South Africa: data protection legislation

Data protection in South Africa is regulated under the broad constitutional right to privacy, the common law and a few pieces of legislation that contained interim provisions relating to data protection. Until very recently, South Africa did not have data protection-specific legislation.

With the increase in electronic commerce globally, large industries managing computerised databases of millions of individuals' records and the surveillance potential of computer systems, prompt demands for specific rules governing the collection and handling of personal information arose.[1] Commissioned in 2005 and completed in 2009, the South African Law Commission finalised an investigation into privacy and data protection in South Africa, with a recommendation that privacy and information protection be regulated by general statute.[2]

The South African Law Commission's recommendation resulted in the creation of the Protection of Personal Information Act (the "Act"). Although signed into law in November 2013, April 2014 marked the partial commencement of the Act with only several sections coming into force, including those related to the establishment of the information regulator, the issuance of regulations to the Act and the definitions clause which, in the latter instance, codified concepts crucial to data protection including "processing" and "personal information". The commencement of the former sections is indicative of the processes being put in place by the government of South Africa to ensure that the commencement of the remaining sections is met with the relevant support, in the form of regulations and the establishment of the information regulator. Outside these sections, the remainder and indeed the material aspects of the Act are not enforceable and have no foreseeable or determinable effective date.

Recognising that a failure to have sufficient data protection is a barrier to international trade, and that the specific obligations in article 25 and 26 of the European Data Protection Directive stipulate that personal data should only flow outside the boundaries of the European Union to countries that can guarantee an "adequate level of protection", the Act draws on data protection principles applied in the European Union, among others, in order to ensure that South Africa can provide "adequate" protection, as gauged from an international perspective.[3]

As a result, the core of the Act consists of eight conditions for the lawful processing of personal information that closely resemble data protection principles utilised in the European Union. These conditions include accountability, process limitations (fair and lawful processing), purpose specification, further processing limitations, information quality, openness, security safeguards and data subject participation.

The Act applies to the "processing" of "personal information", the latter being constructed widely to include information related to the gender, marital status, race, age, health, religion, conscience, belief, language, financial, criminal and employment information, addresses, fingerprints, personal opinions and private or confidential correspondence of a person. The Act covers the processing of personal information by individuals, private and public entities, all of whom are considered "responsible parties" in terms of the Act. The Act also encapsulates the operations of subcontractors of responsible parties, who process personal information for or on behalf of the responsible party, as well as responsible parties not domiciled in South Africa but who make use of automated and non-automated means of processing, situated in South Africa.

By exception, the Act does not apply to the processing of personal information, solely for personal or household activity, that has been de-identified to the extent that it cannot be the re-identified again, by or for the state and for national security, defence or public safety, for exclusively journalistic purposes by persons subject to a professional code of ethics with its own rules for the protection of personal information and as may be exempted by the information regulator.

The Act contains various enforcement and punitive mechanisms to incentivise compliance. From an enforcement perspective, the Act provides for the establishment of an information regulator whose powers and functions include monitoring and enforcing compliance with the Act, the handling of complaints,

1 The South African Law Reform Commission, Project 124 – Privacy and Data Protection Report 2009 page vi.

2 Id. at viii

3 Id. at vii

the issuance and regulation of codes of conduct, and the facilitation of cross-border cooperation. Obstruction of the information regulator or a failure to comply with a compliance notice issued by the information regulator may lead to an administrative fine or a period of imprisonment of up to 10 years. An administrative fine may not exceed ZAR10 million.

The Act also empowers a data subject to institute a civil action for damages against a responsible party for breach of any of the conditions, whether or not there was intent or negligence on the part of the responsible party (strict liability). The Act limits the number of defences that can be raised by the responsible party in response to such claim including force majeure or that compliance with the condition was not reasonably practicable in the circumstances.

Responsible parties will have 12 months from the commencement of the Act within which compliance must be achieved. ■

Leishen Pillay
Senior Associate, Johannesburg
T +27 11 523 6273
leishen.pillay@hoganlovells.com