WERKSMANS
ATTORNEYS

LEGAL UPDATE

South Africa's Information Regulator: What the 2025/26 Annual Performance Plan means for Business (as presented to the Portfolio Committee on 5 May 2026

5 May 2026 *14 min read*

by Ahmore Burger-Smidt, Director and Head of Regulatory

"*It is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community*." Constitutional Court of South Africa, Bernstein and Others v Bester NO and Others (1996)

The Information Regulator's 2025/26 Annual Performance Plan (APP) signals a firmer enforcement posture under the Protection of Personal Information Act 4 of 2013 (POPIA) and a drive to modernise the Promotion of Access to Information Act 2 of 2000 (PAIA), with immediate implications for governance, breach reporting, direct marketing, access-to-information workflows, and cross border transfers.

In short, businesses should expect more proactive audits and higher expectations on PAIA compliance; mandatory e portal use for breach notifications; tighter direct marketing controls following the April 2025 POPIA Regulations amendments; and new guidance and a sectoral code in the pipeline, including a Guidance Note on cross border transfers and a Code of Conduct for "gated access" environments. The Regulator intends to initiate PAIA legislative amendments in the 2025/26 period to strengthen its regulatory toolkit, while Parliament's Committee has indicated it is awaiting broader POPIA and PAIA amendment proposals. As of 5 May 2026, organisations should prioritise closing PAIA/POPIA process gaps, preparing for sector focused scrutiny, and aligning cross border practices to forthcoming guidance.

The APP foregrounds five developments that are immediately decision useful for boards and executive compliance teams.

- First, the Regulator will initiate a PAIA amendment process in 2025/26 to enable it to issue regulations, modernise PAIA for the digital era, and strengthen enforcement, with the Committee explicitly signalling it awaits broader POPIA/PAIA amendment proposals; in practice, this points to a near term policy window in which the Regulator's formal powers to steer PAIA compliance could expand.
- Second, the Regulator will intensify security compromise (breach) oversight by consolidating technical and legal capacity and by requiring breach notifications via its eServices portal, which has been mandatory since 1 April 2025.
- Third, direct marketing compliance moved decisively in April 2025, when amended POPIA Regulations took effect, requiring recorded telemarketing calls, strengthened consent workflows, multi channel objection mechanisms, and clarified complaint handling; these measures raise both operational and audit-readiness expectations.
- Fourth, the Regulator will publish a Guidance Note on transborder transfers and develop a Code of Conduct for processing at gated accesses, with a draft code to be finalised during the next cycle; these instruments will standardise expectations on cross border diligence and curb over collection at estates, offices, and retail sites.
- Fifth, enforcement trends already show a willingness to impose administrative fines and to litigate strategic questions, with significant matters in education, justice, health, local government and direct marketing, alongside an uptick in own initiative PAIA inspections and active use of non compliance notices.

Legislative reform signals for POPIA and PAIA – *The Regulator's plan to amend PAIA in 2025/26*

The APP records the Regulator's intention to initiate legislative amendments to PAIA during the 2025/26 performance period to empower it to develop and issue PAIA regulations, modernise the statute for a digital environment, and strengthen the Regulator's enforcement powers under PAIA. This is framed as necessary to respond to persistent low compliance rates with statutory reporting and to align access to information practice with contemporary processing realities. The envisaged amendments would, if enacted, give the Regulator clearer rule making competence and sharper compliance levers, moving PAIA closer to the more mature sanctioning architecture already present in POPIA.

The Portfolio Committee on Justice and Constitutional Development has stated it is awaiting the Information Regulator's submissions on amendments to the protection and access frameworks, indicating parliamentary openness to receiving consolidated proposals covering both POPIA and PAIA. This point underscores that any legislative programme will traverse the Department of Justice and Constitutional Development (**DoJ&CD**) channels and the normal Cabinet and parliamentary processes, with timelines therefore contingent on executive scheduling and legislative load. From a planning perspective, businesses should assume that a first tranche of proposals could be tabled shortly, with promulgation dependent on parliamentary prioritisation, and should consider making readiness assessments against the likely contours of a strengthened PAIA enforcement toolkit.

Interaction with the April 2025 POPIA Regulations amendments

While not a primary legislative change, the amended POPIA Regulations commenced on 17 April 2025 and have immediate effect on operational compliance. The amendments clarify objection and correction/deletion pathways, allow multi channel submissions, formalise timeframes, strengthen consent for direct marketing, and require records of telemarketing interactions to be retained and provided on request, while also refining Information Officer responsibilities and complaint handling. These changes materially raise the standard for complaint-readiness, direct marketing governance and evidence keeping in both public and private bodies. The Regulator has already flagged direct marketing as an area where it seeks definitive jurisprudence, including whether live telemarketing falls within POPIA's "*electronic communications*" rule, reinforcing that enforcement test cases are part of the strategy to stabilise interpretation.

POPIA–PAIA misalignment: tensions and practical implications – *Enforcement asymmetry and reporting deficits*

The APP and parliamentary reporting highlight a structural gap: PAIA compliance is "*honoured in breach rather than in compliance*," with only 278 of 853 public bodies submitting PAIA annual reports in 2023/24 (approximately 33%), and private body reporting compliance even lower. This enforcement asymmetry is sharpened by POPIA's more developed sanctioning regime and active use of infringement notices, compared to PAIA's historically weaker remedial mechanisms. The Regulator's stated legislative intent is therefore squarely aimed at closing this gap. In practice, this means businesses can expect more frequent own initiative assessments and site inspections under PAIA, focusing on manuals, request processing records, refusal-ground application, and annual reporting discipline, alongside corrective directions and potential follow on enforcement.

Process friction: request forms, manuals and data subject access

The Regulator has formally cautioned that use of repealed PAIA "Form A" is non compliant; requests must be made on a form substantially corresponding to "Form 2" under the 2021 PAIA Regulations, and organisations should align manuals, request workflows and public facing materials accordingly. Inspectors have been testing websites and internal repositories for outdated artefacts and for incomplete section 17 registers, with findings leading to remedial action. The Regulator also expects organisations to publish a clear, internal process for data subject access under POPIA and to harmonise this with PAIA request handling so that data subjects receive a coherent experience and records are complete for audit and complaint defence.

Following the 2025 POPIA Regulations amendments, objection and correction/deletion requests may be made through a broader range of channels and without strict reliance on prescribed forms, provided the form used is substantially similar; this flexibility demands that Information Officers and service teams maintain robust intake, logging, and 30 day outcome communication controls that mesh with PAIA timeframes and records management duties. The Regulator has reiterated that, notwithstanding trimming of Regulation 4 references, organisations remain responsible for up to date PAIA manuals that reflect POPIA commencement and the 2021 PAIA Regulations, and that manual currency is tested during inspections.

Breach reporting workflow and e□portal dependencies

Since 1 April 2025, all security compromises must be reported via the Regulator's eServices portal and no longer by email, a process change intended to improve triage and monitoring. This requirement, coupled with the Regulator's consolidation of POPIA legal and IT expertise for breach matters, raises the bar for incident response readiness, including portal user provisioning, template data completeness, and parallel victim notification content and timing. With 2,374 security compromises reported in 2024/25 and a 40% year on year increase in monthly notifications in early 2025/26, the Regulator has publicly pressed organisations to invest in technical and organisational security measures and to ensure timely, accurate notifications to both the Regulator and data subjects.

Enforcement track□record to date and priorities for 2025/26 – *Sanctions, litigation and sectoral signals*

The enforcement picture is now textured by both administrative fines and strategic litigation. The Department of Justice and Constitutional Development received a R5 million infringement notice in 2023 after non compliance with an enforcement notice linked to a 2021 ransomware incident; this is being challenged in court. This case underscores the Regulator's willingness to deploy the upper tier of administrative sanctions and defend them judicially. In education, the Regulator issued an enforcement notice prohibiting publication of matric results in newspapers on privacy grounds and followed with a R5 million infringement notice for non compliance, before the High Court set aside the notices; the Regulator has applied for leave to appeal, which keeps compliance obligations live pending the appellate outcome and demonstrates an appetite to crystallise POPIA principles through precedent.

At the municipal and private sector level, the Regulator has imposed administrative fines on Blouberg Municipality (R500,000) for unlawful online disclosure of an employee's personal information and on FT Rams Consulting (R100,000) for non compliance with an enforcement notice in a direct marketing matter; both unpaid fines have prompted recovery proceedings, signalling follow through. Lancet Laboratories paid a R100,000 infringement notice after failing to notify both the Regulator and affected data subjects of security compromises, highlighting the Regulator's focus on breach notification failures in health adjacent processing. The Regulator has also settled a high profile transparency dispute with WhatsApp over its 2021 privacy policy update, securing commitments to enhance information for South African users and seeking to make the settlement an order of court, an example of negotiated compliance outcomes in platform contexts.

In PAIA enforcement, the Regulator has issued notices compelling disclosure in matters such as Swartkops Sea Salt, with litigation pending, and has broadened use of non compliance notices to drive procedural discipline, including correct form usage and manual currency across sectors. This, combined with public notices to Information Officers and a growing cadence of own motion assessments, indicates that PAIA oversight is shifting from reactive complaint handling to structured, proactive compliance testing.

2025/26 enforcement focus areas reflected in the APP and oversight reports

The APP ties resourcing and indicators to stricter enforcement and modernisation. The Regulator will reconfigure internal units to concentrate technical and legal breach handling skills, expand PAIA compliance assessments of public and private bodies, and monitor prior year assessment recommendations to closure. These moves are supported by programme indicators that increase targets for own initiative PAIA assessments and follow up monitoring, and that set timeliness standards for complaints resolution and mediation. In POPIA, indicators include completions of complex and simple complaints within prescribed timeframes and the progression of a

Code of Conduct for gated access processing. The focus on "gated access" reflects substantial public concern about over collection at secured estates, office parks and retail premises, an area with high visibility and reputational risk for property, retail, and community management sectors.

Forthcoming guidance and codes of conduct – *Guidance Note on transborder information flows*

The APP confirms that the Regulator will issue a Guidance Note on Transfer of Personal Information Outside the Republic, influenced by instruments such as the AfCFTA Digital Trade Protocol and AU Digital Transformation Strategy, and aimed at empowering responsible parties to conduct cross border commerce in a manner consistent with POPIA's eight processing conditions. This will be advisory but will set out expected diligence, including transfer impact assessment concepts and appropriate safeguard selection. Businesses should therefore anticipate alignment with mainstream international practice, including accountability for ensuring comparable protection at destination.

Given global reference points, organisations should expect the Guidance Note to reflect approaches similar to the EU's GDPR Chapter V, UK ICO guidance and Canada's accountability model under PIPEDA, including reliance on contractual safeguards, risk assessments focused on access by public authorities, and enhanced transparency around foreign processing. This comparative perspective is useful for multinational compliance harmonisation ahead of publication.

Code of Conduct for processing at gated accesses

The Regulator will develop a Code of Conduct on the processing of personal information at gated accesses in response to concerns about over processing at controlled entry points. The APP sets the 2025/26 output as a draft code developed and approved, with finalisation in 2026/27, providing a clear horizon for stakeholder engagement and internal readiness work. The code will be issued as a Regulator initiated instrument, reflecting the intention to standardise proportionality, data minimisation, retention, and security expectations across estates, office parks, campuses and retail sites.

What should be top of mind for business now

Breach readiness and portal compliance

From 1 April 2025, breach notifications must be lodged via the Regulator's eServices portal; failure to use the portal, incomplete submissions, or delays risk procedural non compliance and potential enforcement. With monthly notifications rising by 40% in early 2025/26, boards should satisfy themselves that incident response playbooks embed portal workflows, that user credentials and backups are in place, and that data subject notification templates meet POPIA's specificity and timeliness requirements.

Direct marketing governance and call recording

The April 2025 POPIA Regulations amendments require strengthened consent artefacts for electronic direct marketing, recorded telemarketing calls with records available to data subjects on request, and multi channel, no fee objection mechanisms. Organisations should audit consent capture, retention and revocation flows, ensure automated and live telemarketing scripts are aligned, train call centre and sales teams, and calibrate complaint handling timeframes to the Regulations. The Regulator's stated intent to test whether live telemarketing is an "electronic communication" under section 69 underscores the need for conservative compliance and robust evidence keeping.

PAIA discipline: manuals, forms, registers and annual reporting

Given low sectoral compliance and heightened inspection activity, organisations should verify that PAIA manuals reflect POPIA commencement and the 2021 Regulations, that Form 2 is used consistently for requests, that section 17 request registers are up to date, and that the PAIA annual report is submitted by the Regulator's expected window. Parliamentary oversight notes indicate a submission period between 1 April and 30 June for the 2024/25 reporting year, with online submission via the eServices portal and pre requisite registration of the organisation and its Information Officer. Where the Companies and Intellectual Property Commission (**CIPC**) links are used, businesses should be alert to visible non compliance flags on public platforms and associated commercial implications.

Cross□border transfers: anticipate the Guidance Note

Ahead of the Regulator's Guidance Note, organisations should map cross border flows, identify transfer tools in use, and socialise internal expectations that POPIA accountability applies extraterritorially through contracts and oversight of processors. The likely direction of travel mirrors EU/UK practice: adequacy style determinations are not in play in South Africa, so emphasis will rest on contractual safeguards, risk assessment of destination regimes, and transparency to data subjects about foreign processing and potential public authority access.

Gated access processing: prepare for a stricter code

Property, retail, education, healthcare and corporate campus operators should monitor the Code of Conduct process and undertake pre emptive reviews of entry point collection practices, minimising collection to what is strictly necessary, securing storage, shortening retention, and eliminating bulk ID scans and open visitor logs. Early movement here will reduce retrofit cost when the code is finalised and signal good faith in public consultations.

Conclusion

The Information Regulator's 2025/26 APP and related oversight materials point to an assertive but pragmatic regulatory agenda: enforce where harms are acute or systemic, modernise PAIA so it functions credibly alongside POPIA, and provide guidance and codes to standardise expectations in contested processing environments.

For business, the practical imperatives are clear. Treat PAIA as an enforcement priority, not a formality; institutionalise the April 2025 POPIA Regulations across direct marketing and complaints; operationalise the breach e portal; prepare cross border frameworks that can absorb the forthcoming Guidance Note; and remediate high visibility over collection at gates and entry points ahead of the code.

Uncertainty remains around precise legislative timelines, as Cabinet and parliamentary scheduling will drive how quickly PAIA amendments progress, and around how appellate courts will resolve live POPIA interpretive disputes, such as identifiers in result publication and the scope of "electronic communications." These uncertainties are not reasons to delay compliance investment; rather, they reinforce the need for conservative, well documented practices that will survive audit and litigation. Stakeholder engagement opportunities will arise around the Code of Conduct and the Guidance Note, and well prepared organisations can help shape workable, sector sensitive standards while demonstrating leadership to boards, customers and regulators alike.

Ahmore Burger-Smidt

Head of Regulatory

View Profile