Snap, crackle, POPI

The Protection of Personal Information Act (POPI) is like that DIY chore at home you keep putting off that eventually escalates and becomes a very costly problem.

SVEN HUGO

An Internet meme has a cartoon dog with big floppy ears sitting on his wooden chair at a table, contently sipping tea in a room licked by flames, with a speech bubble that reads: "This is fine, I'm ok with how everything is unfolding right now."

We don't have to explain the analogy, but speaking to compliance experts in the financial services industry, those POPI flames are closer than many in the industry care to think. KPMG's POPI specialist and attorney Nikki Pennel says that following the recommendations of the National Assembly, the publication of the effective date of the substantive provisions of the Act is likely to follow soon.

Companies know it's coming, government has indicated that the commencement date is close, after which companies have one year to comply, but many of the finer details are still lurking in the background. The regulation is bigger than you can imagine.
"Everybody thinks it is the 'protection of personal information', therefore it only applies to human beings, but there are many other jurisdictions, including the information of juristic persons, like a company for example, that need protecting," says Robby Coelho, Webber Wentzel's technology, media and telecommunications group head. It completely changes the application. "It entails literally every bit of information that a company holds, not just your customers but also shareholders and suppliers," he adds. "It has a 360-degree impact on an organisation."

And this complexity in the compliance programme is going to cost you.

Coelho says that companies should do a full compliance restructuring, and not just focus solely on POPI, to avoid duplication. "These programmes require a lot of dedication, time, resources, personnel, expenses and so forth. If a company is going through a process of compliance with POPI, it makes sense to be doing a full information law compliance project," he says.

The regulatory framework of POPI is equally relevant to other laws, and a complete compliance plan will safeguard you against breaking another compliance law by only focusing on POPI. For instance, if you destroy invoices after a specific amount of time, as per POPI regulations, you could inadvertently be breaking another labour law, which would require you to keep the invoices for several years. "Some labour laws require you to keep records for up to 40 years," explains Coelho.

Make hay

So when should companies start with compliance processes? Yesterday, says Coelho. "In our experience, 12 months is not nearly enough and many of our clients have been busy with the compliance processes for several years," he warns.

The first step for companies is to initiate a gap analysis to assess how much the entire process is going to cost, including the expenses of advisers and technology that you may have to purchase. "The sooner you do, the sooner you can budget for it," says Coelho. Companies don't have to do the full implementation but at least do the gap analysis and then make a call, he adds.

IN OUR EXPERIENCE, 12 MONTHS IS NOT NEARLY ENOUGH AND MANY OF OUR CLIENTS HAVE BEEN BUSY WITH THE COMPLIANCE PROCESSES FOR SEVERAL YEARS.

POPI has been years in the making and if timely preparations are made it should not be an unrealistic task, says Charles Stretch, MD of SMSPortal.

Partner with a service provider who understands your business and can commit long-term and help with compliance for the 12-month period, says Eugene Wessels, MD of Genasys Technologies. "Don't partner with a vendor who merely sells you a solution and then leaves the responsibility with you to become POPI-compliant," he warns. "It has to be an end-to-end service provider."

Wessels explains that the entire solution needs to be analysed as an all-inclusive project, from the call-centre operations through to the application, management of sales leads, client information, premium collection process, to the back-end offering of backups and archiving. Then there are also the technological aspects such as the encryption of software, as the loss of a laptop or cellphone with client information on could result in heavy fines for any business.

The amount of work required in achieving POPI compliance is often underestimated by companies, agrees Juan Thomas, chief information officer at PBT Group. It is not a legislative project in isolation but in fact calls for an enterprise-wide approach to not only deal with implications for systems or data management but for employees too.

Steve von Roretz, executive director at Leppard Underwriting, says this legislation will create new exposures that require the need to review liability that will attach, without the need to demonstrate negligence, on the part of the holder of the information.

Take note

The key risk is the security safeguard of data, notes Coelho, because of the sheer disruptive nature of a data breach that affects not only the real subjects but also the company's reputation. The reputational financial losses far outweigh potential law suits from clients, he says. If you take care of the technical and operational safeguards, you indirectly comply with the rest of the act.

The POPI team has to be represented by every functional wing of the company. It must comply with HR, IT, finance, supply chain, marketing, business development … the entire company. "Typically, the compliance officer doesn't understand or have the authority to implement the project throughout every division," says Coelho.

POPI compliance requires ongoing monitoring, so organisations need to appoint an information officer (in fact, all organisations require one in terms of POPI), establish processes and set up systems (if they do not have them) to ensure that data is constantly secured, new data is appropriately handled, and old data is destroyed, says Alison Treadaway, director at Striata.

The approach in data utilisation for data-driven companies increases the importance of a good, but flexible, data governance process, says Thomas from PBT. Companies are adopting hybrid architectures to make use of cloud services, which immediately raises issues of POPI compliance. "These structures are driving POPI from an implementation point of view but not always from an end-user. It is here where POPI should be approached from an enterprise-wide view, making use of IT, legal and POPI professionals," he says.

Local asset disposal specialist Xperien CEO Wale Arewa warns that companies should be extremely cautious when appointing asset disposal service providers. "Very few companies offer IT asset disposal (ITAD) as a core function. There are about 50 operators in the industry providing ITAD services but they range from scrap metal dealers, printer repair and service companies to managers supplying after-hour services and moonlighting to their businesses."

Companies also have to keep in mind that POPI is not just law and order pressed on businesses by a paternal regulator, as there are benefits for the company too.
"There are opportunities to improve existing systems as well as dealing with change management and end-user behaviour," says Thomas. These include business process evaluation, enterprise data model enhancements, data quality improvement, updates of data security policies and service provider contracts.

"Dealing with these opportunities allows a company to involve a larger group of people to participate in the implementation of POPI controls, which creates a larger pool of buy-in but also, more importantly, awareness," concludes Thomas.