POPI Act on our doorsteps

By Ryan van de Coolwijk

24 Jun 2020

The commencement date for the Protection of Personal Information (POPI) Act has been an area of speculation and doubt for many years. However, on 22 June 2020 the Presidency announced the commencement of several additional sections of the POPI Act and companies will have until 1 July 2021 to ensure they comply.

Ryan van de Coolwijk

The POPI Act has been brought into operation incrementally since April 2014 when some initial sections were implemented. These sections related to the establishment of the Information Regulator, the members of which took office on 1 December 2016.

Since then delays in further implementation resulted in legal uncertainty, with some questioning whether the legislation would ever see the light of day. This became an area of concern as having privacy legislation in place became increasingly vital for South Africa to be seen as a legitimate participant on the global digital marketplace. Not to mention the benefits of protecting the individual who needs to entrust their data to businesses to trade with them.

However, much has been done since 2016 which has now culminated in the commencement of several the remaining sections of the POPI Act, which have now been proclaimed by the president.

Take note...

The relevant sections and applicable dates are as follows: Sections 2 to 38; Sections 55 to 109; Section 111, and Section 114 (1), (2) and (3) shall commence on 1 July 2020.

The sections are essential parts of the Act and comprise sections that pertain to, among others, the conditions for the lawful processing of personal information; the regulation of the processing of special personal information; Codes of Conduct issued by the Information Regulator; procedures for dealing with complaints; provisions regulating direct marketing by means of unsolicited electronic communication, and general enforcement of the Act.

Section 114(1) is of particular importance, as it states that all forms of processing of personal information must, within one year after the commencement of the section, be made to conform to the Act.

According to the Presidency, this means that entities (both in the form of private and public bodies) will have to ensure compliance with the Act by 1 July 2021. However, it stands to reason that one should attempt to comply with the provisions of the Act as soon as possible to give effect to the rights of individuals.

Sections 110 and **114(4)** shall commence on 30 June 2021. The reason for the delay in relation to the commencement of **Sections 110** and **114(4)** is that these sections pertain to the amendment of laws and the effective transfer of functions of the Promotion of Access to Information Act, 2000 (PAIA) from the South African Human Rights Commission to the Information Regulator.

Organisations that don't comply with the POPI Act, regardless of whether it’s intentional or accidental, can face severe penalties. Depending on the seriousness of the breach, the POPI Act makes provision for fines of up to R10 million and a jail sentence of up to 10 years.

Organisations that are compromised or suffer a data privacy breach incident, even if this is the theft of a laptop or memory stick with sensitive data on it, will need to ensure that they comply with the requirements of the POPI Act to avoid these penalties.

Dependent on the nature of the incident, organisations will need to:

- Conduct a formal investigation to ensure they understand how the incident occurred, the severity of the incident including what and whose data has been compromised and provide proof of adequately containing the incident.
- Notify the regulator.
- Communicate with affected parties and provide them remediation services such as credit monitoring to prevent them from suffering further damages such as being the victim of further fraud.

Communicating with affected parties is important to assist individuals in preventing themselves from suffering further damages, as a result, organisations are likely to have incidents being further publicised. This will see them:

- Needing to conduct crisis management and public relations campaigns to manage potential reputational damage

- Being exposed to potential ensuing litigation

Cyber insurance is well suited to help organisations respond to and manage these increasing exposures which are further exacerbated by having to adjust to the new normal for working environments resulting from the Covid-19 pandemic.

The New Norm

Remote working and online engagement are no longer a nice to have but an essential way of operating. There are likely to become a permanent feature of the ‘new normal’ after the Covid-19 pandemic.

Protecting your business from cyber threats needs to be prioritised. Cyber insurance provides your business with access to expert knowledge and resources to effectively manage and recover from a cyber incident. Look for a cyber insurance policy that meets your specific requirements.

ABOUT THE AUTHOR

Ryan van de Coolwijk, head of cyber at iTOO