The practical effects of POPI

Hogan Lovells

December 2016
Without Prejudice

Legislative developments currently afoot in South Africa are set to change the way in which businesses outsource their technology operations. These changes will have an effect on the way in which businesses interact with their outsource service providers, with the most substantial effect being that businesses have to take on more responsibility and accountability in respect of the personal information outsource service providers' process.

Once the highly anticipated Protection of Personal Information Act, 2013 (POPI Act) comes into effect, there are several key aspects that will have to be considered by businesses intending to outsource technology operations or in relation to its impact on a live outsourced environment. Chief among these aspects is section 19 of the POPI Act, which introduces new standards in respect of the implementation of security safeguards.

Section 19 of the POPI Act marks a drastic departure from the current largely unregulated IT security landscape in South Africa. POPI legislates the creation and maintenance of a risk register specifically to identify potential risks that affect processing of personal information in businesses. While this in itself may not be new for many businesses, section 19 goes on further to legislatively require businesses to regularly review, verify and update responses to identified risks by the taking of appropriate, reasonably technical and organisational measures.

South African business may have been advised, at one point or another, to transfer onerous obligations in respect of data protection onto their outsource service provider. There are various reasons for this approach.

Primarily among them is the fact that it is the business of the outsource service provider to protect information, and consequently it would be in a position to adopt and apply data protection standards more readily than the business itself. Of course, the cost of that compliance would be shouldered by the outsource service provider and not the business. This approach, in many instances, has separated businesses from the processing of their personal information. In many instances, this has resulted businesses to be unaware of any risks posed to that information, whether threatened or actual. Fortunately, the POPI Act prevents this type of reallocation of responsibilities by including provisions that specifically address the manner in which outsource service providers are to process information, specifically the risks identified by the business itself in terms of section 19.

Section 21 provides that a business must establish and maintain the security measures referred to in section 19. Where there are reasonable grounds to believe that personal information has been accessed or acquired by unauthorised persons, the outsource service provider must notify the business immediately. This notification requirement is currently not provided for in our law and requires special attention in that the application of the standard of reasonable grounds is objective and quite onerous and robust in legal terms. The notification obligation is mirrored by a reciprocal obligation on businesses to notify the Information Regulator and, in certain instances, data subjects of such a breach. Section 19 ensures that businesses take the lead in managing the processing of personal information, despite this being undertaken by an outsource service provider.

The practical effect of sections 19 and 21 of the POPI Act is that both the business and the outsource service provider require the continued application of resources and effort to ensure that personal information is protected and processed lawfully as intended by the POPI Act. One of the direct consequences of the application of section 19 is that businesses will be compelled to record, and address appropriately, the various risks and factors giving rise to cybercrime. This obligation is conspicuous by its absence from the current South African legislative landscape, and has led to the unchecked and rampant rise of cyber and related crime levels.

In light of the onerous obligations placed on businesses by the POPI Act and the serious penalties that may be levied against a business for non-compliance (damages claims and fines of up to ZAR10 million), businesses should obtain a greater understanding of their information technology environment and become prescriptive in respect of their information processing requirements.

The POPI Act will not only change the way in which businesses process and outsource personal information, it will revolutionise the way businesses engage with their own personal information. And this, in the end, is the point of the POPI Act.

As published in Without Prejudice in December 2016.

> Read the full article online