Deloitte.

International Data Privacy Day
28 January 2022

A new Era for Data Privacy – POPIA 6 months on

Global Data Privacy Day coincides with the six-month go live date of the Protection of Personal Information Act, 2013 **("POPIA")** in South Africa, introducing a new era of data privacy. Data privacy compliance activities have increased significantly during this period; and continue to gain traction as we move forward. These are some of the themes that have arisen during these first six-months.

Third party risk still being understood – organisations are still in the process of understanding their third-party risk management landscapes. Visibility of third parties, as well as a triage of high-risk third parties and the processes that are to be followed in order to ensure that they comply with the requirements of POPIA are still being implemented. The management of third parties within an organisation, usually intersect with several business functions including procurement, finance and information technology; and requires integration and alignment across the organisation, on a new axis. A robust third-party process to cover both new and existing high risk third parties is a significant challenge for complex, multi-divisional independent businesses within a singular organisation.

Consolidation of disparate parts of the programme – a number of components of a privacy programme are embedded in several areas of the business including legal, compliance, risk management, cyber security and data governance and management. Organisations have diverted significant effort into the consolidation and unification of these components to create an integrated enterprise-wide privacy programme. Organisations have recognised that the allocation of ownership and responsibility in respect of privacy compliance, across the organisation and beyond the core privacy team, is key to the overall sustainable success of the programme.

Establishment of the privacy office – organisations are grappling with the design of their privacy capability. Capacity, roles and responsibilities, as well as integration with the rest of the organisation are being tackled on an ongoing basis. Organisations are recognising that several cross functional, multidisciplinary skills are required to ensure privacy compliance is effective. Most organisations have recruited or trained people to increase their capabilities to manage privacy compliance, but there are still challenges in headcount and capacity of these individuals.

Customer centricity is still in the process of being operationalised – the customer journey is becoming essential to increasing trust and providing consumers access to their information. However, the question is whether POPIA has increase the control consumers have over their information? Privacy programmes have focussed on internal compliance rather than taking a consumer-centric view. Areas such as cookie consent and management and data subject access rights remain key areas for remediation.

Trust is key – Consumers are more likely to share data with organisations they trust. With the continued surge in personalisation, personal information is being used in ever more complex ways. The ethical use of information, which can reside in the grey area between regulatory compliance and a higher standard, is seen as an increasingly important driver in this level of trust.

Privacy is a global concern – POPIA requires countries outside South Africa to maintain minimum processing standards. Focus is beginning to shift to the extra-territorial processing and the management and enforcement of compliance.

Privacy is not a do-it-yourself proposition

- Organisations have a massive list of data elements they want to protect, and lack the ability to prioritise. In addition, they are rarely positioned to tie the value of data elements to the business.
- Extending data privacy programmes to the cloud requires careful assessment of staff skills, processes, and tools. Cloud adoption can take years, leading data protection programmes to consider a hybrid environment of on-premises and cloud applications.
- Data loss prevention (DLP) and cloud access security broker (CASB) tools are not set-it-and-forget-it applications. Out-of-the-box rulesets rarely provide real value without customisation and tuning by experienced engineers.
- Finding and retaining staff with skills to manage technology, and to work with the lines of business to translate requirements into controls, can be difficult.

What's next?

1. **Customer-centricity and ethics**
   Greater awareness from consumers of their rights and how their information is used will provide an opportunity for organisations to differentiate themselves by putting customers at the centre of everything they do with their information. There will be greater focus on the ethical use of personal information as well as complying with the legislation.
2. **Board level scrutiny**
   Given the significant impact that non-compliance can have, coupled with mandatory breach notification, data privacy is going to remain a board-level risk. This means more scrutiny over business as-usual activities and how compliance is being managed, sustained and proactively demonstrated.
3. **Technology and automation**
   The benefit that technology can bring to streamline existing processes is a well-trodden path across many compliance areas. Many organisations have put in place robust, manual processes to manage their privacy risk. These are commonly positioned as a first step in a longer term programme of work that will see more use of automation and technology to make the processes more efficient and reliable. As privacy processes and controls mature, organisations should assess where technology can have the greatest impact and determine which internal or third party solutions, or combination of solutions provide the greatest return on investment.

Contact

Leishen Pillay
Data Privacy Director
Risk Advisory Africa
Tel: +27 (0)11 209 6418
Email: lpillay@deloitte.co.za