WERKSMANS
ATTORNEYS

REGULATORY

Celebrating International Data Privacy Day: “12 years of POPIA – what next?”

19 February 2026 *5 min read*

by Tebogo Sibidla, Director

On 28 January 2026, the global community celebrated International Data Privacy Day. This year, its commemoration landed in a world where privacy and personal information protection are no longer optional, purely legal, regulatory, or compliance issues, but are central to how organisations design systems, deploy services and/or products, collaborate across ecosystems, and earn trust in a digitally connected world.

In South Africa, the Information Regulator hosted a mini-conference themed “12 years of POPIA – what next?”, indicating a shift in our national conversation on privacy and personal information protection from introducing and implementing POPIA to assessing its real-world impact and planning the future of data protection in South Africa.

POPIA in practice: Where are we?

Since POPIA came into full force in 2021, the privacy compliance and regulatory landscape in South Africa have matured. It has shifted from a primarily awareness-raising phase to an era of active enforcement, strategic guidance, and public engagement:

- The Information Regulator (“the Regulator”) has, over the past 4 years, moved from primarily educating stakeholders and increasing POPIA awareness to formal enforcement action, including imposing administrative fines and compliance directives.
- There is increased institutional visibility on privacy incidents due to data breach reporting and transparency obligations, which have compelled organisations to invest in security and incident response resources.
- The Regulator has also issued updated POPIA regulations that clarify procedural expectations on notifications, correction and deletion rights, and Information Officer responsibilities — an important step in operationalising POPIA's protections across both private and public sectors.
- The Regulator has rolled out a centralised eServices portal that supports compliance, reporting, and public engagement on POPIA and PAIA. Through the portal, organisations and the public can, among others, register their Information Officers, submit PAIA annual reports, check and verify whether organisations have complied with their POPIA and PAIA requirements, report security compromises, submit POPIA and PAIA complaints, apply for exemptions and prior authorisations from the Regulator, and view user personal privacy scores and records. Through these tools, the Regulator has likely reduced administrative delays and increased accountability. These e-services are available here. The Regulator has also, through their partnership with the CIPC, made some of these eServices available on the BizPortal.

What next?

During the Regulator’s mini-conference, attendees reflected on whether our current systems make privacy practical, accessible, and enforceable, and highlighted the move towards a society in which privacy is built into how we operate, instead of being bolted onto systems, processes, and documents afterwards. This is consistent with global themes for International Data Privacy Day this year, which focused on promoting privacy-by-design, the idea that data protection should be embedded in technologies and processes from inception, not added after the fact. It also mirrors emerging expectations from regulators and courts around the world, which focus on accountability and built-in safeguards that are demonstrable rather than mere documentation.

For South African organisations, this emphasis aligns naturally with POPIA's conditions for lawful processing of personal information, including accountability, purpose specification, minimality, security safeguards, and data subject participation. Embedding POPIA principles at design stages reduces compliance risk and strengthens trust with stakeholders.

Key focus areas for South African businesses going forward

Given the domestic enforcement environment and the global direction of privacy regulation, we recommend that South African organisations focus their compliance and risk strategies around several core pillars:

1. *Ensure that you can demonstrate privacy, governance, and accountability.* Merely drafting policies is not enough. You must be able to show compliance through documented and monitored organisational practices, such as appointing and effectively deploying Information Officers, and maintaining inventories of personal information processing activities, data protection impact assessments, and evidence of lawful bases for processing.
2. *Embed privacy into your operational design.* Integrate privacy requirements into business logic, technology selection, vendor processes, and customer experience. Design systems with default privacy settings and robust security, and consider data minimisation and retention at the inception of the project.
3. *Implement responsive systems for enabling data subjects to exercise their rights by, among others,* building workflows to respond to requests and objections within POPIA's timelines, and providing transparent privacy notices.
4. *Ensure that you have well-prepared protocols for addressing and reporting data breaches.* Have a tested incident response, communication templates, and escalation plans. Also maintain and analyse logs of your data breaches, and use these to identify trends and reduce future risk.
5. *Where appropriate, move beyond consent as the basis for processing personal information.* Other lawful grounds often better reflect operational realities, especially when coupled with transparency and security safeguards. It is therefore important that you assess whether consent is necessary or whether other lawful grounds are more appropriate, and avoid reliance on consent where it may cause operational fragility or data subject dissatisfaction.

Conclusion

Global and local privacy discussions on International Data Privacy Day demonstrate the push towards more effective and practical privacy engineering, resilient legal compliance, and demonstrable accountability.

In today's digital era, where data powers commerce, innovation, and social interaction, those who design systems that respect privacy from the outset will avoid legal risk and build deeper trust with customers, employees, and the broader public.

Tebogo Sibidla

Director

View Profile