PoPI requires effective data management structures

By Claude Schuck

31 Oct 2017

The Protection of Personal Information Act (PoPI) will fundamentally change how companies store, process and use personal customer data. And even though it has not yet officially been implemented, organisations have been steadily working on ensuring their compliance to avoid future penalties. But with the one year grace period soon to begin, are businesses taking it seriously enough and starting to act?

© kantver via www.123rf.com

Part of the problem is the fact that while PoPI has been signed into law in 2013, delays in passing draft regulations and getting feedback have resulted in some organisations putting a low priority on their adherence to the act. However, the requirements to comply with PoPI are comprehensive.

For businesses yet to act, fortune had been on their side. In August, the Information Regulator published draft regulations and issued a call to all interested parties to provide comments. The deadline for feedback is 7 November 2017, signifying one of the final steps before PoPI comes into effect and the grace period can start.

Despite this, the hype cycle around PoPI seems to ebb and flow as the media attention grows and dissipates. In certain respects, the growth of data and the pressure to have it always-on and available, combined with a startling number of global cybersecurity breaches have helped refocus efforts around compliance over the past twelve months.

Your IT needs a wake-up call - maybe PoPI is it

Pieter Engelbrecht 13 Oct 2017

Companies understand the value of data in addition to being able to access it irrespective of location or device used. The digital world means data has become fundamental to build competitive advantage and gain insights on everything from buying behaviour, customer preferences, conversion rates, and customised offerings.

Securing data

The traditional way of looking at data, its availability, and security would simply be to have backups in place. But backups mean very little if they are not easily accessible, the frequency with which they are done is low, and the quality of backup is poor. Ultimately if the company is unable to restore data from them, what's the point doing them?

> *"With PoPI placing a lot of attention on availability, frequent testing becomes vital to ensure backups are encrypted and kept in secure locations whether in the cloud, on premise, or a combination of the two."*

In many respects, the 3-2-1 backup rule will come under renewed attention because of this. It states that you need to have three copies of your data, stored on two different media types, with one being offsite. Following this approach enables the business to take a vital step towards compliance to PoPI and other regulatory requirements being delivered globally, including the European Union's General Data Protection Regulation (GDPR), which has requirements on any business with European customers.

Mobile bugbear

Thanks to the growth of mobile and the increased adoption of smart devices to do business while away from the office, enterprises are seeing the value of using analytics and related business intelligence offerings to gain value from their data. And while mobile has contributed to the growing importance of data, it has also unwittingly become one of the biggest loopholes around adhering to regulations.

Not many companies consider the value of data stored on mobile devices as critical if they are lost or stolen. Yet, these smartphones, tablets, or other devices still contain intellectual property that could significantly impact the business if it is compromised.

Database of 30 million+ South Africans leaked online, property group is culprit

Ilse van den Berg 19 Oct 2017

And this is where acts like PoPI in South Africa and GDPR in the European Union fulfil vital roles in aligning what needs to happen around data management and best practice of implementation. With the GDPR grace period ceasing in May next year, Gartner says the threat of fines of up to €20 million or four percent of annual global turnover, for breaching articles in GDPR means companies in Europe are seriously re-evaluating measures to safely process personal data.

The steps these organisations are taking to ensure compliance mirror those of South African companies who are pushing to get themselves ready for PoPI. Aspects like understanding how personal data is currently being processed and how it needs to change under new legislation, considering appointing a data protection officer focused on all aspects of compliance, and understanding cross-border data flows must become part of the standard operating procedure.

Structuring data management

Irrespective of the pressures to adhere to legal requirements, data management in the connected world is all about putting the structures and processes in place to ensure data is kept safe and managed properly. For this to work, organisations need to be more open towards continuous benchmarking and testing their data management strategies. This will contribute to a more structured approach and ensure compliance with all aspects of acts like PoPI are adhered to. In real terms, this data management should already be happening.

If the PoPI regulation was currently operational, an organisation suffering a data breach due to theft or cyberattack would have a case to answer should it be found that it did not take adequate steps to protect the data, or if its security defences were inadequate in protecting such highly confidential information.

So often regulations are a ‘nice way’ of ensuring companies across industry sectors behave in a proper and respectful way. PoPI ensures organisations understand the need to protect data whether on-site or on the mobile devices of employees. And, while some decision-makers might be excused for rolling their eyes and thinking that PoPI is something that might never materialise, the business benefits of managing data effectively mean there are significant returns to be had by embracing compliant measures.

Make no mistake though, the sooner institutions start with the process in order to properly comply with this legislation, the better their situation will be.

ABOUT CLAUDE SCHUCK

Claude Schuck is the regional manager for Africa at Veeam.

- Compliance requires an evolved availability approach - 16 Apr 2018
- Prioritise keeping your Bitcoin safe, secure, and available - 16 Mar 2018
- #BizTrends2018: Welcoming a new era of availability - 22 Jan 2018
- PoPI requires effective data management structures - 31 Oct 2017
- Addressing the risks of data loss - 11 Sep 2017

View my profile and articles...