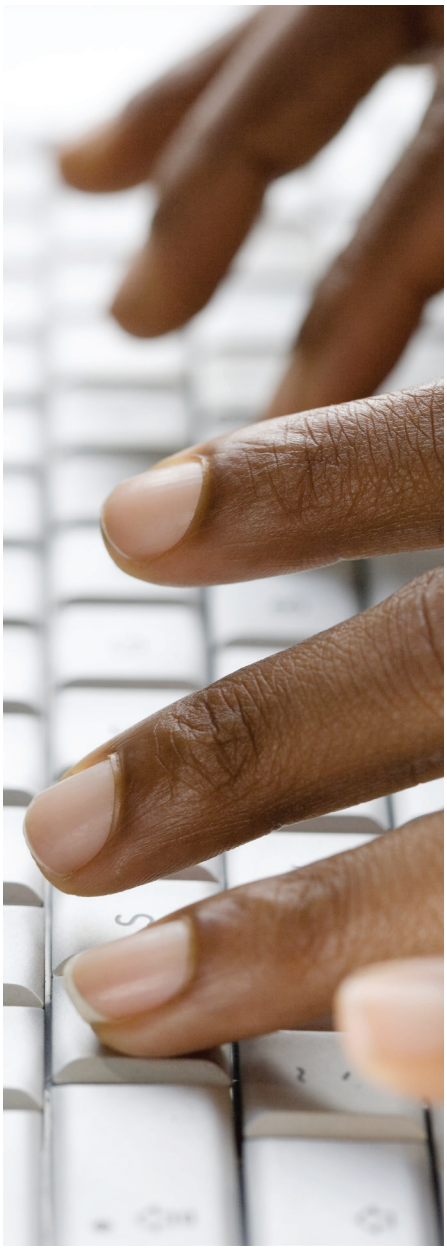
What happens if we violate PoPI?



What is PoPI?

The Protection of Personal Information Bill (PoPI) is likely to be enacted later this year. The bill defines 'personal information' in the broadest possible terms, including 'juristic persons' (i.e. legal entities such as companies) in its definition, requiring that information relating to identifiable natural or juristic persons must be safeguarded and its collection and use limited to specific purposes. PoPI gives individuals the right to object to those uses, on reasonable grounds, and to ask that their information be deleted.

How might violations of or non-compliance with PoPI be discovered?

Firstly, we should understand how such non-compliance might come to light. The most likely source would be the individual 'data subject' themselves, via a complaint to the 'Information Regulator' (which will be created once PoPI is enacted). It is therefore very important for organizations to address data subjects' concerns or complaints as quickly and thoroughly as possible.

The next most likely source would be from organizations themselves. There is a requirement in PoPI for organizations to notify the Information Regulator and the data subjects of any compromises of their personal information. Such compromises would include the hacking incidents often heard of (Sony Playstation network breach that compromised 100 million individuals' information), or lost or stolen laptops containing personal information, but also incidents such as misdirected faxes, paper records thrown in the rubbish without shredding, employees inappropriately accessing information for personal (or more nefarious) reasons, and so on. When organizations notify the Information Regulator or data subjects of such compromises, as required by PoPI, it is likely that an investigation will be initiated.

The third means by which non-compliance might be discovered is if the Information Regulator spontaneously initiated a review or investigation of an organization's compliance, which they are empowered to do under PoPI. The Regulator will likely identify high-risk and/or high-profile organizations and initiate reviews of their practices to ensure compliance.

If an organization fails to comply with or violates PoPI, what are the consequences?

Having conducted an investigation, determined an organization lacks compliance with, or is violating PoPI, the Information Regulator is empowered to formally enforce PoPI in four ways. It should be noted that, overseas, Regulators have initially taken an 'informal' approach to enforcement when their legislation is newly-enacted, provided that the organization is cooperative and has tried to comply. Our Regulator may take a similar approach in the initial year or two.

The Regulator is empowered to levy administrative fines on organizations of up to R10 million. Based on foreign enforcement actions, the amount of the fine is likely to vary in relation to various factors, including: the extent to which the organization has diligently attempted to comply with the law; their cooperation with the investigation; the number of individuals impacted by the incident; and the likelihood or actuality of harm to those individuals. Fines are likely to be on a 'per-incident' basis but, as is the case overseas, also applied on a 'per-individual-affected' or a 'per-provision-of-the-law/regulation-that-was-violated' basis.

The Regulator may also choose to pursue criminal prosecution, the result of which are fines of up to R10 million, as per above, but also prison terms of up to 12 months. In the event that an individual or organization wilfully obstructs an investigation (and similar transgressions), prison terms can be up to 10 years.

The third enforcement power of the Regulator is potentially the most threatening to organizations: they may issue an "enforcement notice" requiring the organization to stop processing personal information. The scope of the order can vary from one individual's information to all personal information processed by the organization. It can be restricted to a department, division, or cover an entire business and conceivably even a group. Naturally, such an order has the potentially for immense disruption and even possibly closure of a business.

The fourth power of the Regulator is to initiate a civil action on behalf of an individual or group of individuals. While many class-action lawsuits have been initiated in the US in reaction to data breaches, they have not succeeded due to the inability of the plaintiffs to prove financial harm. Whilst our law provides for damages for financial harm, unlike the US, our law also provides for damages for non-financial harm, opening the door to claims for emotional distress and lost time while changing ones information due to identity theft, etc.

What should organizations do?

Thus far, the banking industry has been the leader in South Africa in initiating compliance activities, with the insurance and retail industries becoming involved more recently. As this Bill affects all South African companies and has substantial impact on many functional areas of the business, including operations, HR, IT, and procurement, it behoves organizations to:

1. Establish a multi-functional steering committee
2. Provide awareness training
3. Conduct a gap assessment
4. Plan and budget for implementation of their privacy program

Contact details:

Russell Opland

IT Risk Advisory

Russell.Opland@za.ey.com | 083 601 1472

Thagraj Moodley

IT Risk Advisory

Thagraj.Moodley@za.ey.com | 071 895 8736

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com

Studio ref. 130522. Artwork by Sewpersadh.