JUTA
POPIA PORTAL

ISSUE NO 72 • DATA PRIVACY ROUNDUP 2026 Q3 • SEPTEMBER 2026

DATA PRIVACY ROUNDUP 2026 Q3

1. OVERVIEW

This quarter's data privacy update highlights a clear shift from compliance on paper to compliance that can be proved. Locally, the Information Regulator's recent POPIA and PAIA enforcement notices show that public and private bodies must report security compromises, justify refusals of access, honour settlement agreements and keep proper evidence of their decisions. Internationally, developments in Canada and the UK point in the same direction: regulators are focusing on accountable AI deployment, meaningful safeguards, and accessible internal complaint-handling. For South African responsible parties and information officers, the practical message is simple: privacy governance must be documented, responsive and capable of withstanding regulatory scrutiny.


Photo: iStock

2. RECENT ENFORCEMENT NOTICES: POPIA AND PAIA ENFORCEMENT GAINS MOMENTUM


Photo: iStock

The Information Regulator's recent **enforcement notices** show a clear move from guidance and conciliation to binding remedial orders. The notices deal with both POPIA and PAIA, but the common theme is the same: public and private bodies must be able to justify their decisions, keep proper evidence, and comply with the Regulator's directions.

Central Johannesburg TVET College: internal disclosure becomes a POPIA breach

The Regulator issued a POPIA enforcement notice against Central Johannesburg TVET College after employees' credential verification reports, collected for qualification and criminal-record checks, were mistakenly circulated to unauthorised employees. The Regulator found that the college had breached POPIA's accountability condition, further processing limitation, security safeguards, and notification obligations. The mistaken disclosure was incompatible further processing, and the fact that it was accidental did not remove the obligation to notify both the Regulator and affected data subjects of the security compromise. The college was ordered to register its information officer and deputies, notify

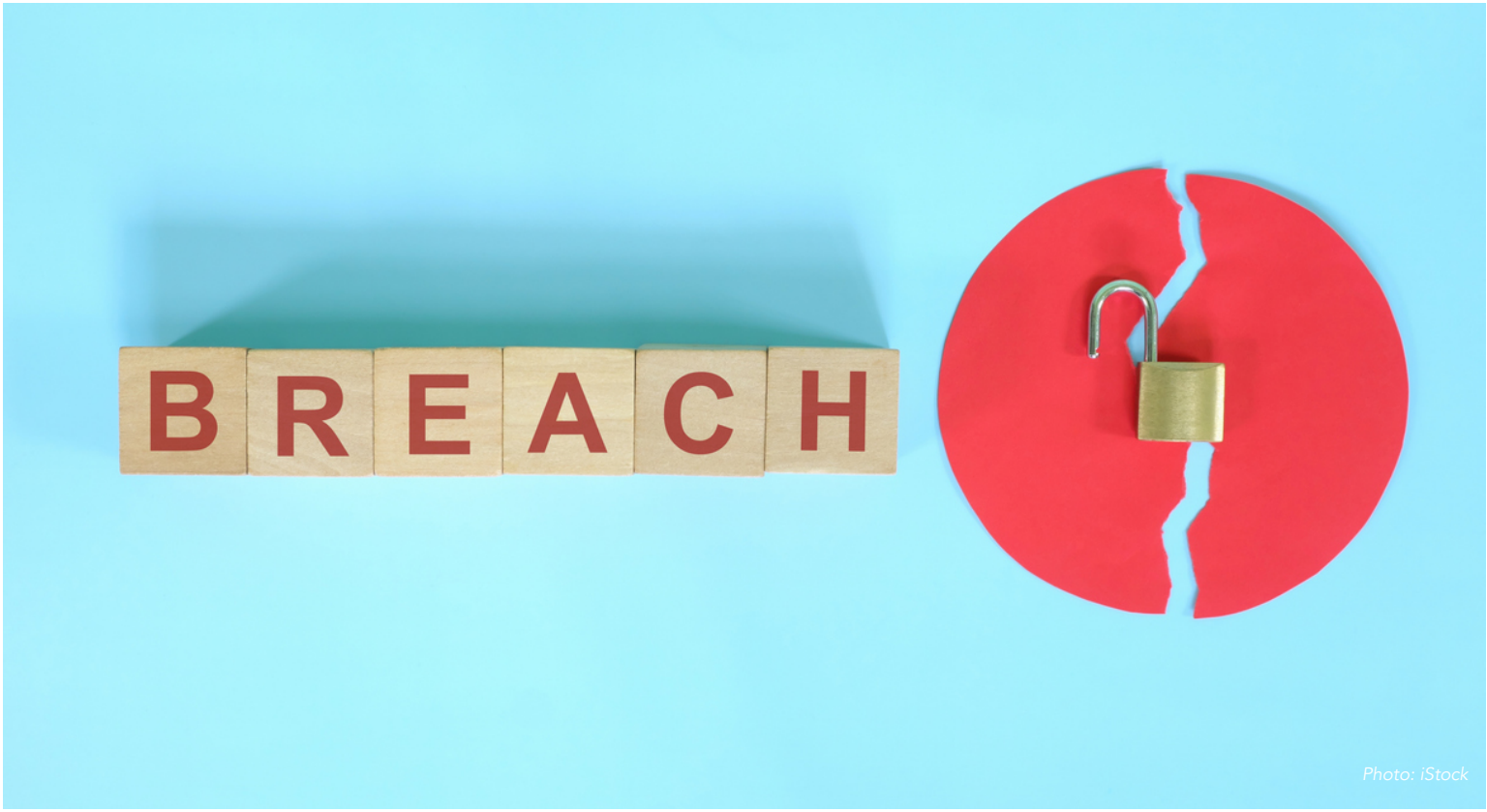

Photo: iStock

the Regulator and affected data subjects, apologise to the complainants, act against the employee involved, develop and submit a POPIA compliance framework, and conduct POPIA awareness and training.

Sibanye-Stillwater: PAIA exemptions require evidence, not assertion

The Sibanye-Stillwater notice is a significant PAIA development for private bodies. The dispute arose after the Centre for Applied Legal Studies requested annual compliance reports linked to Sibanye's 2019–2023 Social and Labour Plans for its Eastern and Western Platinum Mines. Sibanye refused access on commercial-confidentiality grounds under PAIA. The Regulator accepted that the reports may contain commercial information but found that Sibanye had not provided sufficient factual evidence to show likely commercial harm or disadvantage in negotiations. The Regulator ordered disclosure of the reports and emphasised that simply quoting an exemption is not enough. Private bodies must substantiate PAIA refusals with specific facts, not general claims of reputational or commercial prejudice.

Gauteng Department of Health: settlement certificates are not optional

The Gauteng Department of Health notice concerned PAIA requests by journalist Jeff Wicks for Mamelodi Hospital payment records and internal audit reports linked to the broader Babita Deokaran/Tembisa Hospital investigations. The Department failed to respond to the original requests and internal appeal, resulting in deemed refusals, and later entered into a settlement agreement to disclose the records with certain redactions. It then failed to comply fully with that settlement. The Regulator treated the settlement certificate as binding and rejected bare assertions of compliance where the requester had provided specific evidence of missing records. The Department was ordered to disclose the outstanding records and, where records could not be found or did not exist, provide detailed affidavits explaining the searches conducted.

These notices show that the Regulator is increasingly prepared to use enforcement notices to compel both data protection and access-to-information compliance. For responsible parties and information officers, the lesson is practical: mistakes must be reported, refusals must be evidenced, settlements must be honoured, and compliance must be provable. Non-compliance with an enforcement notice may itself trigger criminal consequences, including fines or imprisonment.

3. CANADA: DEEPFAKES = PERSONAL INFORMATION

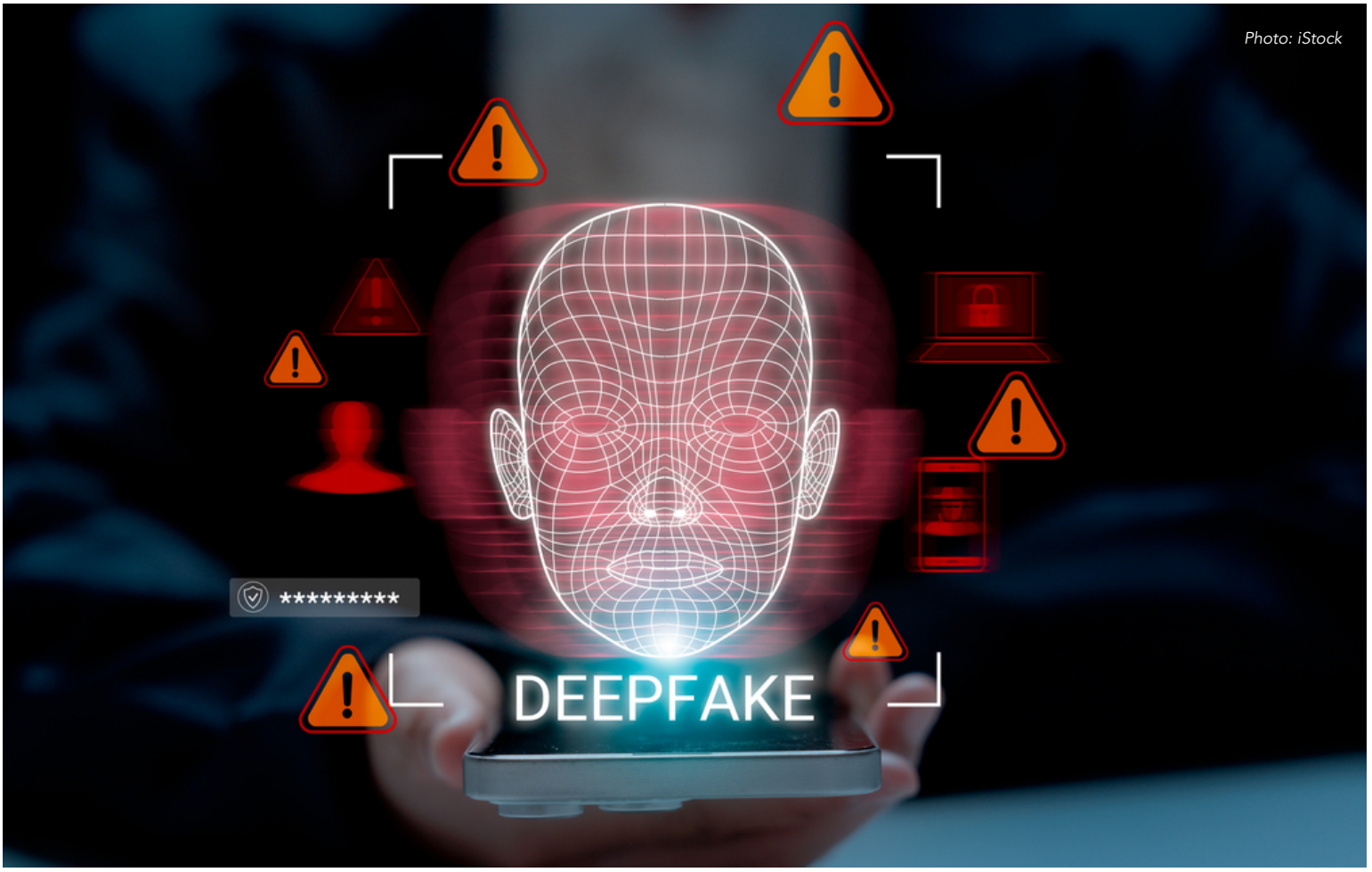

Photo: iStock

Canada's **Privacy Commissioner** has recently treated AI-generated deepfakes as a privacy law issue, not only an online safety issue. In June 2026, the Office of the Privacy Commissioner of Canada found that X Corp and xAI violated Canada's federal private-sector privacy law, PIPEDA, after Grok's image-generation tool was used to create and share sexualised deepfakes of identifiable individuals, including women and children. The OPC found that AI-generated deepfakes can constitute personal information even where the image is synthetic or inaccurate, because it still appears to be about an identifiable person. It also found that sexualised deepfakes contain sensitive personal information, require express consent, and would fall outside the reasonable expectations of people whose ordinary online images are repurposed in this way. Importantly, the OPC rejected the idea that the platform could shift responsibility to users who entered the prompts: X Corp and xAI developed, deployed and made the tool available during commercial activity, and therefore remained accountable for consent, appropriateness, safeguards and risk mitigation. The practical lesson is clear: organisations deploying generative AI tools should:

- assess foreseeable misuse before launch
- treat outputs about identifiable people as personal information
- build robust safeguards into the design of the tool; and
- be able to prove that those safeguards are effective.

4. UK: INTERNAL COMPLAINT-HANDLING PROCESS REQUIRED

Photo: iStock

The UK has moved toward more structured internal complaint-handling as part of data protection accountability. Under the Data (Use and Access) Act 2025, which inserted new complaint-handling provisions into the UK Data Protection Act 2018, controllers must give people a way to lodge data protection complaints directly with them, acknowledge complaints within 30 days, take appropriate steps to respond without undue delay, keep complainants informed, and communicate the outcome. The **UK's Department for Science, Innovation & Technology** explains that this creates new statutory requirements for controllers to put complaint-handling processes in place, and the **ICO** has confirmed that the new duty is now in force.

South Africa does not currently have an equivalent general statutory obligation requiring every responsible party to maintain an internal POPIA complaints process before a complaint reaches the Information Regulator. POPIA provides for complaints to be made to the Regulator in writing, and the Regulator may then investigate, refer the matter to the Enforcement Committee or take other action. However, the UK approach is a useful governance benchmark for South African responsible parties: privacy notices and PAIA manuals should give data subjects a clear route to raise POPIA concerns internally; Information Officers should log, acknowledge, investigate and respond to complaints; and organisations should keep evidence of how complaints were handled. This may help resolve matters earlier and, if the Regulator later becomes involved, demonstrate accountability and responsiveness.