August 11, 2020

Guidelines on the implementation of Protection of Personal Information (POPI) Act - by Gideon Gerber

Countries all over the world have in the past 10 years developed policies and legislation to regulate the flow of information.

This process was prompted by a variety of international factors such as the 9/11 attacks in the USA, international terrorism, human trafficking, illicit flow of money, increase in cyber offences, etc.

Millions of white-collar (office) workers were forced into a remote working environment amid Covid-19 and this trend is largely expected to become the “new normal”.

The extended use of technology outside the traditional physical workplace has substantially increased the risk of individuals and businesses having their personal information syphoned off for ulterior purposes. It is estimated that every individual or business in South Africa has personal information that is held in some or other form by another entity which is not the owner (data subject) of such information. This is necessitated by routine commercial and engagement activities such as buying from entities, opening accounts (cell phones, banks, etc.), confirmation of residential addresses and the need to provide other personal information for a variety of reasons.

The need to protect an individual or business's personal information has over the years gradually gained importance and momentum. South Africa has been lagging behind the international trend to timeously implement legislation in this regard. Consequently, South Africa has witnessed an exponential increase in personal information transgressions, with one of the highest levels of personal information breaches globally.

Some businesses in South Africa adopted a policy and stance whereby they only implement information protection and compliance measures once legislation is in place compelling them to do so.

What is the POPI Act timeline?

The POPI Act, which was enacted as law by Parliament (Legislature) way back in 2013, assigned the power to determine the implementation date of the Act to the President. The President has adopted an approach to implement the Act in three stages.

- **Stage 1 -** The first stage was implemented 2 years ago, with the commencement of the provisions and chapter of the Act providing for the appointment of the Information Regulator and conferring on him/her the power to develop regulations and other codes of conduct as precursor to full implementation of the Act.
- **Stage 2** - The bulk of the provisions dealing with compliance matters applicable to all businesses and persons (responsible parties) who are in possession of and process the personal information of other persons, has now been promulgated for implementation on 01 July 2020 as the second phase.
- **Stage 3 – Stage 3 of the implementation process is due in June 2021 and deals with the amendments to other legislation to be effected based on the implementation of the POPI Act.**

What are the requirements for responsible parties?

- **Section 19(1) of the Act** requires all responsible parties to *"secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent–*

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information".

- **Section 19(2)** further places an obligation on a responsible party to identify internal and external risks; establish and maintain appropriate safeguards; regularly verify the safeguards; and ensure that the safeguards are continually updated.

- **Section 19(3)** requires a responsible party to adopt generally applicable security practices to safeguard personal information in his or her possession or under his or her control.

Responsible parties are given a period of 12 months as from 1 July 2020 to implement the above measures to protect and safeguard personal information and become fully POPI compliant.

Understanding the role of the Information Regulator

The Information Regulator has been assigned the power to enforce both the POPI and PAIA (Promotion of Access to Information Act) legislation.

The Information Regulator also has extensive and wide-ranging powers to enforce the information legislation, namely to–

- receive complaints about non-compliance;
- to conduct investigations;
- summons persons to testify and produce documentary evidence;
- issue a compliance notice; and
- hand down administrative fines not exceeding R10 million.

An administrative fine for non-compliance has the same effect as a civil judgement. The Regulator may, in the event of non-payment, apply for a writ of execution against the movable property of the errant party, which must then be carried out by the sheriff. Such an administrative fine equates to a civil judgement adversely affecting the credit status of a person contravening the Act and, in terms of the Credit Act, disqualifying such person from accessing credit at financial institutions.

Another interesting development with regard to the POPI Act is the provisions in section 99 which offer an aggrieved party additional remedies to claim damages caused by the errant party. An aggrieved party has the option to claim damages in his or her own name as usual or, alternatively, request the Regulator to claim damages on his or her behalf. The latter option will in effect be without any legal cost for the aggrieved person. Under normal circumstances, any claimant suing for damages in a civil delictual matter must be able to prove that the respondent had acted with a degree of negligence or recklessness (*mens rea*).

The POPI Act dispenses with the general delictual requirement of *mens rea* and follows an approach to establish liability for damages without the respondent having acted in a negligent or reckless way. This form of liability, referred to in law as “strict liability” (absence of *mens rea*), is also the approach provided for claims lodged in terms of the *Consumer Protection Act.*

Contravening the POPI Act

A contravention of the POPI Act constitutes a criminal offence by the business entity, which offence is imputed to the directors of a company in terms of section 332 of the Criminal Procedure Act. This means that directors of an errant company can be held liable and be prosecuted in their personal capacity for the contravention of the Act by the company as legal entity in which they are appointed as directors. This principle also applies to Close Corporations, sole proprietors and a partnership operating an enterprise.

The Act therefore holds far-reaching implications for the business and the individual directors of a business.

The services provided by SERR Synergy in terms of *our Information Compliance service offering ensure that businesses comply with the prescriptions of section 19 of the POPI Act* alluded to above, as well as the annual updates of the risk assessments as further required by section 19.

About the author: *Gideon Gerber* is a director of SERR Synergy (Pty) Ltd, an admitted High Court attorney with the qualifications B.Juris (Unisa), B.Proc (Unisa) and LLM (Pret.) with a Master's dissertation titled: *An Appraisal of the Offence of "BEE fronting" in the context of Broad-Based Black Economic Empowerment (B-BBEE) in South Africa.* He has more than 30 years' experience in Business Structuring & Compliance, Training, Skills Development and Business Compliance in South Africa, the UK and Namibia. He is a regular speaker at various B-BBEE seminars and also writes articles for the Business Day and Landbouweekblad that concerns BEE Matters. He also published an article titled *Criminal liability requirements of the new Broad-Based Black Economic Empowerment (B-BBEE) statutory offence* in the Journal of Contemporary Roman-Dutch Law (THRHR) August 2018.