

# POPI looms - what it means for your business

By [Alison Treadaway](#)

6 Oct 2016

Government's implementation of the Protection of Personal Information Act (POPI) will soon be a reality, and this has far-reaching implications for businesses big and small.



©MaksimKabakou via [123RF](#)

South Africa's Parliament recently voted to appoint an information regulator for the POPI Act and the Promotion of Access to Information Act (PAIA). The National Assembly also voted in favour of the nomination of the five candidates earmarked to run the regulator - Adv Pansy Tlakula, Adv Cordelia Stroom, Johannes Weapond, Sizwe Snail and Prof Tana Pistorius.

While still subject to confirmation by the President, their imminent appointment is a good indication that the date at which POPI's remaining provisions will come into effect, is likely to be announced soon. For South African businesses, this means the provisions of the bill not signed into law yet, will likely be signed into effect shortly. Once that happens, any parties which hold personal information will have a one-year grace period to comply (which may be extended to a maximum of three years).

## Universal implication

Every business today holds some level of information on customers and stakeholders, which means POPI applies almost universally to businesses of all sizes and across all industries. If you gather, receive, hold, use or share information about a consumer or business customer, then you are affected by POPI.

POPI stipulates how businesses can legally process the personal information they hold. Personal information, as defined by POPI, means any information that can be used to identify an individual or a juristic person. These include ID numbers, company registration numbers, email addresses, physical addresses to name but a few.

For many businesses, a year will not be long enough to make the IT, process and contractual changes needed to comply. POPI requires that information is used responsibly, and is adequately secured. Amongst other things, POPI requires organisations to only collect information they need for a specific purpose, to apply reasonable security measures to protect it, to ensure it is relevant and up to date, to only hold the information they need, for only as long as they need it, and to allow the person who it relates to, to see it if required.

## **Lengthy audit**

For most organisations this will require an audit to establish what information they hold, where it is housed and what needs to be done to create a framework to manage and secure it. Depending on the size of the organisation and the information it holds (think databases for email marketing purposes, or customer and supplier information held by a large multi-national) this alone could take a minimum of a year to conduct.

POPI compliance requires ongoing monitoring, so organisations need to appoint an information officer (in fact, all organisations require one in terms of POPI), establish processes and set up systems (if they do not have them) to ensure that data is constantly secured, new data is appropriately handled, and old data is destroyed. Additionally, organisations need to notify persons of what information they hold, and how they intend to use it, as well as verifying that it was given voluntarily, confirm that it is securely stored and ask how long they may keep the information for.

In a nutshell, this means that if you haven't started considering POPI and how your organisation is going to comply, you need to do so urgently.

## **ABOUT THE AUTHOR**

Alison Treadaway, director, Striata.

For more, visit: <https://www.bizcommunity.com>