

August 6, 2020

POPI Act - what is the liability of responsible parties?



With South Africa's Personal Information Act 4 of 2013 (POPI Act) that came into effect on 1 July 2020, it is important for business owners to acknowledge and understand the degree of the civil action, criminal offences, fines, damages and compliance notices in terms of the Act.

Companies are obligated to protect information processing, storage and deletion to ensure that such information is safeguarded and that the risk of data breaches and theft of personal information is minimised.

In this blog we will discuss how non-compliance with the POPI Act can impact a business.

How can non-compliance affect my business?

o Reputational damage

The biggest risk posed by non-compliance is reputational damage.

If a civil action has not been instituted, any agreement or settlement may be published in the *Government Gazette* and other public media in any manner the court considers appropriate.

The most affected industries are financial services, healthcare, schools and marketing. Businesses that process special personal information such as children's information, medical information, account numbers, etc. run the highest risk and should therefore take extra precautions when processing information.

o Penalties, administrative fines and damages

Failure to protect personal information may lead to fines and damage claims up to R10 million and/or imprisonment for no longer than 12 months.

o Civil action

Section 19 of the Act provides for employers to take "appropriate, reasonable, technical and organisational measures" to prevent the loss and unlawful processing of personal information.

Section 99(1) of the Act provides that a data subject, or the Regulator at the request of the data subject, may institute a civil action for damages in a court against a responsible party for breach of the POPI Act, whether or not there is intent or negligence on the part of the responsible party.

The same principle is also used in other legislation, for instance the Consumer Protection Act (CPA), where a business may be held liable for the conduct of its employees, regardless of whether there is any wilful or negligent conduct on the part of the business. If the business is able to show that it took all reasonable and practicable measures to ensure compliance with the POPI Act, this would serve as a defence for non-compliance and the business may avoid a fine; however, the business may still be civilly liable due to the "no fault test" of both POPI and CPA.

o Enforcement notices

Businesses will be affected if they can no longer process information. Section 95 of the Act stipulates that when the Regulator confirms that the Responsible party is not compliant with the provisions of the Act, the Regulator may require the Responsible party to take specified steps within a period stated in the issued notice and/or to stop processing personal information with immediate effect during the notice period.

In conclusion

The restrictive nature of the defences creates an onerous risk for employers which may not be adequately addressed by the steps typically taken by employers to limit the risks. *Full implementation of POPI involves onsite audits, assessments, amendment of agreements with certain suppliers and training of staff.*

Businesses should therefore minimise the risk of damages by implementing internal policies relating to the processing of personal information, compulsory training sessions and awareness campaigns. Consent forms should be updated for all data subjects to ensure proper processing of information.

SERR Synergy assists businesses in compiling Data and Information Protection Reports. Our professional legal team ensures that physical information and cybersecurity risks of organisations are identified and managed to maintain the confidentiality, integrity and availability of data. We provide organisations with various policies to ensure compliance in such a way that it adds business value to our clients and allows for improvement in efficiencies and effectiveness.

About the Author: Retha van Zyl completed her BCom Hons (Economics and Risk Management) studies at the North West University. She joined our team in January 2016 and currently holds the title 'Information Compliance Advisor'. She specialises in POPI and PAIA compliance, which includes compiling and submitting PAIA Manuals to the Human Rights Commission. She also compiles the Data and Information Protection Report to identify risks associated with information security and drafts Information Security policies for procedural compliance in each department within an organisation.

Sources:

https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

<https://www.michalsons.com/blog/popi-act-summary-in-plain-language/18618?gclid=Cj0KCQjwpNr4BRDYARIsAADlx9witLPIWPiY1qYiGzpAIKZKJ95tGApvqJgI>

<https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/Employment/popibumper-special-alert-30-june-The-POPI-Act-increased-liability-for-employers-.html#:~:text=Bumper%20Special%20Alert-,The%20POPI%20Act%20%E2%80%93%20increased%20liability%20for%20employers,99%20>

©SERR Synergy, www.serr.co.za