May 2, 2018

What businesses need to know about POPIA and the GDPR

How will the POPI Act and the European General Data Protection Regulations (GDPR) impact businesses in South Africa?

In a progressively connected world, the protection of personal information and data has become a main concern for legislators in a number of jurisdictions.

The right to privacy of each South African citizen, including juristic persons such as companies, closed corporations, etc. is entrenched as a human right in the Constitution of South Africa, 1996.

Businesses operational in South Africa are presently facing the enactment of the *Protection of Personal Information Act 4 of 2013* (POPIA). *POPI legislation* will soon come fully into effect with its main objectives being to control the processing of personal information and data protection in a robust effort to align all South African data protection laws with international standards. An Information Regulator has already been appointed and is gradually becoming involved in matters relating to information security breaches.

As many South African businesses are already in the process of implementing systems to ensure *POPI compliance*, they cannot afford to ignore the **European General Data Protection Regulations (GDPR)** to be implemented soon**.** South African businesses are barely coming to grips with POPI and must now also get their heads around the implications of the European privacy and data protection legislation. This week, we are answering the most important questions that businesses may ask relating to this burning topic.

What is GDPR and what are the implications for South Africa?

The GDPR is a new privacy and data protection law adopted by the European Parliament early in 2016. It has many similarities with the POPI Act (POPIA) and various other privacy laws globally. It aims to safeguard against any data and privacy breaches in a new global milieu where business has become entangled with technology and most data is conveyed electronically.

- Businesses operating in South Africa need to take cognisance of the fact that the GDPR applies in EU member states, as well as data transfer to or from the EU. It simply means that the GDPR applies to businesses that are not established in the EU but offer services or goods to EU-based citizens (*either free or paid*) and to websites or any other related online services accessed by EU-based individuals, predominantly in the country's local language.
- It also applies to any organisation that holds or processes data on EU citizens, regardless of where it has is its headquarters, including South Africa. It is therefore extremely relevant to South African businesses who engage in business with persons in EU member states, especially those that import or export goods or services from or to European counterparts.

POPIA and the GDPR

South Africa’s main data protection law, POPI, was enacted in 2013. Since then, certain provisions of the Act relating to the establishment of the Information Regulator and regulations under POPI have come into force. The full POPI Act will take effect once a date has been determined by the President.

The European Parliament set a two-year grace period implementation of the GDPR after it came into effect on 25 May 2018. The Information Regulator will most likely be guided by the implementation of the GDPR in order to determine the commencement date for POPI, with a one-year grace period for implementation.

The GDPR is seen as the international gold standard for protecting personal information and will impact on compliance obligations and monitoring and also advise all international stakeholders.

- ***GDPR states:*** “The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected”.
- ***POPIA states:*** “A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures”.

Why should we be concerned about the GDPR?

A key fact is that if we are not prepared to be compliant in order to do business with companies in European countries, we might be seen as a high-risk country from a personal information protection perspective in the case of those companies who need to be compliant.

Non-compliance with GDPR

The GDPR and POPI Act have similar definitions, conditions and principles. The GDPR covers the same fundamental rights but is far more extensive.

There are severe consequences for GDPR non-compliance, including a fine of up to 4% of an organisation’s annual global turnover or EUR20 million (whichever is greater). This may have devastating consequences for non-compliant organisations. In contrast, POPI’s penalty for non-compliance is a fine of up to R10 million or 10 years’ imprisonment.

Conforming to the legal framework to be in line with the GDPR will therefore be crucial for all South African businesses. The effect is that all South Africans will understand the value of personal information and start implementing measures to safeguard personal information as an organisational asset, taking the operational costs, technical measures and risks into account. The South African Information Regulator will start monitoring and enforcing the POPI Act to enhance cross-border cooperation and international harmony. Given the imminence of the ***25 May 2018 enforcement deadline***, it is now the time to get started with all compliance initiatives, and the same can be said for compliance with POPIA.

South African companies are encouraged to take the necessary steps to ensure compliance with POPI, which will also to a large extent ensure compliance with the GDPR to avoid unnecessary exorbitant statutory sanctioning. Compliance is inevitable. It doesn't have to be complex. Business owners should engage with the right people to assess their businesses and assist with the development of an implementation strategy based on best practices that will streamline compliance.

About the Author: Retha van Zyl completed her BCom (Economics and Risk Management) studies at the North West University. She joined our team in January 2016 where she currently holds the title of 'Information Compliance Advisor'. She specialises in *POPI and PAIA Compliance*, which includes compiling and submitting PAIA Manuals to the Human Rights Commission. She is operationally involved with the POPI auditing process for our clients. She also compiles and implements *Information Security Management Systems (ISMS)* where she identifies the risks associated with information security in each department within an organisation.