

# PoPIA anniversary: Have you done enough?

By [Zaakir Mohamed](#), [Savanna Stephens](#) and [Mawande Ntontela](#)

8 Jul 2022

The 1st of July 2022 marks the one-year anniversary of the compliance deadline of the Protection of Personal Information Act No 4 of 2013 (PoPIA) for all organisations. While the operational provisions of this Act became effective on 1 July 2020, a one-year grace period was granted to allow businesses to effect the necessary changes. This resulted in a compliance drive to bring various information practices in line.



Image source: [tumsasedgars](#) – [123RF.com](#)

Compliance with this Act requires ongoing vigilance. At this stage, it is imperative that organisations understand the implications of their personal information practices and put in place systems and measures to manage both their existing and ongoing obligations.

## What has happened since PoPIA came into effect?

In order to address compliance with PoPIA, your organisation has most likely had to:

- Undertake exercises in training staff to comply with PoPIA across all operations;
- Conduct personal information impact assessments to address areas of non-compliance;
- Address issues relating to the consent, transfer and sharing of personal information with third parties (ie. suppliers, customers, etc); and
- Navigate the intricacies of dealing with incidents of data breaches.

Compliance with PoPIA has in certain circumstances necessitated a fundamental shift in the manner in which businesses approach various aspects of their operations. With this shift has come various challenges in accommodating such a transition.

### Examples include:

- There has been a slow uptake in the registration of Information Officers;
- Many organisations are yet to put in place or update their existing Promotion of Access to Information Manual (PAIA Manual) as required; and
- There are still issues in the interpretation of certain provisions of PoPIA which remain uncharted territory and must be navigated through the use of the appropriate processes and legal mechanisms.

Over the past year, developments in case law relating to data privacy have aided us in better understanding the compliance requirements set out in PoPIA. However, this understanding must be accompanied by practical guidelines to assist organisations in the development and implementation of compliance programmes that take into account their specific needs and operational parameters.



### PoPIA: Can businesses ask for vaccine status information?

Preeta Bhagattjee, Aphindile Govuza and Reece Westcott 9 Mar 2022



## How to ensure your compliance

To address any potential compliance gaps within your business, a number of fundamental steps should be considered and taken. These may include:

- Conducting a gap analysis to determine your organisation's readiness for PoPIA;
- Undertaking data mapping exercises to understand the type of information processed by your organisation, and for what purpose such information is processed;
- Considering the relevant data transfer requirements and how they may affect your company's commercial arrangements with third parties or the sharing of data between companies;
- Updating the PAIA manual to accord with the relevant requirements set out in PAIA (as amended) and PoPIA;
- Developing a culture of privacy by:
  - Conducting an awareness campaign;
  - Training staff; and
  - Updating the relevant organisational policies.
- Updating customer and supplier contracts to ensure they accord with the relevant requirements set out in PoPIA;
- Preparing the relevant consent and notification documentation;
- Implementing a system for data subject access management; and
- Preparing and/or updating a data breach incident response plan.

The above-mentioned steps are useful in establishing certain best practices in your organisation's PoPIA compliance journey; however, ongoing obligations necessitate a constant review of your organisational processes to ensure that they do not fall short of the PoPIA requirements over time.



## GDPR and PoPIA: Cost of non-compliance is hefty

20 Sep 2021



### How to educate yourself further

In recognition of the one-year anniversary of PoPIA, CMS will be publishing a series of articles to take stock of the relevant developments since the enactment of PoPIA, which will broadly deal with:

1. The role of employees in data protection compliance programmes;
2. Understanding personal information impact assessments;
3. The management of data transfers;
4. Notifications and disclosures of processing activities;
5. Understanding the various types of cyber risk; and
6. A broad account of data breaches.

Understanding the intricacies and implications of the requirements set out in PoPIA will require your active engagement and consultation to test your operations against the prescripts of the Act. It is not sufficient to deal with your obligations on a theoretical basis alone, as the requirements relating to various organisations may differ on a case-by-case basis. Compliance with the present and ongoing obligations of PoPIA must be accompanied by a practical process that allows your organisation to meaningfully measure compliance and address the deficiencies identified.

### ABOUT THE AUTHOR

Zaakir Mohamed, Director: Head of Corporate Investigations and Forensics; Savanna Stephens, Senior Associate: Corporate and Commercial; and Mawande Nontela, Associate: Corporate Investigations and Forensics, at CMS South Africa

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