

A Date with Data Destiny

The Imminent Commencement of South Africa's Protection of Personal Information Act

By Rui Lopes (Managing Director, Lopes Attorneys Inc., South Africa)

With the rapid rate of technological change occurring within economies throughout the globe, the value of personal information has increased astronomically, as personal data is ever-increasingly mined, traded and monetised, which has brought with it real fears by both companies and individuals on the manner in which such personal information is stored and processed. Even more concerning is that data breaches are on the rise globally, in terms of which this personal information is then stolen and utilised for ulterior purposes. Globally, there is a shift by Governments to enact legislation regulating, *inter alia*, the processing and storage of such personal information, as well as the steps required to be undertaken by data processors, where personal information has been compromised.

South Africa is no different, having enacted the Protection of Personal Information Act, 4 of 2013 (**POPI**), which is South Africa's main piece of legislation, based off to a large extent on the European Union's General Data Protection Regulation (**GDPR**), and is aimed at protecting the personal information of persons, which personal information is obtained and processed by institutions (both public and private). In doing so, POPI attempts to balance the rights to one's privacy, as enshrined within the Constitution, with other rights operating parallel to this, including the rights to access to information.

Although throughout the lifecycle of POPI, there has been much uncertainty in the past as to when all of the provisions of POPI would become effective, this has now been resolved, with the effective date having been announced last year as 1 July 2020. That being said, however, the provisions of POPI afford data processors (responsible parties) with a grace period of 1 (one) year to ensure full compliance with the provisions of POPI, meaning all data processors (responsible parties) would need to be fully compliant by no later than **1 July 2021**. Accordingly, data processors (responsible parties) have a little less than 5 months to ensure that they are fully POPI compliant.

The provisions of POPI have established a number of conditions, which data processors (responsible parties) are required to comply with in order to lawfully process personal information of persons (data subjects). These conditions are (i) accountability, (ii) processing limitation, (iii) purpose specification, (iv) further processing limitation, (v) information quality, (vi) openness, (vii) security safeguards and (viii) data subject participation.

Moreover, the provisions of POPI establish a regulatory body, called the Information Regulator, which has been established to oversee the implementation and adherence to the provisions of POPI. POPI requires that data processors (responsible parties) appoint an Information Officer, who will ensure that their respective organisation is compliant with the provisions of POPI.

Non-compliance with the provisions of POPI may very well result in financial penalties being imposed upon the data processor (responsible person) by the Information Regulator, as well as periods of imprisonment (where applicable). Additionally, non-compliant data processors (responsible parties) stand to suffer extreme reputational impacts for non-compliance with the provisions of POPI, which is especially prevalent in light of the increase in data breaches.

Industries which are to be most impacted by the provisions of POPI include telecommunication companies, financial services, the healthcare industry, private security as well as those entities which process large amounts of personal information as a main aspect/feature of their day-to-day operations.

There is, however, a silver lining for data processors (responsible parties). As indicated above, the provisions of POPI are similar to those of GDPR, which would mean that there is no strict need for data processors to re-invent the proverbial wheel, where they have worked towards GDPR compliance. That being said, however, data processors (responsible parties) would be required to make sure that the nuances present in the provisions of POPI are complied with in order to ensure full compliance with the provisions of POPI.

Accordingly, data processors (responsible parties) would be well-advised to seek expert advice on the active steps required to be undertaken in ensuring that they become fully POPI compliant, prior to the lapsing of the grace period.