JUTA
POPIA PORTAL

ISSUE NO 41 • CONSEQUENCES OF NON-COMPLIANCE WITH POPIA • NOVEMBER 2024

CONSEQUENCES OF NON-COMPLIANCE WITH POPIA

OVERVIEW

The Protection of Personal Information Act 4 of 2013 (POPIA) sets the standard for how businesses and individuals process personal information in South Africa, ensuring it is done responsibly. Non-compliance with POPIA is not just a legal misstep but also a costly one. Financially, reputationally, and even criminally. Here's a breakdown of the consequences for non-compliance with the Act.

Photo: iStock

1. FINANCIAL PENALTIES

Photo: iStock

Failure to comply with POPIA can result in serious financial repercussions. The Information Regulator can issue administrative fines of up to R10 million. These fines are imposed without needing a court ruling, making them an immediate and severe consequence of non-compliance. See 19.10.3 Administrative fines.

The Department of Justice and Constitutional Development (DOJ & CD) received an administrative fine of R5 million after ignoring an enforcement notice following a significant data breach. This is an example of how businesses may be held accountable. See the media statement for details on the infringement notice and administrative fine issued.

2. IMPRISONMENT

Photo: iStock

It is important to remember that general non-compliance with the act does not constitute an offence. See 19.10.1 'Offences and penalties created by POPIA' for a table breakdown of offences created by POPIA and PAIA, the possible consequences and who can be held liable.

2.1. Who can be imprisoned?
Some offences apply to any individual who commits them, while others apply specifically to the Responsible Party.

- Employees
  If employees commit these offences in their personal capacity, acting on their own behalf, they can face imprisonment or fines. However, if they're acting within the scope of their employment or under the direction of a Responsible Party, the Responsible Party will be held accountable and may face up to ten years in prison or a combination of imprisonment and a fine.
- Responsible Party
  If the Responsible Party, as an organisation, is fined, the penalty applies to the organisation, not the individual who committed the offence, as they acted within the scope of their employment. However, depending on the circumstances, the Information Officer may still be held liable by the organisation.

3. CIVIL LIABILITY

Photo: Pixabay

Beyond fines and imprisonment, affected data subjects can seek civil remedies. Under POPIA, they may claim damages, which can range from direct financial loss to claims for reputational damages, interest, and legal fees.

While an Information Officer can be held personally liable by an organisation for civil claims related to any losses, damages, or costs incurred, the organisation must demonstrate that the Information Officer failed to meet the expected standard of conduct for their role.

4. REPUTATIONAL DAMAGE

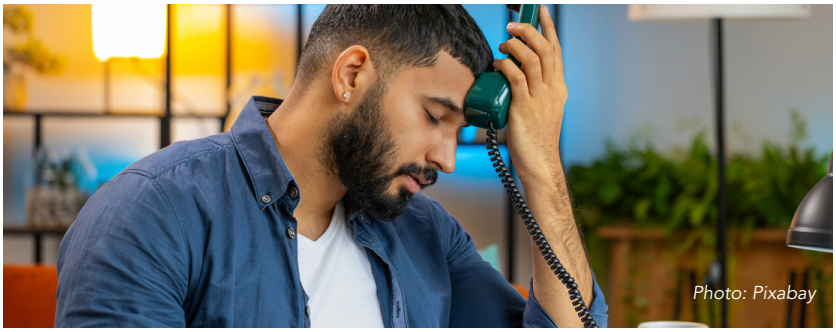


Photo: Pixabay

Data breaches and the effect of failing to comply with POPIA can lead to damage to public trust. Businesses risk losing customers, service providers, and other stakeholders. In today's digital age, a single breach can destroy years of trust in mere seconds, crippling a business's ability to maintain its position in the business market and even disrupt operations.

5. OPERATIONAL DISRUPTIONS

When a business is found to be non-compliant, the Information Regulator may issue enforcement notices. These notices require businesses to take corrective actions, which often disrupt regular business operations. Ignoring these enforcement actions can lead to further fines, and prolonged failure to comply could escalate into more severe legal consequences.


Photo: AdobeStock

6. INCREASED REGULATORY SCRUTINY


Photo: AdobeStock

Once marked for non-compliance, businesses are likely to face increased scrutiny from the Information Regulator. This involves more frequent audits and closer inspections and investigations. The Regulator is actively monitoring businesses to ensure they meet their obligations under POPIA, and they can also launch an own-initiative investigation without receiving a complaint.
See 19.9.3 'Investigations initiated by the Information Regulator'.

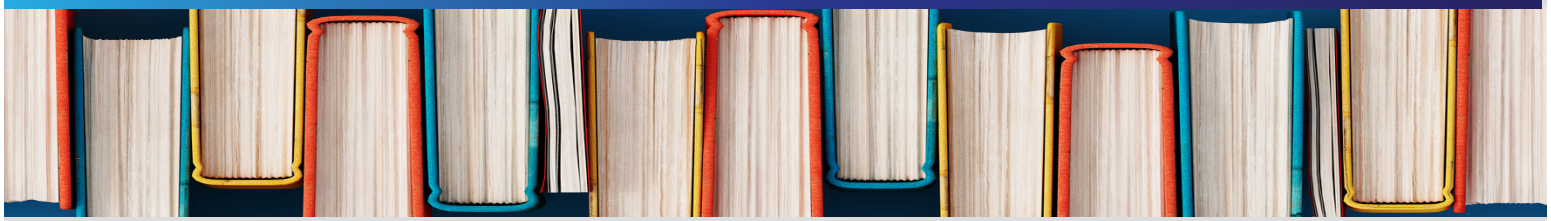
7. CONCLUSION

Businesses must take proactive steps to ensure compliance, which includes appointing a dedicated Information Officer, conducting regular audits, having a compliance framework and training their employees on risks and the prevention of non-compliance.


Photo: AdobeStock

8. READ MORE

Photo: AdobeStock



Read more about enforcement notices, in Enforcement notices issued by the regulator in terms of POPIA.

To read more about 'Enforcement of POPIA', see Chapter 19.