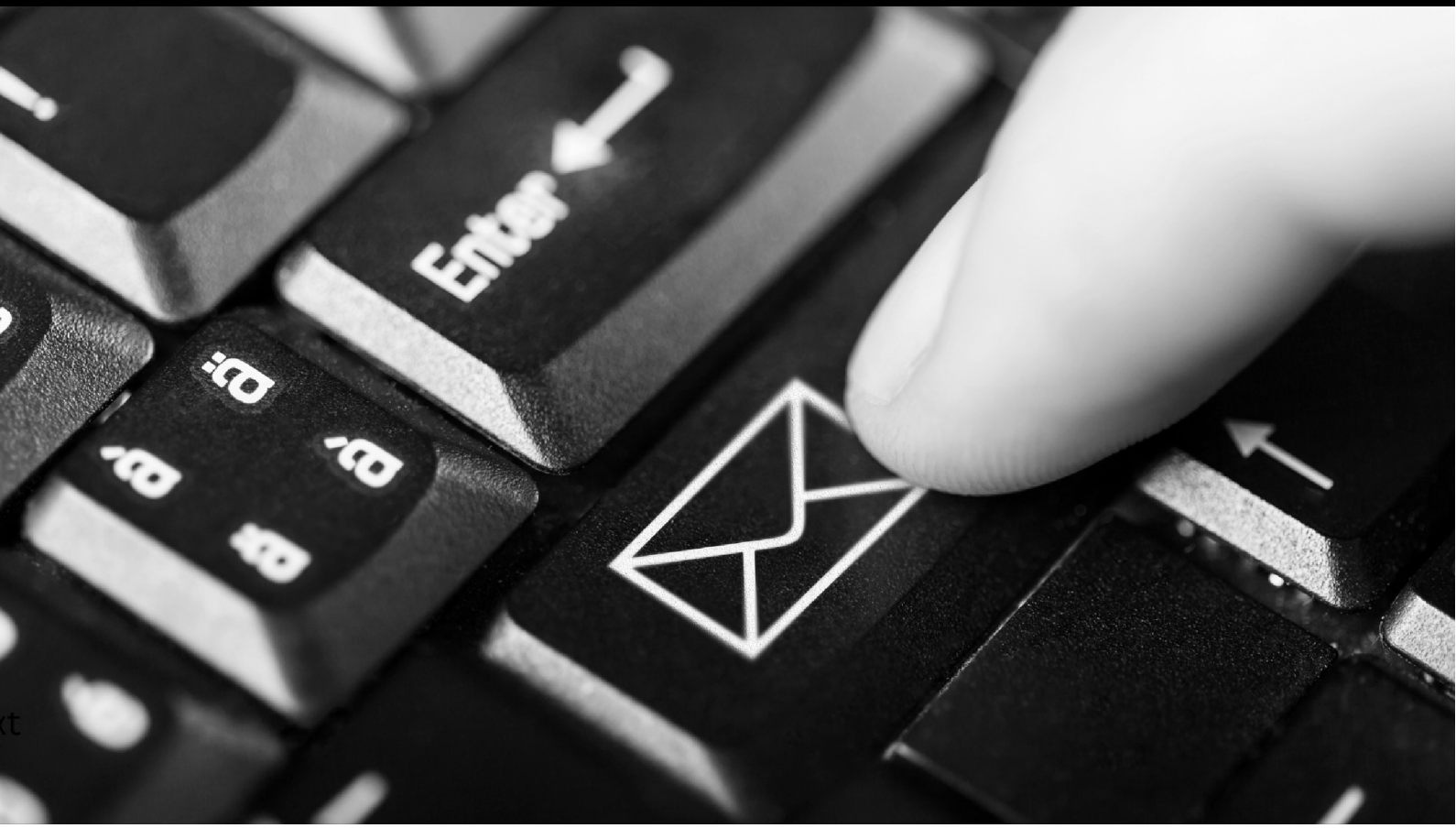
WERKSMANS
ATTORNEYS



REGULATORY

When a misdirected email becomes a data breach: The Information Regulator issues an enforcement notice on internal and accidental security compromises

18 June 2026 *6 min read*

by Armand Swart, Director, Hlonelwa Lutuli, Associate and Isabella Keeves, Candidate Attorney

On 22 May 2026, South Africa's Information Regulator served an enforcement notice on the Central Johannesburg TVET College after employees' personal credential verification reports were accidentally emailed to unauthorised staff. The enforcement notice sets a significant precedent: even accidental, purely internal disclosures of personal information to unauthorised parties constitute a "security compromise" under the Protection of Personal Information Act 4 of 2013 ("**POPIA**"), triggering formal breach notification obligations. This article examines the enforcement notice, analyses its implications under POPIA, compares the position to the GDPR, and offers practical guidance for businesses.

Background

The Central Johannesburg TVET College (the "**College**") had been placed under administration to address governance failures, including undisclosed criminal records and conflicts of interest among staff. As part of this process, employees' personal information was collected to verify their academic qualifications and criminal records. This was done by a service provider preparing Personal Credential Verification Reports ("**Verification Reports**"). The Acting Chief Financial Officer erroneously included the complainants' Verification Reports in a folder of finance policies, which was then emailed to unauthorised employees.

The email was recalled and a follow-up was sent alerting staff to the error. An investigation was launched and corrective action was taken against staff who forwarded the document.

The Information Regulator (the "**Regulator**") identified three categories of POPIA violation. First, the College had failed to register an information officer or designate deputy information officers, breaching POPIA's accountability condition (section 8). Second, distribution of the Verification Reports to staff uninvolved in the governance restoration exercise constituted further processing incompatible with the original collection purpose (section 15). Third, the College's failure to maintain separate files for Verification Reports and finance policies, coupled with its failure to register an information officer, evidenced an absence of organisational controls to prevent unlawful access or processing (section 19). The Regulator found that the accidental internal disclosure triggered POPIA's security compromise notification obligations under section 22, which the College had failed to discharge.

The Regulator directed the College to: (i) register an information officer and deputy information officers; (ii) formally notify the Regulator and affected data subjects of the compromise; (iii) issue a written apology to the complainants, to be circulated to all staff; (iv) take disciplinary action against the responsible employee; (v) develop and submit a POPIA Compliance Framework; and (vi) conduct staff awareness and training programmes. Failure to comply with an enforcement notice is a criminal offence punishable by a fine of up to R10 million, imprisonment of up to ten years, or both (section 103).

Accidental and Internal Breaches are Security Compromises

The most significant aspect of this enforcement notice is the Regulator's confirmation that both accidental breaches and internal disclosures fall within the meaning of a "security compromise" for POPIA purposes. Section 22(1) requires a responsible party to notify the Regulator and affected data subjects "where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person". The provision does not distinguish between external attackers and internal employees, nor between deliberate and inadvertent disclosures. Any access by a person not authorised to receive the information is sufficient to trigger the obligation.

In the College's case, the breach was entirely accidental: an employee attached the wrong file to an email, and the recipients were internal staff members, not external third parties. Nevertheless, the Regulator held that this constituted a security compromise triggering POPIA's notification obligations in full. The College had attempted to mitigate the error by recalling the email, launching an investigation, and alerting employees that the information was not for staff use. However, the Regulator held that these good-faith remedial steps did not absolve the College of its statutory duty to formally notify the Regulator and affected data subjects. The message is clear: informal internal remediation, however swift, is no substitute for formal compliance with POPIA's security compromise notification requirements.

This interpretation is grounded in the broad language of section 19(1), which requires responsible parties to take "appropriate, reasonable technical and organisational measures" to prevent, among other things, "unlawful access to or processing of personal information". Read together with section 22, the statutory framework imposes a duty to safeguard personal information against all forms of unauthorised access, whether originating externally or internally, and whether intentional or accidental.

Key Takeaways for Businesses

Organisations must implement robust security measures to protect against both internal and external breaches. This requires both: (i) technological measures, such as access controls and data loss prevention technology; and (ii) organisational measures, such as policies, clear processes, and employee training. As the College's case demonstrates, something as simple as storing personal information in a separate, access-controlled folder could have prevented the breach entirely.

Businesses should implement appropriate access controls to limit internal exposure to personal information. Personal information should be accessible only to those who require it for the specific purpose for which it was collected. Role-based access controls, file segregation, and clear protocols for handling sensitive documents are essential.

Every organisation should develop and maintain a comprehensive data breach response plan. The College's experience illustrates that good-faith remedial steps – such as recalling an email and investigating internally – do not satisfy statutory breach notification obligations. A proper response plan should include: clear procedures for identifying and escalating potential security compromises; templates for notification to the Regulator and affected data subjects; designated personnel responsible for managing the response; and defined timelines to ensure notification is made "as soon as reasonably possible" as required by POPIA.

Most importantly, businesses must recognise the obligation to report all breaches to both the Regulator and affected data subjects. Unlike the GDPR, POPIA contains no materiality threshold. Every security compromise, no matter how minor, must be formally notified.

Organisations should ensure that staff at all levels understand this obligation and that internal reporting channels are in place to escalate potential breaches promptly to those responsible for regulatory notification.

Conclusion

Although other jurisdictions, such as the EU and UK, also require reporting of internal and accidental breaches, they apply a materiality threshold and only high-risk breaches have to be reported. POPIA contains no such exception. The practical consequence is that private and public bodies under POPIA must report every security compromise, however minor, even a misdirected internal email. This places a considerable administrative burden on responsible parties, and it stretches the Regulator's finite resources. In the absence of a materiality threshold, there is a real risk that regulatory attention is diverted from serious incidents to trivial ones. Until the legislature revisits this position, however, organisations must comply with the law as it stands.

Responsible parties must treat their data security obligations with the seriousness they demand or face the risk of a simple mistake inviting the full scrutiny of the Regulator, as was unfortunately the case for the College.

Armand Swart

Director

View Profile

Hlonelwa Lutuli

Associate

View Profile