WERKSMANS
ATTORNEYS

DIGITAL MEDIA & ELECTRONIC COMMUNICATIONS

Code Red to Code Regulated: South Africa's Data, AI and Cybersecurity Shift in 2025, and What's to Come in 2026?

21 January 2026 *7 min read*

by Armand Swart, Director, Hlonelwa Lutuli, Associate and Hanán Jeppie, Candidate Attorney

South Africa's data protection, cybersecurity, and artificial intelligence ("**AI**") landscape matured significantly in 2025. Key developments included: new POPIA regulations; a joint cyber security standard for financial institutions coming into effect; the Information Regulator issuing draft regulations for healthcare data; and the publication of an AI report by financial sector regulators. At least two notable POPIA-related judgments were also handed down.

This article recaps 2025's key developments and forecasts what is on the horizon for 2026.

Amended POPIA Regulations

On 17 April 2025, amended regulations ("**Amended Regulations**") to the Protection of Personal Information Act 4 of 2013 ("**POPIA**") and the Promotion of Access to Information Act 2 of 2000 ("**PAIA**") came into effect. The Amended Regulations contained several notable changes, including:

Direct Marketing: Organisations must obtain a data subject's written consent before conducting direct marketing by sending unsolicited electronic communication. Consent cannot be inferred from silence or pre-ticked boxes (i.e. opting out), and a copy must be provided upon request. Consent obtained via telephone or automated calls must be recorded.

Enhanced IR Complaints Processes: The list of persons who may submit complaints to the Information Regulator ("**IR**") has been expanded to include persons acting on a data subject's behalf or in the public interest.

Negotiating Fines with the IR: Responsible parties can negotiate instalment plans for administrative fines, with affordability assessed on a case-by-case basis.

Access and Monitoring: The process for data subjects' objections to processing has been simplified: it is free and can be lodged by post, fax, email, or WhatsApp.

The Amended Regulations will lead to improved and more efficient POPIA and PAIA processes, with increased direct marketing enforcement also expected.

Data Breaches

Data breaches remained a key focus for the IR, even though fewer enforcement notices were issued in 2025. Some 1,607 breaches were reported between April and September 2025 – a 60% increase from 2024. On 1 April 2025, the IR launched a mandatory security compromise reporting tool on its eServices portal to streamline reporting.

Data breach reporting and enforcement are likely to remain a focus area for the IR in 2026, and organisations should ensure their data breach response plans are up to date. Responsible parties should ensure any operators are aware of their breach reporting obligations.

Cybersecurity for Financial Institutions

The Prudential Authority ("**PA**") and the Financial Sector Conduct Authority ("**FSCA**") published a Joint Standard on Cybersecurity and Cyber Resilience Requirements ("**Joint Standard**"), which took effect in June 2025. Financial institutions ("**FIs**") – such as banks, insurers, and fund administrators – have to comply.

Key requirements include a comprehensive cybersecurity strategy, cyber resilience capabilities, employee training, continuous monitoring, incident response plans, regular control testing, vulnerability assessments, and malware protection. The Joint Standard requires FIs to report any material cyber incident to financial sector regulators.

Enforcement action by the PA and FSCA is likely in 2026, and it is possible that significant fines may be issued for non-compliance, similar to those issued for Financial Intelligence Centre Act / FICA non-compliance.

Health Data Regulations

On 26 September 2025, the IR published draft regulations ("**Draft Regulations**") on the processing of personal information relating to health or sex life ("**health data**"). The regulations apply to insurance companies, medical schemes, pension funds, administrative bodies, and employers working for such bodies (each a "**Relevant Body**"). The following is highlighted at a bird's eye view:

Lawful Basis: Where a Relevant Body processes health data for compliance with laws, pension regulations, or collective agreements, it may only do so to comply with the law; or to pursue the legitimate interests of the Relevant Body or data subject. The Draft Regulations have been criticised for requiring both a lawful basis to process health data as special personal information (section 32) and as personal information (section 11). Additionally, legitimate interest is not considered a lawful basis for processing health data under POPIA – which is consistent with the EU and UK GDPR approach.

Security Safeguards: A Relevant Body must employ specific measures to comply with POPIA's security safeguard requirements. The Draft Regulations contain an unusual provision requiring a written agreement with a data subject before processing their health data, which requires further clarification.

Cross-Border Transfers: Organisations must notify data subjects of intended transfers and the level of protection afforded to their health data, unless the data subject has consented or the transfer is in their legitimate interests.

Record Retention and Deletion: Health data must not be retained longer than necessary for its original purpose, unless required by law or contract, or the data subject consents. Data must be destroyed or de-identified once no longer necessary.

Final regulations are likely to be published in 2026.

Notable Case Law Developments

Judicial interpretation of POPIA's provisions remained limited in 2025. Two notable decisions emerged.

De Jager v Netcare Limited ("Netcare"): De Jager challenged the admissibility of surveillance footage on the basis that it breached POPIA. The court held that it was in the interests of justice to admit the footage and that under POPIA, the processing was necessary for Netcare to enforce its rights (POPIA, section 27). The Court raised concerns regarding the processing of "non-data subjects" and children's data in the footage but stated that its hands were tied by section 6(e) of POPIA exempting compliance relating to judicial functions. The court's reliance on this exemption is misplaced.

IR v Department of Basic Education ("DBE"): The IR sought to prevent the DBE from publishing matric results by examination number, arguing learners could be indirectly identified through sequential number allocations. The High Court rejected this, ruling that the publication of an examination number alone does not constitute processing personal information. The DBE published the 2025 matric results on 13 January using examination numbers. The IR has applied for leave to appeal.

AI

In November 2025, the FSCA and PA published a joint report on AI in the South African financial sector. The report outlines key opportunities, such as enhanced data analytics and cybersecurity capabilities, while highlighting significant risks including data privacy concerns, bias, and systemic vulnerabilities.

Though not binding, the report urges FIs to adopt international standards for AI explainability, establish strong data governance with board-level oversight, and ensure adequate disclosure to consumers when AI is used in decision-making.

The report signals that South African regulators are proactively implementing the national AI framework, although specific AI laws or regulations are not imminent in 2026.

Child Data

Protections for children online and their personal data are increasing globally. The UK's Age-Appropriate Design Code mandates high default privacy settings for minors, and Australia banned social media for children under 16 in late 2025. POPIA already provides some protection for children's personal information, but targeted regulations addressing children's digital life could strengthen safeguards given the risk of harm.

Cloud Computing

The National Policy on Data and Cloud may drive more structured approaches to data residency and public-sector cloud procurement. Organisations should anticipate closer alignment with POPIA's cross-border transfer rules and clearer shared-responsibility frameworks between cloud customers and providers.

Conclusion

Going into 2026, organisations should be mindful of improved POPIA processes, as well as a regulatory focus on electronic direct marketing compliance and data breach reporting. FIs must ensure they comply with the Joint Standard or risk facing enforcement action. Final healthcare regulations are likely to be published in 2026, while AI policy continues to develop, especially for FIs. Ultimately, strategic investment in your business's data, AI, and cyber security compliance is critical.

Armand Swart

Director

View Profile

Hlonelwa Lutuli

Associate

View Profile