INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

MEDIA BRIEFING ADDRESS BY ADV PANSY TLAKULA

CHAIRPERSON OF THE INFORMATION REGULATOR

INFORMATION REGULATOR PRESENTS INVESTIGATION INTO POPIA AND PAIA CONTRAVENTIONS AND OTHER HIGH-PROFILE CASES

31 AUGUST 2026

INTRODUCTION

Good morning to members of the media, our stakeholders in this briefing today, and greetings to everyone joining us live via our digital platforms. Thank you for taking the time to join us for this media briefing, where we will provide an update on a number of high-profile matters and other key developments from the beginning of this year relating to the implementation of the Information Regulator's mandate.

NEW MEMBERS

Allow me to extend a warm welcome to my fellow Members of the Regulator. I acknowledge Adv Stroom, the full-time Member responsible for PAIA, and Mr Gwala, our part-time Member. I would also like to extend a special welcome to the two new Members who joined the Regulator on 1 August 2026: Ms Noma-Gcina Mntshontshi, the full-time Member responsible for POPIA, and Ms Alison Tilley, our part-time Member who has been re-appointed for another term.

Colleagues, we congratulate you on your appointments and warmly welcome you to the leadership of the Regulator. We are delighted to have you join us and look forward to your strategic insight, support, and guidance as we continue strengthening the institution and advancing the mandate entrusted to us by the Constitution and the laws of the country.

I also wish to acknowledge and extend greetings to our Chief Executive Officer, Mr Mosala, and the team of Executives whose commitment and dedication continue to drive the work of the Regulator.

LAUNCH NEW HEADQUARTERS

Today marks another important milestone for our institution as you meet us in our new headquarters following a year during which we operated both remotely and in the field, while our offices underwent extensive renovations. These improvements were undertaken to ensure that our facilities are fit for purpose, capable of serving members of the public and stakeholders effectively, and conducive to the wellbeing and productivity of the staff of the Regulator.

We are proud to announce our new home and warmly invite members of the public and stakeholders to visit us at 54 Maxwell Drive, North Office Park, Woodmead, Johannesburg.

10 YEARS OF THE REGULATOR & 5 YEARS OF ENFORCEMENT POWERS

It would be amiss if I did not acknowledge that this year holds special significance for the Information Regulator. The Regulator was formally established on 1 December 2016 and in 2026, we mark ten years since our establishment as South Africa's independent institution responsible for the protection of personal information and the promotion of access to information rights.

The past decade has been characterised by both significant challenges and important achievements. We have worked tirelessly to build an institution capable of safeguarding the constitutional rights to privacy and access to information, while navigating a rapidly evolving technological and regulatory landscape. As the CEO would often say, it is not yet “Uhuru”, because we still have a huge task to ensure that we empower all persons to exercise and fully enjoy their information rights.

This year also marks five (5) years since the commencement of POPIA enforcement in 2021, and five (5) years since the Regulator assumed responsibility for the administration and oversight of PAIA from the South African Human Rights Commission. During this period, the Regulator entered a new and critical phase of its evolution. We transitioned from establishing the regulatory framework to actively exercising our statutory enforcement powers. We began receiving complaints, conducting assessments and investigations, issuing enforcement notices, referring matters to the Enforcement Committee, and, where necessary, approaching the courts to uphold and protect the rights enshrined in POPIA and PAIA.

Over the years, we have engaged extensively with stakeholders across both the public and private sectors to foster a culture of compliance with POPIA and PAIA. We have developed and published more than ten guidance notes and regulatory instruments to assist organisations and the public in understanding and exercising their rights and responsibilities under these laws.

At the same time, we have travelled across the country engaging communities, raising awareness, and empowering people to exercise their rights to privacy and access to information.

Ten years on, one reality stands out clearly, the demand for the work of the Information Regulator has grown exponentially.

The world in which data protection and access to information operate today is vastly different from the one that existed when PAIA and POPIA were enacted. Technological innovation continues to reshape every aspect of society. The collection, sharing, and processing of personal information occur on an unprecedented scale. Artificial intelligence, automated decision-making systems, biometric technologies, and digital platforms are increasingly embedded in both public and private sector operations.

These developments present immense opportunities for economic growth, innovation, and improved service delivery. However, they also introduce new and complex risks to privacy, transparency, accountability, and human rights.

Against this backdrop, our role as the Information Regulator has never been more important. As we reflect on the past decade, we remain committed to ensuring that technological progress is matched by responsible governance, that innovation is accompanied by accountability, and that the fundamental rights of all people in South Africa continue to be protected and advanced.

POPIA

Security Compromises (Data Breaches)

As a country, South Africa is experiencing an increasingly hostile cybersecurity environment, with security compromises (data breaches) and cyberattacks exposing the personal information of millions of people, and this is one of our growing concerns. The Regulator therefore finds itself operating at the intersection of privacy, technology, security, commerce, law enforcement and fundamental rights. It is a challenging environment. But it is also an environment in which the work of the Regulator has never been more necessary.

Public and private bodies that hold personal information are, in effect, entrusted with information that belongs to individuals (data subjects). When this information is compromised, the consequences can be devastating. To date, the Regulator has received over eight thousand (8000) security compromises, with over one thousand, two hundred and twenty (1220) received from 1 April 2026 to date, which is less than five (5) months from the beginning of this financial year, with this trend, we may have over three thousand (3000) reported data breaches by the end of the financial year.

The consequences of a security compromise can extend well beyond the exposure of personal information. Depending on the depth, a security compromise can interrupt essential services, damage institutional credibility, undermine public confidence and have significant economic consequences.

SABS Enforcement Notice

Last week we issued the South African Bureau of Standards (SABS) with an Enforcement Notice following SABS suffering a significant ransomware attack in 2024. The attack encrypted its information systems and caused a severe disruption to its operations. This prompted us to conduct our own-initiated assessment of the circumstances surrounding the security compromise, and to assess other compliance areas under POPIA.

Following the completion of that assessment, we issued an Enforcement Notice against SABS. We found that they have violated the POPIA conditions for lawful processing of personal information, such as processing excessive, irrelevant information; having inadequate consent mechanisms; weak security safeguards;

failure to address known vulnerabilities; lack of incident response plans; and failure to inform data subjects of collection methods, amongst many other breached conditions.

We have instructed SABS to improve security and data protection practices by revising its policies, conducting thorough personal information impact assessments, and implementing security measures to protect personal information it processes within 90 days of receipt of the Enforcement Notice.

We want to emphasise that this enforcement action is not being taken simply because SABS was the victim of a cyberattack. The Regulator recognises that cyberattacks are increasingly sophisticated, and that no organisation can guarantee that it will never be attacked.

The SABS incident must also be viewed against the broader cybersecurity environment in which South Africa currently operates. The Auditor-General has identified cybersecurity weaknesses across government and public entities, including ageing infrastructure, compromised security environments, cybersecurity skills deficits, weaknesses in third-party risk management and underinvestment in cybersecurity. In her assessment, shortcomings were identified and significant vulnerabilities highlighted.

The more dependent organisations become on these systems, the more important it is to ensure that the personal information processed through them is secure. We warn against organisations that treat the protection of personal information as merely a tick-box exercise rather than an important organisational operational requirement that needs to be planned for and adequately resourced.

Direct Marketing

Another matter that keeps me awake at night is the growing frustration among data subjects with direct marketing through unsolicited electronic communications. Last year the Regulator received over three thousand, eight hundred (3800) complaints. 10% of complaints received were related to direct marketing. Direct marketing therefore remains a material area of concern. The complaints demonstrate continued concern among data subjects about the use of their personal information for marketing purposes, particularly through electronic communications.

Two direct marketing matters (OUTsurance & MTN) have been referred to the Enforcement Committee. These matters are significant because they raise important questions regarding the interpretation and application of section 69 of POPIA on direct marketing by means of unsolicited electronic communications. The outcomes of these matters will be important in providing greater certainty to both responsible parties and data subjects. We emphasise that POPIA is not an obstacle to legitimate commerce. It is a framework within which commerce must take place lawfully and fairly.

The Regulator welcomes the recent amendments to the Consumer Protection Act Regulations aimed at curbing unsolicited marketing communications, including spam calls. We regard the pre-emptive block register as an important additional measure in addressing the scourge of unwanted direct marketing. Registration in the pre-emptive block register does not displace the obligations imposed by POPIA, bodies have an obligation to obtain consent from a person before sending unsolicited direct marketing communication to them.

We have engaged with the National Consumer Commission to identify areas in which the two institutions can work jointly in creating public awareness and receiving and handling complaints. We welcome this cooperation. We trust that closer collaboration between us and the National Consumer Commission will strengthen the fight against unwanted electronic communications and provide greater protection to consumers and data subjects.

Madlanga Commission and POPIA

The issue of privacy is also increasingly intersecting with matters concerning the criminal justice system. On 23 July 2025, the President established the Judicial Commission of Inquiry into Criminality, Political Interference and Corruption in the Criminal Justice System chaired by Justice Mbuyiseli Madlanga. Since its establishment, the Commission has undertaken important work in examining allegations concerning criminality, political interference and corruption within structures of the criminal justice system.

In February 2026, the Commission referred to the Regulator concerns relating to the alleged unlawful processing of personal information by Dr Imogen Mashazi, the former City Manager of the Ekurhuleni Metropolitan Municipality. We accepted the referral and initiated an own-initiative investigation in terms of section 76(3) of POPIA. That investigation has been completed. The matter was referred to the Enforcement Committee, and appropriate action will be taken.

The Regulator subsequently received further referrals from the Commission on 4 August 2026. Investigations have been initiated in relation to Major General Lesetja Senona, Mr Vusimuzi Matlala, Mrs Linda Gxasheka and Sergeant Fannie Nkosi. These investigations are ongoing and, as a matter of fairness and due process, the Regulator will not comment on the merits of those matters and will do so following completion of the investigation.

Data privacy and data protection issues now affect how law enforcement obtains information, how personal information is processed, and how it is used in criminal investigations.

POPIA is still a relatively young legislative framework, and the development of jurisprudence is essential to clarifying how the Act is to be interpreted and applied. We therefore appreciate the role of the judiciary in developing the law of data protection in South Africa. The courts provide an important mechanism through which the powers of the Regulator, the rights of data subjects and the obligations of responsible parties can be tested and clarified.

Matric results and development of jurisprudence.

The same principle applies to the ongoing litigation concerning the publication of matriculation results by the Department of Basic Education. We continue to challenge the publication of matriculation results by the Department. Although the High Court set aside our Enforcement and Infringement notices in December 2025 and dismissed its application for leave to appeal this year in June, the Regulator maintains that the matter raises important questions about the application of POPIA to learners' information and has therefore approached the Supreme Court of Appeal.

Our view is that regardless of the outcome of litigation on the interpretation of POPIA, such outcome must be sound in law and provide the Regulator with adequate clarity on the interpretation of POPIA whilst protecting the rights of every person in South Africa.

We will continue to pursue matters of principle through the appropriate legal processes where we believe that clarification is necessary. The matric results matter illustrates why judicial engagement with POPIA is so important. It is through these cases that South Africa will develop a body of jurisprudence that will provide greater certainty to data subjects, public bodies and private organisations alike.

Other POPIA investigations

The Regulator is currently investigating and assessing several other matters involving both public and private sector organisations, including the National Credit Regulator, Truecaller, Pick n Pay, the Gauteng Department of e-Government, Land Bank, and Standard Bank. These investigations and assessments seek to establish whether the conduct or practices of the bodies comply with POPIA and, where appropriate, will culminate in findings and recommendations.

PAIA

As we often remind the public, we have a dual mandate and have a responsibility to monitor and enforce compliance with the Promotion of Access to Information Act. We are currently in the process of reviewing PAIA to improve the legislation and ensure that the law truly serves the members of the public, so that they can exercise their constitutional rights and access records held by public and private bodies.

With recent high-profile matters in which we found contraventions of PAIA and subsequently issued Enforcement Notices, we have noted a concerning trend. Increasingly, the Enforcement Notices are being challenged, with bodies instituting review proceedings against the Regulator. While PAIA is intended to promote transparency and access to information, some bodies are opting to take us on review or to court rather than complying with the Enforcement Notices directing them to release requested records. In recent Enforcement actions, Sibanye Stillwater and the

Johannesburg Stock Exchange are amongst the bodies that have approached the courts to challenge our decisions rather than disclose the information as ordered.

Annual reporting

We are empowered, in terms of sections 32 and 83 (4) of PAIA, to receive PAIA Annual Reports from public and private bodies regarding the statistics on how each body has processed requests for access to any information held by the body. This allows us to track whether requests are handled within legal timeframes and how internal appeals are resolved. The submission of the annual reports fosters transparency with the public and stakeholders regarding how constitutional rights to information are upheld. Failure to submit PAIA annual reports prompt that we conduct compliance assessments and formal investigations, which may be followed by enforcement proceedings.

Noted improvements but with concerns

For the 2025/26 reporting cycle, the Regulator received PAIA Annual Reports between 1 April 2026 and 30 June 2026. During this period, four hundred and seventeen (417) of the eight hundred and fifty-three (853) public bodies, including national and provincial departments, municipalities, public entities, universities and TVET colleges, submitted their Annual Reports. This translates to an overall compliance rate of approximately 52%.

While this represents a notable improvement from the 2024/25 financial year, during which only three hundred and fifty-eight (358) public bodies submitted reports, reflecting a compliance rate of just 33%, the current figures remain a cause for concern.

The reality is that nearly half of all public bodies are still failing to meet their statutory reporting obligations under PAIA. This not only undermines transparency and accountability in the public sector but may also impede the ability of members of the public to exercise their constitutional right of access to information. Compliance with PAIA is not a mere administrative requirement, it is a fundamental component of open, responsive and accountable governance.

Our greatest concern remains the low level of compliance among municipalities. Of the 257 municipalities across the country, only ninety-one (91) submitted their Annual

Reports, resulting in a compliance rate of approximately 35%. This is particularly troubling given that municipalities are the sphere of government closest to the people and are at the forefront of service delivery. Access to information at local government level enables communities to hold municipal authorities accountable, monitor the use of public funds, and participate meaningfully in decisions that affect their daily lives.

The continued low level of compliance in local government therefore poses a significant risk to transparency, accountability and public participation. In response, the Regulator will intensify its compliance monitoring and assessment activities and strengthen its engagement with the relevant oversight structures to ensure that municipalities fulfil both their legal obligations and their constitutional responsibilities to the public. Other low levels of compliance that remain a matter of concern are with Political Parties, TVET Colleges, Schedule 3 and Major public entities.

The Public Protector has also been failing to submit the Section 84 (b) (x) report. This report must be submitted as a statutory requirement under PAIA. This report demonstrates the nature of access to information complaints referred to the Public Protector, the number of complaints, and the outcome of investigations and the resolution of matters.

Other key compliance concerns and enforcement activities

The Regulator conducted compliance assessments of Schedule 3A entities, Non-Profit Organisations and Real Estate Agencies. In an overview of the compliance status, low levels of compliance with PAIA have been observed. Public and private bodies tend to ignore recommendations, with the understanding that there are no punitive and stringent enforcement measures emanating from PAIA assessments, hence, the review of PAIA to improve the Regulator's powers to enforce and issue sanctions remains an apex priority.

IMPROVED SYSTEMS

As a maturing organisation, we are committed to providing guidance that enables public and private bodies to comply before infringing on human rights. The Regulator will therefore continue to strengthen its guidance and compliance work so that public and private bodies continue to advance its digital transformation agenda through the expansion of its digital platforms and the introduction of new online regulatory services aimed at improving accessibility, service delivery and regulatory effectiveness. We introduced several new digital services, such as the POPIA and PAIA Complaints Management System, to enable members of the public to lodge POPIA complaints more seamlessly.

POPIA Exemption Application allows responsible parties to submit applications to request exemptions electronically and allows these applications to be managed through an integrated internal workflow.

POPIA Prior Authorisation Application, which was developed to enable responsible parties to apply for prior authorisation electronically and reduce the manual application burden.

We urge members of the public to utilise our iSupport Query Management System, which is a centralised platform for members of the public and other stakeholders to submit general queries to the Regulator, with queries routed internally to the appropriate divisions for management and efficient response.

CONCLUSION

As we conclude, let me reaffirm that the Regulator remains steadfast in its commitment to protecting and advancing the rights to privacy and access to information. We will continue to resolve complaints with urgency, provide practical guidance to public and private bodies, promote a culture of compliance, and where necessary, exercise our enforcement powers without fear, favour or prejudice.

The rights we are entrusted to protect are fundamental to human dignity, accountability and democracy. As South Africa continues to navigate an increasingly digital future, the Regulator will remain a vigilant guardian of these rights, ensuring that technological progress is accompanied by transparency, responsibility and respect for the law.

Thank you.

---- END ----

For media enquiries, contact Nomzamo Zondi, Senior Manager Communication and Media, 078 674 2598 or NZondi@inforegulator.org.za.