KPMG

POPIA Data Privacy Governance Structures

The Protection of Personal Information Act ("POPIA") is relatively silent on the topic of data privacy governance structures and operating models. This state of affairs, on one hand makes it difficult for companies to know definitively, how to create systems that comply with POPIA and on the other hand, gives organisations an opportunity to tailor their privacy governance framework to their needs.

A data privacy governance structure varies from business to business depending on the type of information being processed, the sensitivity and the volume of information. Furthermore, what is required for an international organisation with various branches locally and abroad will vary to that of a small business based locally.

POPIA requires the responsible party ensures that the conditions set out in POPIA and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing of personal information.

There are plethora of factors that determine what an appropriate privacy governance structure and operating model means for a particular firm. We list 5 tips every organisation should be thinking about as it establishes its governance structure:

1. POPIA requires the registration of an Information Officer by default, the role of Information Officer falls to the head of the organisation. We know that most CEOs have more than enough complex business decisions to make and may not have the time to drive privacy at the level required by POPIA, it is therefore important to consider the extent to which Deputy Information Officers and senior management can assist the Information Officer with driving privacy initiatives down within business; echoing the importance of privacy compliance and attending to certain privacy-related actions and queries. It is important that these roles and responsibilities are properly documented to ensure that no balls are dropped and that these individuals are held accountable for their responsibilities.
2. Organisations should consider whether it is appropriate to establish of privacy committees and forums which provide an in-depth level of focus on privacy matters or whether the mandate of existing committees and forums should be enhanced to deal with privacy matters. In both cases, the committee privacy objectives and responsibilities should be clearly documented in terms of reference and an organisation must be able to evidence that these committees/forums are empowered with sufficient management information to make privacy-related decisions. It is also important to document these decisions in the minutes of the committee/forum.

3. Of course implementing appropriate privacy policies and procedures is important however these documents alone will not ensure the success of a privacy programme particularly when employees do not understand the relevance of the policies to their job. Since each employee forms part of the privacy governance structure and has a role to play in managing privacy risks it is important that employees are trained and are aware of their privacy obligations and that job descriptions are updated to include privacy responsibilities that are appropriate for their role and processing activities. Better yet, organisations should consider how they can assess and reward employees who are meeting privacy expectations- particularly where an employee's role poses a high privacy risk.
4. While certain privacy non-compliance (both actions and omissions) will certainly trigger the formal disciplinary process, the "stick approach" will not be enough to cultivate and foster an ethical data culture within an organisation. All organisations should start with considering "what does the 'ethical' use of data mean to our firm and what outcomes do we want to achieve?" and build a data ethics framework with this vision in mind. While one of the framework elements may include training and awareness–organisations will need to a lot more work to achieve an ethical data culture.

Data and more particularly personal information is one of the most important assets for any organisation… It informs and thus allows organisations to evolve, innovate and grow. Used inappropriately or in a non-compliant way, trust can very quickly be eroded, resulting in regulatory censure, reputational damage and financial loss. It is imperative that all organisations implement an appropriate data privacy governance structures and operating models to ensure compliance with POPIA and other privacy legislation.

Contact our Privacy Team:

dataprivacy@kpmg.co.za

Finn Elliot
Associate Director and member of the KPMG Privacy Team
M: +27 79 039 9367
E: finn.elliot@kpmg.co.za

Beulah Simpson
Legal Manager and member of the KPMG privacy Team
M: +27 60 602 3066
E: beulah.simpson@kpmg.co.za

Sharmlin Moodley
Partner and member of the KPMG Privacy Team
M: +27 60 992 4789
E: sharmlin.moodley@kpmg.co.za

Marcelo Vieira
Associate Director and member of the KPMG privacy Team
M: +27 82 718 8485
E: marcelo.vieira@kpmg.co.za