KPMG: POPI takes effect

Monday, 14th April 2014; It has now been announced that certain sections of the Protection of Personal Information Act (POPI) came into effect on 11th April 2014. The relevant sections deal with the establishment of the information regulator, the procedure for making regulations and the nature of the regulations which the Information Regulator may make with regards to POPI (including how complaints will be submitted, investigations, administrative fines and the responsibilities of the information officer of a company), amongst others.

The fact that the provisions allow for the establishment of the Information Regulator before the remaining provisions of POPI become effective means that companies cannot rest on a belief that the establishment of the regulator will cause further delays with regards to the implementation of this legislation.

POPI aims to give effect to the constitutional right to privacy of consumers by introducing measures to ensure that organisations process personal information in a fair, responsible and secure manner. The legislation covers why and how they collect, use, disclose and store personal information belonging to natural and juristic persons.

Graham Teare, head of KPMG's privacy multi-disciplinary team in South Africa, says, "Globally, we are seeing a move to enforcing privacy protection, with significant regulatory fines in the cases of non-compliance."

All companies, that process personal information, are required to comply with POPI. Non-compliance has serious consequences, such as fines and possibly, prison terms, and most significantly reputational risk.

"Organisations should not underestimate the potentially negative effect of a non-compliance on the company's reputation," says Teare. "The consequences of a tarnished reputation, including customers' loss of trust in the organisation could far exceed the effects of a fine."

Nikki Pennel, KPMG legal privacy specialist, acknowledges that most companies have some sort of privacy standards and processes in place. However, she suggests that organisations conduct an analysis identifying gaps in their current state of privacy readiness for compliance with POPI.

"Critical to the gap analysis is identifying practical strategies which can be implemented easily and are aligned to the operations of business," explains Pennel.

Teare suggests that "POPI should be considered from a number of perspectives - legal, business processes, systems and overall governance, amongst others."

Complying with POPI is challenging as proven in the Breaches of Privacy and

Loss of Data Survey, conducted by the Ponemon Institute (using 2012 data), on breaches of privacy in the United Kingdom. The survey identified negligent employees or contractors (37%), system and business process failures or glitches (29%), malicious or criminal attacks (34%) as root causes for data breaches.

“Companies therefore need to ensure that their current processes, employees or contractors and systems can handle the potential demands POPI could place on them,” cautions Teare. “The Act should not be viewed in isolation. It provides a broad framework but must work in conjunction with other industry-specific legislation which touches, to some extent, on data protection.

“POPI requires a dedicated team of specialists with a full complement of privacy experts to assist clients navigate the new legislation,” explains Teare. “An effective POPI team should comprise of specialists from Corporate Law, Information Technology, Regulatory Compliance team and Forensics. The POPI solution will have to be commercially-focused, client-centric and practical.”