October 29, 2020

Practical steps to comply with the POPI Act

South Africa's Personal Information Act 4 of 2013 (POPI Act) commenced on 1 July 2020, giving businesses 1 year to comply.

In a previous blog article titled *'Final POPI Act Regulations published - what you should know',* we discussed a few steps that can be implemented to secure the integrity and confidentiality of personal information.

The purpose of this blog is to highlight the "appropriate reasonable technical and organisational measures" that businesses can implement in terms of section 19(1) of the POPI Act which will be essential for compliance.

Which security safeguards would be regarded as appropriate?

Section 7 of the POPI Act relates to security safeguards. It requires businesses to secure the integrity and confidentiality of personal information by applying security practices and procedures that protect the business against information threats and vulnerabilities.

Section 19 of the POPI Act is aimed at preventing the loss, damage or unauthorised destruction of personal information by identifying the personal information risks to which the business is exposed to and how these risks are mitigated and managed.

- Businesses should consider whether their current measures will leave the personal information in their possession or control vulnerable to loss, damage and unauthorised access.
- Businesses should therefore take reasonable steps appropriate to the type of information being processed, the size of the business as well as the cost and time relating to the implementation of these measures.
- *Certain industries may have additional requirements for safeguarding personal information, such as the medical industry.*

What are reasonably foreseeable risks?

Section 19 of the POPI Act goes further to explain that the *reasonably* foreseeable internal and external risks are identified by an external audit to implement Information Security management systems, standards or frameworks.

- This will establish where the vulnerabilities in the business lie, and which safeguards to implement. These safeguards can range from technical solutions, such as firewalls, anti-virus and encryption, etc., to practical implementation of policies and procedures for processing information and preventing data breaches. In the global economy it is becoming increasingly important to focus on cyber security, which should also be included in these policies and procedures.
- This section also requires businesses to verify whether these measures are effective and updated on a regular basis.

It is important to note that if the business, in its capacity as the responsible party, outsources certain services, they will still be responsible for protection of the information even though the third party further processes such information.

Conclusion

The POPI Act will ensure that all businesses adhere to the compliance requirements by ensuring that they take “appropriate, reasonable, technical and organisational measures” to prevent the loss and unlawful processing of personal information, which will include onsite audits, assessments, amendment of agreements with certain suppliers and training of staff.

SERR Synergy assists businesses in compiling Data and Information Protection Reports. Our professional legal team ensures that physical information and *cybersecurity risks of organisations* are identified and managed to maintain the confidentiality, integrity and availability of data. We provide organisations with various policies to ensure compliance in such a way that it adds business value to our clients and allows for improvement in efficiencies and effectiveness.

***About the Author*:** Retha van Zyl completed her BCom (Hons) in Economics and Risk Management at the North West University. She joined our team in January 2016 and currently holds the title 'Information Compliance Advisor'. She specialises in POPI and PAIA compliance, which includes compiling and submitting PAIA Manuals to the Human Rights Commission. She also compiles the Data and Information Protection Report to identify risks associated with information security and drafts Information Security policies for procedural compliance in each department within an organisation.

Sources:

https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

http://popisolutions.co.za/popi-security-safeguards/

https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/corporate/popi-bumper-special-alert-30-june.html