THE IMMINENT PROTECTION OF PERSONAL INFORMATION ACT

Caryn Myers is the Managing Partner at Myers Attorneys. She completed her BA Honours in Political Science at the University of Natal, and an LLB through UNISA. Caryn specialises in commercial law, with a broad range of services within the Commercial, Compliance and Empowerment law space. She thrives on providing innovative, tailor-made solutions, based on best practice, with a full understanding of the continuously evolving regulatory and business environment she operates in.

The Protection of Personal Information (PoPI) Act was signed into law on 26th November 2013. Once the Act becomes effective, organisations will have a one-year grace period to comply with the requirements, unless the Act extends this grace period.

In 2014, the President signed a proclamation declaring some parts of the Protection of Personal Information Act No 4 of 2013 effective as of 11th April 2014:

- A Section 1;
- B Part A of Chapter 5;
- C Section 112; and
- D Section 113.

The Regulator will be responsible for the education, monitoring and enforcement of compliance, as well as handling complaints, conducting research and facilitating cross-border cooperation. Adv Pansy Tlakula was appointed as the Information Regulator, effective 1st December 2016. The Regulator released an invitation to comment on the Draft Regulations relating to the Protection of Personal Information on the 8th September 2017.

POPI, WHAT'S THE BIG DEAL?

In July 2013, McAfee estimated that cyber-crime cost the global economy between $300 billion and $1 trillion per annum. In comparison, the global statistics for piracy are approximately $16 billion, with drug trafficking estimated at $600 billion.The South African economy is not exempt when it comes to cyber-crime, as it costs the economy around R6 billion per annum. This amount increases year-on-year.

What these figures indicate is that cyber-crime is an international threat. What makes it worse is that this type of a crime is difficult to combat. The primary reason is that countries are increasingly resorting to legislation that converts the "lack of accountability to prevent the crime" as a criminal offence; enter the PoPI.

The best analogy is that of a physical burglary. Essentially, what PoPI does is turn lax and irresponsible behaviour, such as not having burglar bars on windows or alarm systems in the home, into a criminal offence.

Our increasing dependence on information has brought new risks, which further highlights the right to privacy that is enshrined in Section 14 of our Constitution. The ever-increasing ability to process increasingly large volumes of personal information about individuals has for some time has been identified as a risk area.

Organisations might query why they should invest effort and resources to secure personal information when so many people freely flaunt their information on social media networks? The simple answer is the inherent right to privacy. It is a person that has the right to choose how their information is used or shared, not that of a third-party. PoPI legislation fundamentally respects that right to privacy.

Upon PoPI coming into effect, organisations will be duty bound to safeguard personal information. However, similar reference is made in the Companies Act. It states that business must be conducted with the degree, skill and care which may reasonably be expected. In this respect, POPI merely provides the framework or the enforcement of these rights, in particular to the processing of personal information.

Safeguarding the integrity of Information

The first thing to do is to understand the law surrounding POPI requirements, as well as technologies that exist to ensure the safeguarding of information. This includes establishing policies and processes to govern the proper use of such technologies and to ensure that employees are properly trained to adhere to the policies and processes. Without such safeguards in place an information management system would not comply with PoPI.

PoPI defines personal information as a wide range of data pertaining to individuals and juristic persons. PoPI is not confined to electronic information, as it includes information on paper as well as text. Furthermore, PoPI differentiates between the different types of personal information and the sensitivity thereof, which has greater protection under the law. More sensitive information is referred to as 'special information', which is defined as, inter alia, religious beliefs, health data, trade union membership, political persuasion or criminal behaviour of a data subject.

The jurisdiction of PoPI is any person or entity that collects, uses or stores, in any manner whatsoever, personal information. PoPI has been built upon eight conditions of compliance for lawful processing of information.

1 **Accountability**	An organisation is accountable for the lawful processing of the personal information it collects, stores and disposes of
2 **Processing Limitation**	Information processed must meet four criteria: 1. Fit the purpose it was collected for – no more, no less; 2. Collection of data should not infringe on people's privacy; 3. Consent from the person that the information may be processed is required; and 4. Data must be sourced directly from the person, not through a third-party;
3 **Purpose Specification**	Personal information can only be collected for a specific purpose, then used for this reason only. It may only be utilised for the initial purpose of collecting this information. The person in question must be made aware of the reason the information will be processed and stored;
4 **Further Processing Limitation**	If it is necessary to share information with a third-party, it can only be done as a continuation of the original purpose – not for any other purpose.
5 **Information Quality**	It is the responsibility of an organisation to ensure all data and information is accurate and complete. Only necessary information maybe collected, and it can only be kept for the minimum required time;
6 **Openness**	If an organisation is registered in terms of PAIA, in other words, has complied with the requirements of the Promotion of Access to Information Act, then that organisation will not need to inform the person of its intention to process personal information before processing it. Such an organisation would have submitted a Section 52 access to information manual, which states what information an organisation can keep and exactly how people can access the information.
7 **Security Safeguards**	Organisations must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures.
8 **Data Subject Participation**	People whose information is held by a particular organisation retain the right to interact with them regarding this information. For example what the information is required for, the duration the information will be held. They further have the right to request such information is deleted. Evidence of such interaction must be kept on record.

Organisations will be compelled to ensure that the person - juristic or otherwise - to whom the personal information relates to is aware of the actual purpose for which the information is collected. Importantly, organisations are obligated to notify affected people of any compromises to their personal information, including loss, theft, unauthorised access or disclosure, hacking incidents, to name but a few.

What is the penalty for non-compliance? Why should an organisation comply with the requirements of PoPI?

On the allegation of a breach, the regulator could fine a perpetrator up to R10 million, depending on circumstances and sensitivity of the information. Note, a fine becomes payable upon the allegation; there is no burden of proof required to make it an offence. The only recourse to avoid a fine is to opt to be tried in court. Other penalty risk factors are civil claims and class action.

In conclusion, PoPI is imminent. While its requirements may demand significant resources from an organisation, there may be benefits such as improved reliability of internal data or an opportunity to interact with clients. On a personal note, telemarketing without explicit approval will be a thing of the past. Essentially, it is the availability of personal information that drives cybercrime, an issue which affects all of us. Some advice, approach PoPI holistically, not in isolation.

Source of Reference:

1 *http://www.justice.gov.za/legislation/acts/2013-004.pdf*