KPMG

Data Privacy Watch

Thought leadership
Issue 1: July 2023

Privacy by design: The cornerstone of addressing privacy risks

The privacy and protection of personal information has been front of mind for many organisations since the enactment of the Protection of Personal Information Act (“POPIA”) in 2013 and its subsequent commencement in July 2020. Most organisations have been scrambling to become “POPIA compliant” within the short transitional period and have not had the time or inclination to “future proof” new technology, processes, services or products from a privacy perspective. That is, they have not been applying the concept of ‘Privacy by Design’ into their business.

The concept of ‘Privacy by Design’, a term coined by Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, Canada, necessitates that data privacy is embedded into every new and/or modified technology, process, service or product that involves the processing of personal information at its inception. The European Union’s General Data Protection Regulation (“GDPR”) provides for the term ‘Protection by Design’. The effects of both concepts are similar.

In terms of the ‘Privacy by Design’ principles, organisations should proactively ensure that appropriate and effective measures and standards exist from the outset to comply with the conditions for the fair, transparent, lawful and secure processing of personal information throughout the lifecycle of the personal information within the organisation. Privacy should be the default setting from the outset – it should not be an add-on or afterthought. Respect for the data subject is paramount, making sure that the measures employed by organisations that process personal information are user-centric is also important.

01

An EU perspective of 'Privacy by Design'

It is an explicit requirement, in terms of the GDPR, that data protection principles should be considered throughout the project lifecycle, from implementation and on an ongoing basis after the new technology, process, service or product has been designed.

In this regard, technical and organisational data protection measures are required to be implemented taking into account (i) state of the art of available technology; (ii) cost of implementation; (iii) nature, scope, context and purpose of processing; and (iv) impact the data processing will have on the rights and freedoms of individuals. Ultimately, the measures deployed by the organisation must be appropriate and effective as assessed against their purpose (i.e., to protect the rights of the individuals whose personal information is being processed in a manner that is compliant with data protection principles). The safeguards that have been identified by the organisation must be integrated into the processing activities to protect the personal information of individuals.

One of the key methods used to give effect to the concept of 'Privacy by Design' is the performance of a Data Protection Impact Assessment (another explicit requirement under the GDPR) when the processing of personal information could result in a high risk to the rights and freedoms of natural persons. A Data Protection Impact Assessment is designed to support organisations systematically in identifying, assessing and mitigating the data privacy risks of new / changes to technology, process, service or product.

02

Are there similar requirements in South Africa?

Although POPIA contains no explicit provisions that are comparable to the GDPR requirements of embedding 'Privacy by Design' into business processes, Regulation 4 of the POPIA Regulations places an obligation on Information Officers to complete a Personal Information Impact Assessment ("PIIA") to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information. The PIIA process is analogous to that of the Data Protection Impact Assessment.

Organisations would do well to be cognisant of all prevailing privacy principles from the onset of a new technology, process, service or product, as opposed to the challenge of "unscrambling the egg" by implementing privacy measures retrospectively once the technology, process, service or product is already embedded in business. Failing to consider the privacy risks that may exist, and appropriately managing and mitigating such risks, can have significant consequences on business. A consistent, reasonable and proportionate methodology to assess how personal information will be processed within business will enable organisations to focus on creating systems that comply with POPIA and simultaneously mitigate against any privacy risks which may be present.

There is no definition in POPIA or the POPIA Regulations defining the PIIA. However, in our view it is an important tool that should be used to assist Information Officers in identifying privacy risks in respect of any new and/or modified technology, process, service or product that involves the processing of personal information and would trigger that data privacy controls and measures are taken into the design thereof on a proactive (rather than reactive) basis.

At a minimum, the PIIA should assess the sensitivity of the personal information processed, the nature of the processing being performed with the personal information, the risks that the processing of the personal information will have on data subjects, and the measures that will be taken to ensure compliance with POPIA and to mitigate against the identified risks.

The Information Regulator has yet to provide guidance regarding when a PIIA should be conducted or the minimum subject matter to be considered in performing a PIIA. In the absence of such clarification from our Information Regulator, we consider it prudent for Information Officers to:

01 Develop a template PIIA that can be completed in respect of any new and/or modified technology, process, service or product where the nature of the processing of the personal information is likely to constitute a 'high risk' to the rights and freedoms of data subjects .

02 Develop an internal procedure and process for conducting PIIA which defines:

- When a PIIA must be performed
- Who is responsible for completing the PIIA
- Methodology to be applied by the Information Officer in assessing the PIIA
- What are the approval processes
- What are the risk acceptance protocols that may need to be invoked

This will ensure that there is a consistent approach to performing a PIIA within an organisation and a clear understanding of when a PIIA should be performed by the organisation.

03

How KPMG are assisting Information Officers

The KPMG Data Privacy team has leveraged off international best practice within its global privacy network to create a PIIA solution that will streamline the assessment in any sized organisation, thus protecting one of the most important data sets in a business – personal information.

We have created straight forward PIIA templates and procedures to support Information Officers in discharging their very important obligation in the POPIA Regulation in a consistent and reasonable manner.

We understand that the Information Officers' responsibilities are onerous and, more often than not, are an "add on" to their existing roles and responsibilities. We also offer managed service assistance to Information Officers by supporting with some of the key day-to-day activities required of an information officer – including assessing completed PIIAs.

KPMG

04

About the KPMG Data Privacy team

This article was written by **Nada Ford** and **Fathima Rawat,** who are both privacy lawyers. Nada and Fathima form part of the larger KPMG Data Privacy team, led by Beulah Simpson and Finn Elliot, consisting of privacy lawyers, information security experts, risk management and change adoption specialists, with deep knowledge, experience and understanding in data privacy.

Nada Ford
Legal Manager
Tax & Legal
T: +27 11 647 7111
E: nada.ford@kpmg.co.za

Fathima Rawat
Legal Manager
Tax & Legal
T: +27 11 647 7111
E: Fathima.rawat@kpmg.co.za

Beulah Simpson
Associate Director
Tax & Legal
T: +27 606023066
E: beulah.simpson@kpmg.co.za

Finn Elliot
Legal Partner
Tax & Legal
T: +27 79 039 9367
E: finn.elliot@kpmg.co.za

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia