-wide data privacy programme in the first 100 days.

In addition, organisations should consider certain services and tools in order to support a robust privacy programme that can withstand legal, regulatory and compliance scrutiny. What follows below are some of the activities organisations should be contemplating:

**Privacy Compliance Programme –** By now, your compliance programme should have been established and accountable stakeholders capacitated to bring about compliance. However, in order to maintain ongoing compliance obligations, a privacy programme review and maturity assessment should be undertaken to ensure that the privacy programme is sufficiently designed and implemented effectively to meet the compliance requirements. The purpose of a maturity assessment is to measure the current state of the privacy programme and the programme's ability to meaningfully bring about compliance continuously, across all required domains. Areas identified that have not met the desired maturity, should be prioritised, and be matured systematically to meet the necessary standards.

**Third Party (Operator) Assessments –** A methodology to categorise high-risk third parties, the assessment to which such third parties will be subject, and the necessary documentation required to evidence compliance should already be in place. Ideally the first assessment of high-risk third parties, including the evidence supporting such compliance, should have been undertaken prior to the commencement date. During the first 100 days, a prioritised number of high-risk third parties should be selected for review or audit by the responsible party themselves or an independent third party to determine their actual level of compliance. A process should be implemented to compare the outcome of the review to the initial assessment; and the results incorporated into any risk management strategy moving forward, including strategies to mitigate or remediate areas of non-compliance.

**Privacy Information Impact Assessment (PIIA) –** A PIIA is a vital requirement in terms of the POPIA regulations, the purpose of which is to ensure that adequate measures and standards exist in order to comply with the conditions for lawful processing. A PIIA should be designed and be ready to be executed in the first 100 days, in the minimum targeting high-risk areas in the organisation. Areas of non-compliance should be identified and progress against remediation tracked and monitored to bring about compliance.

**Internal Audit/Independent assurance –** High-risk or prioritised areas of the business that have indicated compliance readiness should be subjected to an internal audit or independent assurance to ensure the relevant measures that have been implemented are adequate and effective. In the case of an annual internal audit, it is important to focus on privacy related controls within the larger audit plan to ensure that areas of non-compliance are given visibility as soon as possible.

**Incident and breach simulation and support services –** A security compromise in terms of POPIA is required, as a matter of law, to be reported to the Information Regulator "as soon as reasonably possible after the discovery of a compromise".

While there is no fixed timeframe associated with the reporting of a breach, "as soon as responsibly possible" requires that the notification to the Information Regulator be made within a timeframe which, objectively measured, was reasonable in the circumstances taking into account the nature of the compromise and the steps required to assess and validate the compromise prior to notification. It is important to note that substantial harm and prejudice may be brought upon the data subject if the notification is not found to be reasonably made in the circumstance, as it deprives the data subject from acting quickly to reduce the impact of the breach, and conversely provides cyber criminals with more opportunity for unlawful activity. The elapse of time during this period is therefore material. Thus, a notification found to be unreasonably delayed will aggravate any consequences a responsible party may be exposed to as a result of the compromise. Thus, it is important that an organisation functions effectively, efficiently and with common purpose during the discovery of a security compromise. Thus, a spontaneous incident or breach exercise, simulating a security compromise should be undertaken to ensure that the organisation can meet the required timeframe and disclosure requirements.

Equally as important are the support services that an organisation would require during this period. These may include external legal support, cyber security professionals and crisis management services. Their role in an organisation's incident and breach response should be clear.

**Metrics, monitoring and reporting –** It is important to ensure that all processes, procedures and protocols regarding the management and reporting of privacy key-risk indicators within an organisation goes live as soon as possible after the commencement date, and subsequently occur at regular reporting intervals. This is to ensure that the relevant stakeholders internally, including the Information Officer, have a regular update of the areas of non-compliance within the environment in order to ensure sufficient resources are diverted to mitigate or remediate risks identified. Horizon scanning for new data privacy requirements should also be implemented to ensure that an organisation can keep up-to-date with new compliance requirements, as data privacy requirements are likely to continue to develop into the future. Continuous monitoring and the enhancement of current capability in the existing programme should be imbedded into the business moving forward.

**Internal Awareness Sessions –** Internal awareness sessions should be executed on an ongoing basis to ensure that all stakeholders within an organisation are sufficiently aware of the requirements of POPIA. Specifically, any new processes that apply post 1 July 2021 should be brought to the attention of all stakeholders as soon as possible. Information security related awareness should be included in this type of training, especially where it relates to appropriate handling of personal information, and how to respond to potential breaches. Typical topics are phishing, protecting personal information, password security and the correct use of multi-factor authentication.

**Identity and access management –** This capability should function to ensure that logical and physical access is controlled and monitored so that only authorised persons access personal information based on their role. This applies to both staff of the organisation and any third parties involved in the processing of personal information. Appropriate identity verification mechanisms should be in place to verify the identity of anyone requesting access to personal information.

**Actively Manage Risks of Non-Compliance –** The risk of non-compliance with POPIA materialises on 1 July 2021. Non-compliance with POPIA carry with it significant legal, administrative, imprisonment and civil penalties; and more broadly consequential reputational damage and losses of business arising therefrom. The need to manage areas of non-compliance effectively becomes critical to avoid such consequences. Section 19(2) of POPIA requires the establishment and maintenance of a risk register which is a powerful compliance tool to guide risk management efforts as it requires the regular identification of risks, and the establishment of effective safeguards in respect thereof; and the continuous update of such safeguards in response to new risks. However, what is important is that this exercise be extended specifically in respect of areas of non-compliance to ensure that compliance activities are accelerated. The risk management activities should include the allocation of risk owners to areas of non-compliance, timeframes to mitigate or remediate the risks, regular monitoring to ensure agreed actions and plans are executed. In the context, any deviations in progress from the agreed actions should result in a readjustment, escalation or reprioritisation to the

**Data Access Rights –** The ability to empower data subjects to exercise their rights in terms of POPIA becomes essential. Data access rights represents a low-water mark to evidence non-compliance by an organisation by not being able to comply with these requests from 1 July 2021. It is therefore critical that roles, responsibilities, systems and processes required to give data subjects access to their information are operationalised.

It is important that POPIA compliance becomes embedded and operationalised as part of the business as usual activities of an organisation as this will reduce the organisation's exposure to the risks of non-compliance; and ensure that the true value beyond compliance is realised by the organisation.

***Deloitte is ranked no.1 by revenue for 2019 in security consulting services by Gartner, the world's leading information technology and advisory company.***

## Contact us:

**Leishen Pillay**
**Associate Director**
**Cyber Risk | Risk Advisory Africa**
Tel: +27 (0)11 209 6418
Email: lpillay@deloitte.co.za