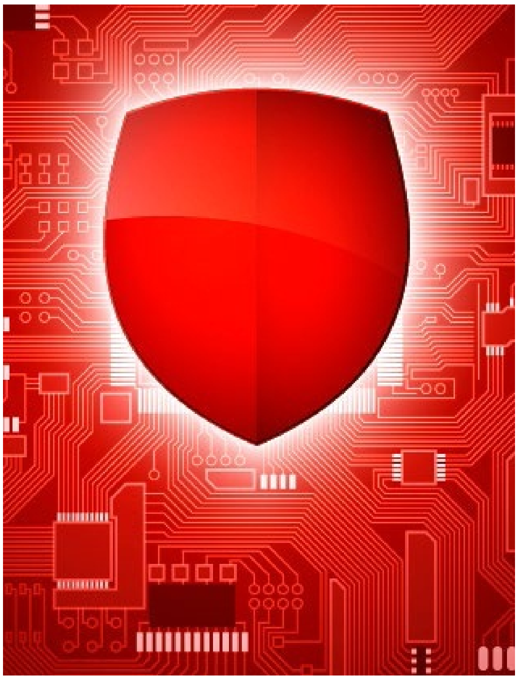
Focus

Data privacy compliance: With a King IV mindset



With a King IV mindset

The Protection of Personal Information Act (POPIA) is South Africa's data privacy legislation which regulates how personal information must be processed from the moment of collection until the moment of destruction to ensure that it is adequately protected and secure. POPIA was enacted in 2013 but a commencement date has yet to be published, after which organisations will have one year to become POPIA compliant before the Act becomes fully effective.

In an era of digitisation and rapid technological advancement, the commercial value of data to an organisation, together with its use, management and protection are key points of discussion around many boardroom tables

The Protection of Personal Information Act (POPIA) is South Africa's data privacy legislation which regulates how personal information must be processed from the moment of collection until the moment of destruction to ensure that it is adequately protected and secure. POPIA was enacted in 2013 but a commencement date has yet to be published, after which organisations will have one year to become POPIA compliant before the Act becomes fully effective.

However, notwithstanding the delayed commencement of POPIA, the concept of data privacy is a global topic and putting effective data privacy measures in place within an organisation sooner rather than later is crucial to achieve good corporate governance and to ensure that the organisation is not left behind from a global data privacy perspective. Many organisations may also already be required to be GDPR (General Data Protection Regulation) compliant. While the focus of this article is on POPIA specifically, the general data privacy considerations and guidelines provided in this article from a corporate governance perspective will also apply to those organisations aiming to achieve GDPR compliance.

Complying with POPIA in a King IV environment

In keeping up with rapid technological advancements coupled with ever-increasing focus, accountability and responsibility being placed on good corporate governance, including the alignment to King IVs principle-and-outcomes-based approach, organisations should consider tackling their data privacy compliance projects with a King IV mindset that embodies King IV's desired governance outcomes of *ethical culture, good performance, effective control and trust, reputation and legitimacy.*

What is a King IV mindset?

The overall theme of King IV is the establishment of an outcomes-based approach towards achieving good corporate governance rather than compliance through a mechanical tick-box approach. An organisation's approach to data privacy should follow the same principle. Data privacy, like good corporate governance, should be enshrined in the organisations culture and should be practised on a day to day basis through effective measures and controls that are put in place to achieve effective compliance, rather than through a tick-box approach that is only considered or reviewed on an annual basis once in place.

King IV's emphasis on technology governance and security

King IV recognises the importance of technology governance and security, which by its nature includes data privacy, and places a responsibility on the organisation, and in particular the organisations governing body, to pay critical attention to this ever-developing, fast-paced area of the organisation.

'Technology governance and security have become critical issues. Technology is no longer simply an enabler; the systems created by an organisation provide the platform on which it does business, and technology is now both the source of many of an organisation's future opportunities and of potential disruption – an excellent example of how risk and opportunity are increasingly two sides of the same coin.

Technology is now part of the corporate DNA. Thus the security of information systems have become critical. Technology governance and security should become another recurring item on the governing body's agenda' (King IV Report Foreword).

Establishing effective control

From a corporate governance perspective, POPIA compliance, in its simplest form, is about taking control of the personal information that an organisation processes, managing it effectively, and ensuring that it is secure.

Although POPIA is limited to the protection of personal information (as defined in the Act), an organisation would, as a starting point, be required to consider all the data that it processes, which includes historical data already in its possession and new data that it collects, stores and processes, in order to determine which data qualifies as personal information and requires protection in terms of POPIA and what measures must be put in place by the organisation to do so.

'You cannot effectively manage and protect your data until you know what data you have, where it is being stored and how it is being processed.'

Effective management and protection of personal information must be addressed throughout the entire data lifecycle, from collection through to use, data retention processes and the ultimate destruction or de-identification of the data once it is no longer required by the organisation or retention is no longer permitted in terms of POPIA.

In practice, the effective management of data can be a daunting and complex task, given the sheer volume of data that is processed by organisations on a daily basis. Organisations should carefully consider tools available to them in the market to assist in mapping out the data that they collect, process and store, to assist them in achieving effective management and control over their data.

Accountability for data privacy

In terms of POPIA, an organisation is accountable for the personal information it collects and processes (as a responsible party) and remains accountable for that personal information even where the processing activities of the data are outsourced to a third-party data processor (that is, an operator in terms of POPIA).

It is essential that the organisation adopts a top-down approach to accountability. The organisation's governing body must be fully engaged in and committed to the organisations data privacy compliance initiatives and to creating a culture of data privacy within the organisation in order to achieve success in its compliance initiatives. Governing body engagement is therefore critical to success and to ensuring that accountability is achieved and that effective control of the organisation's data privacy initiatives is maintained by the governing body.

The importance of training and awareness

Training and awareness is the backbone of an organisation's data privacy culture and its compliance journey as a whole. To ensure accountability for data privacy within an organisation, data privacy training and awareness should be done at every level of the organisation from top to bottom.

Training and awareness is probably one of the most important risk areas when it comes to data privacy readiness within the organisation. Human error accounts as one of the highest areas of risk for data breaches globally and is very often overlooked or overshadowed by the emphasis and effort that organisations place on securing IT infrastructure.

From a corporate governance perspective, an organisation's governing body needs to be in position to provide key input into many of the data privacy initiatives being undertaken by the organisation and to interrogate data privacy compliance initiatives that are proposed by it, to ensure that these initiatives are the best fit for the organisation and are in line with its overall objectives and goals. This cannot be done effectively unless the governing body is aware of the data privacy obligations that the organisation has been tasked with achieving under POPIA.

Training and awareness of employees within the organisation is equally as fundamental. The reality is that in their every-day work, employees deal with, create and receive personal information in various forms. Not only in the systems they work with but also in their every-day interactions via email, instant messaging and verbal/ telephonic conversations.

Training and awareness within the organisation is one of the first steps to creating data privacy compliance readiness but probably doesn't go far enough to mitigate the risks. What is important is to create a *culture of privacy,* ensuring that every employee as well as an organisation's contractors, suppliers and even customers are sensitised to identifying personal information and how it should be managed. It's almost like trying to establish an 'information etiquette' that is as commonly known and as prevalent as good manners.

Privacy by design and privacy impact assessments

Privacy by design is the concept that privacy should be considered and built into all new technology, processes, products and/or services that involve the processing of personal information at the initial design stages and throughout the complete development process.

Although POPIA does not directly address the concept, it is addressed and mandated in the GDPR and should be strived towards to ensure effective compliance.

The drive for privacy by design should be led by the organisation's governing body and should be considered and interrogated with the organisation at the time of the initial approval of the new technology, process, product and/or service to ensure that privacy is considered and placed as a priority from the start.

The organisation's governing body should also interrogate the privacy of third-party products and services that the organisation intends to use and that will involve the processing of personal information, before approval, to ensure that these third party products and services adequately protect the personal information that it is accountable for in terms of POPIA.

Enquiries of this nature will re-enforce the organisation's culture of data privacy by driving it from the top down and will ensure that the governing body is applying its mind to the accountability obligations under POPIA.

Managing the risks of noncompliance and data breach incidents

Data privacy compliance measures should be viewed as risk mitigation measures that are put in place to achieve compliance and reduce the risk of data breaches occurring. However, this must be done with the mindset that these initiatives are risk-mitigation measures and that having these measures in place will not mean that a data breach incident will never occur in the organisation.

Data breach incidents and non-compliance with POPIA can carry both legislative risks and reputational risks. Reputation risks are often far more severe than the financial penalties imposed by law, as they have a direct impact on how the organisation is viewed by consumers and the public at large, which impacts the organisations trust, reputation and legitimacy.

Appropriate measures must be put in place to address how the organisation will handle a data breach incident through a well-planned and practised incident response plan. The incident response plan should be carefully developed, in compliance with the data breach reporting requirements of POPIA, to manage the potential reputational fallout of a data breach incident and take into account the best way of dealing with the incident to safeguard the trust, reputation and legitimacy of the organisation.

The organisation's ability to address the incident quickly is important to reduce reputational risks, and all key resources in the organisation that will play a part in responding to a data breach incident should be aware of the role they are required to play in reacting to an incident, to ensure the efficient roll-out of the incident response plan.

Kicking off your data privacy compliance journey

Wherever an organisation is in its data privacy compliance journey, the governing body's commitment to and participation in that journey is critical. The organisations governing body must play an active role in the organisation's data privacy journey to achieve good governance from a data privacy perspective. Data privacy compliance must also be viewed as an ongoing journey that will evolve over time and should never be seen as a once-off compliance objective.

Creating a culture of privacy throughout the organisation is a critical success factor in achieving effective data privacy compliance readiness and in mitigating the organisation's data privacy risk. As important as it is to have the right leadership buy-in and initiatives in place, data privacy is a core principle that needs to extend beyond the organisations governing body to every employee in the organisation, much like the vision of King IV which has been developed to apply much more broadly through its principles to businesses of any size.

If you have not yet started your data privacy compliance journey, here are a few key steps to get your organisation started:

- **Step 1** Up-skill on data privacy and POPIA. Data privacy is the way of the future, and a topic that the organisations governing body will need to be up-skilled on. Executive Management/governing body training and awareness is required as a first step to ensure top-level buy-in to the process and enable them to properly apply their mind to data privacy compliance and implementation matters affecting the organisation.

- **Step 2** Establish your team and choose your lead. Put appropriate organisational structures and teams in place to take the organisation through its data privacy compliance journey. This will include identifying your privacy information officer, who should lead and drive the project (or identifying the need to recruit one). These teams may evolve as the organisation moves through its implementation journey.

- **Step 3** Key resource and implementation team training. The key resources and implementation teams that will be driving POPIA implementation and compliance must be trained to ensure that they are aware of the organisation's compliance obligations in terms of POPIA and are equipped to drive implementation and compliance.

- **Step 4** Data mapping and gap assessments. An organisation cannot effectively manage and protect personal information data until it knows what personal information it collects and processes, where it is being stored, how it is being processed, who it is being processed by and how is it retained and destroyed. The organisation will need to identify and map out its data processing activities and identify its data privacy compliance gaps.

- **Step 5** Implementation planning, budget allocation and resource planning. Once data processing activities have been mapped out and gaps identified, the organisation can commence its implementation planning. This will include budget planning for infrastructure upgrades that are identified in order to achieve compliance and determining staff resourcing requirements that may be required for the project.

- **Step 6** Training and awareness throughout the organisation. Training and awareness at every level of the organisation on the overall requirements of POPIA and the key components of data privacy that need to be focused on towards achieving a state of compliance readiness is a crucial step and is essential to creating a culture of privacy. Effective training and awareness initiatives will enable every member of the organisation to work towards achieving the organisation's data privacy compliance goals. Training and awareness should also be seen as an ongoing compliance objective to keep the focus of data privacy alive within the organisation and to strengthen the organisations culture of privacy on a continuous basis.

- **Step 7** Compliance implementation. Implementation of all the compliance measures that have been identified, planned, budgeted and resourced should then be rolled out. The responsibility for management and control of the organisation's implementation measures should be driven and overseen by the organisation's appointed privacy information officer in collaboration with the key resources and implementation teams established by the organisation to achieve POPIA compliance readiness.

AUTHORS | Natasha Jansen, Data Privacy and Corporate Commercial panel member at Caveat Legal, in collaboration with Lionel Moyal, Commercial Partners Lead at Microsoft, and J Michael Judin, Partner at Judin Combrinck Inc