
Mark J Calaguas
SOUTH AFRICAN PARLIAMENT ENACTS COMPREHENSIVE DATA PROTECTION LAW: 
AN OVERVIEW OF THE PROTECTION OF PERSONAL INFORMATION BILL

Mark J. Calaguas*

After several years of deliberation since its introduction in 2009, the national assembly of Republic of South Africa passed the Protection of Personal Information Bill (“POPI”)\(^1\) on August 20, 2013.\(^2\) The act will come into force upon President Jacob Zuma’s signature, which is anticipated sometime before the start of 2014.\(^3\) While the South African constitution guarantees the right to privacy, POPI is the first comprehensive law that addresses information privacy and data protection,\(^4\) thus declaring in its preamble “the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.” Certain activities impacting information privacy, such as direct marketing\(^5\) and freedom of information,\(^6\) are already subject to government regulation under previously enacted statutes. The information privacy framework established by POPI contains stricter measures that in some cases supersede data protection requirements already in force.\(^8\)

The process of drafting standalone data protection legislation having been first initiated by the South African Law Reform Commission in 2003,\(^9\) the recently approved POPI states its purpose as “safeguarding personal information when processed by a responsible party,” while at the same time considering “the right of access to information” and the protection of “important interests, including the free flow of information within the Republic and across international borders.” “Responsible parties” encompasses entities both in the public and private sectors, while processing refers to the collection, receipt, recording, organization, collation, storage, updating or modification,

\* Mark Calaguas is an attorney and Certified Information Privacy Professional (CIPP) based in Chicago. He graduated with a B.A. with Distinction from the University of Michigan and a J.D. with Certificate in International Law and Practice from Loyola University Chicago School of Law.


3 Aplin, supra note 2.


5 Protection of Personal Information Bill, Preamble.


9 Aplin, supra note 2.

retrieval, alteration, consultation, use, dissemination, distribution, merging, linking, blocking, degradation, erasure or destruction of “personal information,” which denotes identifiable information that relates to living natural persons or existing juristic persons. Categories of personal information covered under POPI include:

a) race, ethnicity, national origin, gender, sexual orientation, age, marital status;
b) medical history, physical and mental health, pregnancy status, disability, biometric information; and
c) educational, financial, criminal, and employment history; and
d) physical address, email, telephone number, location information, online identifier, or any identifying number or symbol; and
e) personal views, opinions, and preferences (including religion, belief, conscience, culture, and language); and
f) the views and opinions of other individuals about a person; and
g) private or confidential correspondence sent by a person, as well as further correspondence revealing the contents of the original correspondence.

Generally, POPI provides that data subjects, i.e. those persons to whom the above information relates, have the right to be notified that their information is being collected and shall be allowed access to that information and have it corrected or deleted, as appropriate. Furthermore, data subjects must be informed whenever their personal information has been accessed or acquired by unauthorized parties. Keeping in mind the aforementioned rights accorded to data subjects, POPI warrants that responsible parties may process personal information if they abide by eight conditions:

1) Accountability: Responsible parties must ensure that all conditions are met at the time when the purpose and means of processing are determined, as well as during the actual processing of the information itself. (Practically speaking, this means that companies should appoint personnel to monitor compliance and respond to privacy complaints.)

2) Processing Limitation: Information must be processed lawfully and in a reasonable manner that does not infringe the data subject’s privacy.

3) Purpose Specification: The collection of personal information must be for a specific, explicitly defined, and lawful purpose that is related to the responsible party’s functions or activities.

---

11 Id. at § 1.
12 Id.
13 Id. at § 5.
14 Id.
15 Id. at § 8.
17 Id. at § 13.
18 Protection of Personal Information Bill at § 9.

2
4) **Further Processing Limitation:** If information is to be processed more than once, it must be compatible with the purpose for which the data is collected.\(^{19}\)

5) **Information Quality:** Reasonably practicable steps must be taken to ensure personal information is complete, accurate, not misleading, and updated as necessary.\(^{20}\)

6) **Openness:** Responsible parties must document their personal information collection practices and notify data subjects about the facts as well as the purpose behind their collection of data, including third-party transfers, among other things.\(^{21}\)

7) **Security Safeguards:** Responsible parties must secure the integrity and confidentiality of personal information by taking appropriate and reasonable technical and organizational measures to prevent the loss, damage, or unauthorized access or processing of data.\(^{22}\)

8) **Data Subject Participation:** Data subjects have the right to access their personal information, including a right to request that the information be corrected or deleted, as warranted.\(^{23}\) Subject to valid consent and other exceptions, responsible parties may not process certain categories of “special personal information”\(^{24}\) or personal information relating to children.\(^{25}\)

In addition, responsible parties may not transfer personal information to third parties outside of South Africa unless: (1) the third party recipient is subject to laws, binding corporate rules, or contractual terms that provide an adequate level of data protection that is substantially similar to that found in POPI; (2) the data subject consents to the transfer; (3) the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject’s request; (4) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or (5) the transfer is for the benefit of the data subject and (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer, and (ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.\(^{26}\)

Notably, POPI also contains specific provisions relating to direct marketing activities, an issue that has already been the subject of earlier legislation.\(^ {27}\) Under POPI, a responsible party may not electronically process the data subject’s personal information for direct marketing purposes unless (1) the data subject gives consent, or (2) the data subject is an existing customer of the responsible party.\(^ {28}\) In other words, businesses can send electronic marketing communications (such as emails, faxes, and automated telephone calls) to an individual who is not already a customer only if the individual “opts in” to receive such correspondence.\(^ {29}\) Direct marketing laws currently enacted

---

\(^{19}\) Id. at § 15.

\(^{20}\) Id. at § 16.

\(^{21}\) Id. at § 17-18.

\(^{22}\) Id. at § 19(1).

\(^{23}\) Id. at § 23-24.

\(^{24}\) Id. at § 26 (These categories include: religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information, as well as criminal history).

\(^{25}\) Id. at § 34.

\(^{26}\) Id. at § 72.

\(^{27}\) See POPI Bill Will Make or Break Online Marketers supra note 2; Nkabinde, supra note 8.

\(^{28}\) Protection of Personal Information Bill at § 69.

\(^{29}\) POPI Bill Will Make or Break Online Marketers supra note 2; Nkabinde, supra note 8.
merely allow for an “opt out” mechanism as opposed to requiring affirmative consent.\textsuperscript{30} POPI also provides that customers be allowed a reasonable opportunity to object, free of charge, to the use of their personal information for marketing purposes when that information is collected at the time of sale and in each and every subsequent electronic communication with the customer.\textsuperscript{31}

In light of the many rights and obligations enumerated by POPI, the law notably establishes the brand new office of the Information Regulator, which will be tasked with educating the public about data protection issues, monitoring and enforcing compliance with POPI, consulting with interested parties, handling information privacy complaints, conducting research, reporting to parliament, issuing codes of conduct, and fostering cross-border cooperation in the enforcement of data protection laws.\textsuperscript{32} With regard to enforcement, POPI violations carry maximum penalties of 10 years imprisonment and up to R10 million in administrative fines.\textsuperscript{33}

As it has taken an entire decade for POPI to wind its way through parliament, the law has attracted a significant amount of commentary, much of it acknowledging South Africa’s efforts in drafting legislation that attends to personal privacy interests in a world increasingly driven by the commoditization of information.\textsuperscript{34} For example, in a report for the Open Democracy Advice Centre, Iain Currie characterizes POPI as “an important legal reform” that “create[s] a regime of consumer protection that has become essential in the information age.”\textsuperscript{35} In particular, Currie praises how POPI makes up for certain deficiencies in the Promotion of Access to Information Act of 2000 (“PAIA”), which only provides for a right of access to information but does not impose specific recordkeeping requirements or regulate the actual mechanics of personal information collection.\textsuperscript{36} Additionally, POPI gives rise to new statutory offenses and sets up a national data protection office, while PAIA relies on private actions in the ordinary courts to enforce its general obligation that public and private bodies take “reasonable steps to establish adequate and appropriate internal measures” to allow for the correction of a data subject’s personal information records.\textsuperscript{37} Consequently, the increased control that South African consumers will exercise over their data under POPI could act as a deterrent to identity theft,\textsuperscript{38} which would come as a welcome development in a nation cited as one of the world’s top cybercrime hotspots.\textsuperscript{39}

\begin{footnotes}
\item[30] Id.\textsuperscript{.}
\item[31] Protection of Personal Information Bill at § 69.
\item[32] Id. at § 40.
\item[33] Id. at §§ 107, 109.
\item[35] CURRIE, supra note 34.
\item[36] Id. at 3.
\item[37] Id. at 4.
\item[38] Bruce Cameron, Identity Thieves Eye Offshore Accounts, INDEPENDENT ONLINE (Sept. 15, 2013), available at http://www.iol.co.za/business/personal-finance/identity-thieves-eye-offshore-accounts-1.1577546#.Umc-4nCe8IV.
\end{footnotes}
POPI's proponents have argued that businesses stand to benefit from the new information privacy standards as well. While clearly defining the obligations of enterprises at the local level (with the added side effect of compelling companies to clean house and purge unnecessary records, thereby generating a windfall for data destruction firms), POPI would facilitate international commerce since its provisions closely resemble the data protection laws of South Africa's trade partners in Europe. Although South Africa is not the first African country to enact information privacy legislation, POPI is the only national data protection statute on the continent modeled after European Union (“EU”) law and one whose drafters hope will be deemed to provide “a sufficient level of privacy protection consistent with the EU Data Protection Directive,” thus permitting the free flow of personal data between the two jurisdictions. Touted as a potential driver of foreign investment, such harmonization could prove especially advantageous for South Africa’s big data, cloud computing, and business process outsourcing industries.

On the other hand, critics have also warned that POPI’s regulatory scheme might impose an undue burden on businesses and therefore discourage economic activity. For example, in order to comply with POPI’s information management and security requirements, many firms will probably have to make additional investments in technology infrastructure, either in-house or through third-party service providers. Furthermore, the one year period set out by POPI for companies to become fully compliant is likely impracticable, as one survey of South African businesses from early 2013 revealed that less than fifty percent of respondents had begun setting up privacy programs despite estimates that achieving compliance could take up to three years, especially for providers of healthcare, telecommunications, or financial services. Additionally, although POPI’s EU-style limitations on cross-border data transfers should facilitate access to European markets that are governed by similarly stringent rules, South African companies ironically may find themselves legally


Claasen, supra note 40.


Aplin, supra note 2; Wehler, supra note 42.

Claassen, supra note 40; Wehler, supra note 42.

Aplin, supra note 2; Wehler, supra note 42; see also Craig Wilson, The Popi Nightmare Awaiting SA Business, TECH CENTRAL (July 18, 2013), http://www.techeentral.co.za/the-popi-nightmare-awaiting-sa-business/41984/.


hamstrung when doing business with clients located in neighboring African countries, where data protection regimes tend to be feeble or nonexistent.\textsuperscript{48}

Following years of public debate, however, POPI is just one pen stroke away from full implementation, all strengths and weaknesses included. The true measure of the law’s success will then lie in the enforcement of its provisions, particularly by the yet to be established Information Regulator.\textsuperscript{49} As such, adequate funding and an ability to recruit qualified personnel to staff the regulatory office pose the biggest challenges in translating POPI’s mandate into meaningful results.\textsuperscript{50} Given the continually low rates of compliance for comparatively modest legislation such as PAIA,\textsuperscript{51} the initial outlook for POPI is not entirely encouraging. Nevertheless, by adopting robust standards that reflect internationally recognized practices in data protection, POPI not only represents a significant legal development for South Africa, but it also serves as an instructive model for other governments in the region.\textsuperscript{52}

\textsuperscript{48} Wilson, supra note 42.
\textsuperscript{49} Aplin, supra note 2; Mawson, supra note 16.
\textsuperscript{50} Wehler, supra note 42.
\textsuperscript{52} POPI Bill Will Make or Break Online Marketers supra note 2.