3 steps to POPIA compliance

The African Union's Convention on Cyber Security and Data Protection (known as the Malabo Convention) outlines principles which urge all AU member states to respect and protect individuals' rights to privacy online and offline.

© tumsasedgars – 123RF.com

Multiple member states have already ratified the Malabo convention or put in place data protection laws and South Africa has become the latest African country to legislate the protection of personal information, with the country's Protection of Personal Information Act (POPIA) in South Africa that came into effect on 1 July 2020.

Along with countries including Kenya, Botswana and Nigeria, South African organisations must now move to comply with new regulations to protect identifying and personal information it collects, stores and manages.

Global best practice in the protection of personal information will become increasingly important as pan-African trade picks up, and as African countries seek to boost exports internationally.

However, compliance with pan-African and global data privacy, security laws and regulations can be a daunting task for any organisation. Especially since requirements are often vague and ambiguous, with little specific guidance as to how to achieve compliance. According to a 2019 survey conducted by Sophos, only 34% of South African organisations are

reportedly ready to comply with POPIA.

So where should you begin? Here are three simple steps to help you get started:

1. Start with a business privacy impact assessment

Condition seven of the South African POPIA Act ("Security Safeguards") requires organisations to take "appropriate and reasonable measures" to safeguard personal information. The concept of acting "reasonably" is used in many privacy laws all over the world and requires a business to do what is appropriate to protect its data. Note that this does not require perfection. Rather, the business must take a risk-based approach and do what is reasonable to mitigate that risk. By conducting a business privacy impact and risk assessment, you'll identify privacy risks in your organisation and come up with a plan to either remediate or accept them.

2. Prioritise your high-risk processes

High-risk processes should always come first. Start with client/customer personal data and work your way towards employee personal data. This will involve collaboration with many departments, so executive buy-in is a must; and privacy compliance should be pitched as business enablement.

3. Drive an awareness campaign

Employees need to be made aware of and get trained in the security requirements of the organisation, as well as learn about the basic privacy principles and best practice, and how to apply these at work. Security awareness training for employees is one of the most effective means for reducing the potential for costly errors in handling sensitive information and protecting company information systems.

Requirements around data protection can seem tedious, but they provide the foundation for trust in the digital environment and there are plenty of resources to assist with training around POPIA, GDPR and other privacy and cybersecurity content.