THE PROTECTION OF PERSONAL INFORMATION ACT WAS SIGNED INTO LAW IN NOVEMBER: 8 PRACTICAL TIPS TO GET YOU COMPLIANT

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Lucien Pierce | December 12, 2013

The president signed the Protection of Personal Information Act ("**POPI**") and it became law on Wednesday 26th November 2013. POPI essentially regulates how anyone who processes personal information must process, keep and secure that information. It may have taken over eight years to complete, but the final result is a good piece of legislation.

As much as it has been signed into law, POPI isn't effective yet. The president still has to decide on the commencement date. If this sounds confusing to those non-lawyers out there: the date when an Act is signed into law and the date when it actually applies, can be different.

There's another aspect to when POPI's provisions begin to apply. Not only do we need to wait for a commencement date, but POPI also gives everyone an additional year from the commencement date to comply with its requirements.

The fact that everyone who processes personal information still has more than a year to make arrangements to comply, shouldn't make us complacent.

POPI is a good piece of legislation but is also strict and has substantial penalties. Anyone who contravenes POPI's provisions faces possible jail terms and fines of up to R10 million. POPI also allows individuals to institute civil claims so there's the possibility of further financial loss on top of any fine that may be imposed.

So what can anyone who processes personal information do to ensure that, when the one year grace period is over, they are POPI compliant? You should, as a bare minimum consider doing the following:

- Read the Act. It's not a highly technical piece of legislation. It is long though, so if you have time constraints focus on chapter three. It sets out eight conditions for the lawful processing of personal information.
- Give some thought to the type of personal information you process and how your processing complies with the eight conditions in chapter three. A spaza shop and a huge medical aid scheme could both possibly process personal information but the sensitivity of the information and what POPI would expect of each would be very different.
- Consider whether your organisation's operations warrant information security awareness training for your staff. For example, your staff would need to be trained on the simple confidence tricks, such as a phone call to an unwitting staff member, that are often used to access personal information.
- Train your staff on laptop, data storage and mobile device security. Put processes and procedures in place to limit who can access certain information on those devices and your organisation's computer system.
- Ensure that laptops and other mobile devices have passwords and similar security and are preferably encrypted. Try to implement systems and software that allow lost devices to be remotely "wiped clean". An unencrypted back-up disk that Zurich Insurance lost in South Africa, cost it a fine of 2.3 million British pounds. You should draft policies dealing with each of these issues and educate your staff on them.

- Look at the physical security of the premises where you store the personal information that you process. Do you have reasonable security measures in place such as access control, burglar bars, CCTV and alarm systems? Assess these physical security measures in the light of the type of personal information you process (remember: spaza shop versus medical scheme).
- Assess whether any service providers who process information on your behalf, have considered and implemented each of the five points above. Put proper contracts in place that compel your service providers to give you assurances that they will also comply with POPI.
- Given the potential for huge financial losses, consider whether your organisation would be justified in securing cyber insurance. Your current “generic” insurance policy is not likely to cover losses arising out of a data breach by your organisation.

Your organisation has more than a year to make changes that will help it comply with POPI. If you start attending to them now, you should be fully compliant by the time POPI starts showing its teeth.