Technology wont solve POPI problems

The Protection Personal of Personal Information Act (POPI) is often mistakenly compared to Acts such as Consumer Protection, and subsequently not taken very seriously. This is a grave mistake and could cost a company, most especially an SME, a big loss in revenue says Drew van Vuuren, CEO of 4Di Privaca.

Drew van Vuuren, CEO of 4Di Privaca

POPI has been signed into law, and businesses should therefore be taking this particular Act seriously, giving it the respect and notice that it deserves.

POPI holds organisations liable for the security of their customer's information, and because most, if not all, businesses deal with personal data in some way or another, whether it is employee or client information, all businesses are affected. In the EU the fine for contravening data privacy is £85 million, indication that globally data protection is taken very seriously, and with POPI signed into law, businesses should beware, as South Africa is not far behind.

Technology plays a role in the remediation component of the POPI requirements. Systems like Data Loss Prevention, Encryption, Database Management Tools and Access Governance go a long way in assisting organisations to meet remediation gaps, however, technology should not sit alone as a solution, and is no silver bullet for adherence to the Act.

Technology will not be able to address the myriad of challenges dictated by the principles laid out in the Act. For example, principle seven in the Act deals with information security, which is not only about technology; it consists of people, processes and technology, and businesses relying too heavily on the technology component tend to falter when considering the requirements to comply under POPI. User behaviour is a prime example of where technology cannot solve the challenge - security awareness and defined policies on how user's process personal data will address this.

The biggest challenge for organisations is knowing where the personal data is being processed. Data owners are spread through an enterprise, and managing a co-ordinated process of data capture, analysis and archiving, is difficult if not impossible. Although technology can assist with this process, ensuring authoritative data sources are the biggest challenge

when understanding where an organisation has placed personally identifiable information.

Organisations electing to ignore the POPI requirement should beware of the dangerous implications. The gamble could result in both financial as well as reputational loss, risking business closure through liabilities imposed by the regulator and the loss of confidence from suppliers, customers and peers in the industry.

The role of POPI in any organisation should be assigned to a business function defined as data protection. There is a requirement for a data protection officer, and it should be this resources responsibility to manage the compliance process, represent the business to the regulator and be the contact point for data subjects who are querying the business on the data they hold on them.