South Africa Enacts New Data Protection Law

Jan Dhont
Partner
Lorenz
Brussels, Belgium
j.dhont@lorenz-law.com

Katherine Woodcock
Senior Associate
Lorenz
Brussels, Belgium
k.woodcock @lorenz-law.com

On November 26, 2013, the Parliament of the Republic of South Africa enacted the Protection of Personal Information Act ("POPI"). President Jacob Zuma has not yet declared the commencement date of the POPI, however once declared there is a one year transitional period for all processing to come into compliance with its provisions.

I. Similarities with EU Data Protection

Many of the provisions of the POPI are similar to those in the EU Data Protection Directive 95/46/EC ("EU Directive") and one can see that where inspiration is drawn from.

A. Scope of Application

The POPI applies to processing[1] entered in a record by (or for) a responsible party that is 1) domiciled in South Africa or 2) making use of means located in South Africa. This scope is similar to the EU Directive's applicable law rules, as the POPI applies to processing 1) by or on behalf of South African based 'controllers' - i.e. by processors for South African companies – or 2) when a controller is using means for processing located in South Africa. Unlike the EU Directive however, there is a specific provision in case of conflicts with other laws. The POPI applies to the exclusion of any other data protection laws that may apply, unless such law "provides for conditions for the lawful processing of personal information that are more extensive than those set out in [the POPI's conditions for lawful processing,]…the extensive conditions prevail."[2]

[1] Unlike the EU Directive, however both manual and automated processing are included in the POPI. If personal information is manually processed, then it must be part of a filing system or 'structured database'.
[2] POPI, Section 3(1)-(3).

B. Processing and Privacy Principles

Another similarity is the POPI's inclusion of a broad definition of "processing"[3] and the basic privacy principles - accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.[4] Furthermore, the relevant legal bases upon which the processing personal information is permitted are remarkably similar to (albeit not exactly the same as) the EU Directive. These legal bases are not restricted to data subject consent and clearly draw inspiration from the EU Directive.[5]

C. Creation of Data Protection Authority

The POPI also creates a data protection authority ("Information Regulator"), which has powers to monitor and enforce data protection compliance. This power includes consulting with interested parties, handling of complaints, issuing codes of conduct, facilitating cross-border cooperation in privacy enforcement[6] as well as issuing prior authorizations in certain circumstances.[7]

D. International or Cross-Border Transfers of Personal Information

For cross-border transfers, the POPI takes a similar approach to the EU's adequacy mechanism. Transborder information flows to third parties must be subject to a law, binding corporate rules (BCRs), or binding contractual agreement that provides "an adequate level of protection". This level should "effectively uphold principles for reasonable processing… that are substantially similar to the conditions for the lawful processing of personal information…[of] a data subject". the principles for processing Furthermore, the law, BCR or contractual agreement must include provisions "that are substantially similar" to those in the POPI's on cross-border transfers.[8]

There are also other bases for cross-border transfers, including data subject consent, where necessary for performance or conclusion of a contract with the data subject or with a third party where the contract is in the data subject's interest.[9]

---

[3] POPI, Section 1.

[4] See POPI, Sections 8-25. These principles also echo the privacy principles from the Organisation for Economic Co-operation and Development's newly revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Full text available at www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[5] The legal bases include where the processing is:

1. with the data subject's consent,
2. where necessary for conclusion or performance of a contract,
3. legal obligation,
4. protection of the legitimate interest of the data subject,
5. necessary for the proper performance of a public duty by a public body or
6. where necessary for the pursuit of legitimate interest of a third party or third party to whom the information is supplied

[6] See POPI, Sections 39-40, specifically, and Sections 41-54 for the general provisions of its operation.

[7] POPI, Section 57.

[8] POPI, Section 72(1) generally.

[9] Id.

The POPI also contemplates an additional basis for the transfer, where it "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."[10]

E. Direct Marketing

Echoing the direct marketing rules from the E-Privacy Directive 2002/58/EC, the POPI has a specific section on unsolicited direct marketing. Similarly, the POPI provides for an opt-in consent mechanism. This requirement is exempted when the data subject is a customer and his/her contact details are obtained "in the context of the sale of a product or service" for "direct marketing of the responsible party's own similar products or services" and the data subject is provided with an opt-out opportunity.[11]

II. Variances from EU Data Protection

There are also marked differences from the EU Directive, as the POPI takes into account certain national variations or conflicts which the EU has experienced with the implementation of the EU Directive. It appears that the POPI benefitted from looking at the conflicts arising in EU national laws and the variances when implementing the EU Directive.

A. Definition of Personal Information

Interestingly, the definition of "personal information" extends beyond the definition from the EU Directive and includes "juristic person" or legal entities. This brings the POPI in line with some EU and other European member states' national law approach, which extends data protection to certain corporate information.[12]

B. Provisions on Sensitive or Special Personal Information

Similar to the EU Directive, there is a prohibition on processing sensitive data unless the processing qualifies under one of the exemptions in the POPI.[13] However, sensitive data or "special personal information" is more expansive in the POPI. It includes "religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information" and criminal behavior that "relates to (i) the alleged commission…of any offence" or (ii) "any proceedings… of any offence allegedly committed…or the disposal of such proceeding".[14] Criminal convictions and allegations are not consistently regulated throughout the EU; the POPI clearly subsumes both past and present allegations as well as convictions of crimes to create a uniform approach on what qualifies as sensitive data.

[10] POPI, Section 72(1)(e).
[11] POPI, at section 69(3).
[12] POPI, Section 1. Personal data of legal persons is also protected in other countries, including Austria, Italy and Switzerland, *inter alia.*
[13] POPI, Sections 27-33, generally.
[14] POPI, Section 26(b).

Unlike the EU Directive, there is an explicit definition of biometrics: "[a] technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition".[15] A definition of biometrics has been included in some EU national data protection laws[16], however there is widespread divergence in the EU on the inclusion of a specific definition in addition to how the processing of biometric data is treated.

C. Processing of Children's Personal Information

In addition to the prohibition on processing sensitive information, another marked difference is the inclusion a definition of a child and specific provisions on processing children's information. A child is defined as a person under the age of 18 "who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself."[17] Protections for personal information of children is currently be considered in the re-drafting of the EU's General Data Protection Regulation, however there has yet to be consensus on this point from the EU level.

D. Security and Risk Provisions

Although the POPI does include requirements on security and confidentiality of personal information, it takes the EU rules[18] a bit farther. There is an obligation to "take reasonable measures" to identify foreseeable risks (i.e. risk assessment) and take measures against these identified risks and verify them regularly.[19] Furthermore, the security provisions are also extended to 'processors' or "operators or anyone processing personal information on behalf of a responsible party or an operator".[20]

Regardless of the similarities and differences between the POPI and the EU Directive, we will have to wait and see how the law is implemented and enforced in practice before having a clear picture on how the new South African data protection rules will play out for companies.

The full text of the enacted law is available at www.gov.za/documents/download.php?f=204368.

[15] POPI, Section 1.
[16] See, for example, Slovak Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, Section 4.3)f), which defines 'biometric data' as "personal data of the natural person that specifies his biological or physiological characteristic, based on which the natural person is unambiguously and unmistakably identifiable; biometric data is especially fingerprint, palm print, analysis of DNA,"
[17] POPI, Section 1.
[18] As laid out in Article 16 and 17 of the Directive.
[19] POPI, Section 19.
[20] POPI, Section 20.