WERKSMANS
ATTORNEYS

LEGAL UPDATE

The Regulator is Watching: New Enforcement Signals for POPIA and PAIA Compliance

31 August 2026 *9 min read*

by Ahmore Burger-Smidt, Director and Head of Regulatory, Armand Swart, Director and Hlonelwa Lutuli, Associate.

The Information Regulator (Regulator) has put down a marker. In a media briefing held today, 31 August 2026, the Regulator delivered a comprehensive account of its enforcement activities under both the Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA). The briefing also marked a significant institutional milestone: 2026 is the Regulator's 10-year anniversary, having been formally established in December 2016, and five years since the enforcement provisions of POPIA commenced.

Key Developments

Enforcement Notices Under POPIA

The Regulator has issued several enforcement notices under POPIA in this financial year, while each warrant careful attention, the following enforcement notice issued against South African Bureau of Standards (SABS) was highlighted:

- Following a significant ransomware attack in 2024 that disrupted SABS's information systems and operations, the Regulator conducted an own-initiated assessment and found that SABS had violated multiple POPIA conditions, including processing excessive or irrelevant

information, having inadequate consent mechanisms, insufficient security safeguards, and failing to inform data subjects of collection methods.

- SABS has been directed to revise its policies, conduct risk and impact assessments, and implement adequate security measures within 90 days. The Regulator emphasised that the enforcement action was not taken simply because SABS was a victim of a cyber-attack, but because of the underlying compliance failures identified during the assessment.

POPIA Fines Imposed

The Regulator disclosed the fines that have been imposed under POPIA to date. These include:

Entity	Fine	Status
Department of Justice	Column 2 Value	Column 3 Value
Department of Basic Education	Column 2 Value 2	Column 3 Value 2
Column 1 Value 3	Column 2 Value 3	Column 3 Value 3
Column 1 Value 4	Column 2 Value 4	Column 3 Value 4
Column 1 Value 5	Column 2 Value 5	Column 3 Value 5

Ongoing POPIA Matters and Investigations

- Matric Results: The Regulator continues to challenge the Department of Basic Education's publication of matriculants' exam numbers together with their results. The Regulator has applied for leave to appeal directly with the Supreme Court of Appeal following the High Court's refusal for leave, maintaining that the matter raises important questions about the interpretation and application of POPIA to learners' personal information.
- The Regulator confirmed that is has various ongoing investigations and assessments underway, including TruCaller and the Gauteng Department of E-Government.
- eThekwini Metropolitan Municipality: The Madlanga Commission of Inquiry referred concerns to the Regulator in February 2026 regarding the unlawful processing of personal information by a former city manager of the eThekwini Metropolitan Municipality. The Regulator accepted the referral, initiated an own-initiative investigation, and has completed the investigation. The matter has been referred to the Enforcement Committee for appropriate action.
- On 4 August 2026, the Regulator received a further referral from the Madlanga Commission relating to, among others, Vusimuzi Matlala.

PAIA Annual Report Compliance

The compliance figures on PAIA annual reporting are, frankly, dismal:

- Between 1 April and 18 August 2026, the Regulator received PAIA annual reports from 417 out of 853 public bodies, a compliance rate of approximately 9%. This is an improvement on the 2024/25 period (358 submissions, compliance rate of approximately 42%).
- Municipal compliance remains critically low: only 91 out of 257 municipalities submitted reports, a compliance rate of roughly 35%.
- Other low-compliance categories include political parties, TVET colleges, Schedule 3A and 3C public entities, and notably the Public Protector, which has failed to submit its own section 84(b) report.

The Regulator is clearly frustrated and is seeking stronger enforcement tools.

Direct Marketing and Spam Calls

The Regulator has confirmed its position that telephone calls constitute "electronic communication" under POPIA. This remains a contentious legal question, with the direct marketing sector arguing that telephone calls fall outside the Act's scope. The Regulator disagrees. Of the over 3,800 complaints received last year, approximately 10% related to direct marketing, demonstrating the scale of the issue. Two key matters

have been referred to the Enforcement Committee and raise important questions about the interpretation and application of section 69 of POPIA (unsolicited electronic communications).

The Regulator has welcomed the recent amendment to the Consumer Protection Act (CPA) regulations establishing the opt-out/block registry for unsolicited marketing communications, and has engaged with the National Consumer Commission on collaborative awareness-raising and enforcement. The Regulator highlighted that CPA compliance does not displace POPIA compliance obligations in respect to direct marketing.

Security Compromises

The Regulator has received over 8,000 security compromise notifications since POPIA's enforcement provisions commenced. In the current financial year (from 1 April 2026), over 1,220 notifications have been received, with a projected 3,000 by year end. The Regulator highlighted common causes include inadequate security controls, employee negligence, weak passwords, and malware/ransomware attacks. The public sector was criticised for insufficient investment in security measures.

The Auditor-General has identified severe cybersecurity weaknesses across government, including ageing infrastructure and skills deficits. The Regulator observed that organisations are treating data protection as a "tick box exercise" rather than an operational priority.

Proposed Legislative Amendments

The Regulator intends to submit proposals to Parliament for amendments to PAIA and POPIA:

- PAIA: Current enforcement provisions are considered too weak. Unlike POPIA, PAIA does not provide for administrative fines for non-compliance with enforcement notices. Instead, the Regulator must lodge a criminal complaint against the non-compliant information officer, which is a cumbersome process. The Regulator is pursuing proposed legislative amendments to PAIA to introduce enforcement mechanisms equivalent to those available under POPIA, including the ability for the Regulator to release information directly where an order has been made and not complied with within 180 days.
- POPIA: The Regulator has identified structural weaknesses, including the observation that once a responsible party complies within the grace period set in an enforcement notice, the Regulator can no longer impose a fine, which limits the deterrent effect. The Regulator acknowledged that the current fines regime may not be high enough to deter repeat offenders. Proposals under consideration include moving towards immediate fines upon a finding of non-compliance, mirroring the GDPR model, rather than the current "grace period" approach.

These amendments would significantly harden the regulatory framework.

New Digital Platforms

The Regulator has introduced new digital platforms including a POPIA online complaint/case management system, a POPIA exemption application portal, a POPIA/PAIA authorisation application system, and a centralised enquiry management system (iSupport).

Proactive Monitoring

The Regulator has begun a proactive monitoring exercise, sending letters to responsible parties requiring them to demonstrate compliance – rather than waiting for complaints. The private sector was noted to have materially higher compliance levels than the public sector.

What does this mean?

We draw the following practical conclusions from the briefing:

- Heightened enforcement activity. The Regulator is demonstrably moving beyond awareness-raising and into active enforcement. Organisations should treat compliance with POPIA and PAIA as a matter of immediate operational priority, not a project for next quarter.
- Security compromise preparedness. With over 1,220 security compromise notifications received in fewer than five months (and a projected 3,000 by year end), organisations must ensure they have robust incident response plans in place, including the ability to comply with section 22 notification obligations in a timely manner.

- Direct marketing compliance. Organisations that engage in direct marketing, particularly via telephone, should urgently review their practices against the Regulator's stated position on consent requirements and opt-out mechanisms.
- PAIA annual report submissions. Both public and private bodies should ensure they submit PAIA annual reports as required under sections 32 and 83 of PAIA. While compliance rates have improved (to approximately 49% for public bodies), they remain unacceptably low, and the Regulator's express intention to seek stronger enforcement powers means that non-compliance is likely to attract consequences in the near future.
- Anticipate legislative change. The proposed amendments to both POPIA and PAIA, including the move towards immediate fines, signal a shift towards a more punitive enforcement regime. Organisations should begin preparing for a stricter compliance environment now, rather than waiting for the legislation to catch up.

Conclusion

The message from the Regulator is unambiguous: the era of soft enforcement is over.

In its first decade, the Regulator has moved from institutional establishment to active, assertive regulation, and the trajectory is clear. The combination of escalating enforcement action, proactive compliance monitoring, and proposed legislative amendments designed to introduce immediate fines signals a fundamental shift in the South African data protection landscape.

Organisations, in both the public and private sectors, can no longer afford to treat POPIA and PAIA compliance as peripheral or aspirational. The Regulator has demonstrated that it is willing to act against government departments, state-owned entities, and private sector operators alike. The SABS enforcement notice, the ongoing IEC and Department of Basic Education matters, and the growing list of entities under investigation all confirm that no sector is immune from scrutiny.

For the private sector, the takeaway is straightforward: invest in compliance now, or face the consequences later, consequences that, if the Regulator's proposed amendments are enacted, will be materially more severe than those available under the current framework. For the public sector, the picture is even starker. Compliance rates remain alarmingly low, cybersecurity infrastructure is ageing, and the Regulator has made clear that it regards government's performance as wholly inadequate.

Ten years in, the Information Regulator has found its voice, and its teeth. South African organisations would be well advised to listen.

Ahmore Burger-Smidt

Head of Regulatory

View Profile

Armand Swart

Director

View Profile

Hlonelwa Lutuli

Associate

View Profile