JUTA
POPIA PORTAL

ISSUE NO 68 • DATA PRIVACY ROUNDUP 2026 EDITION 3 • MAY 2026

DATA PRIVACY ROUNDUP 2026 EDITION 3

1. OVERVIEW

Two recent developments stand out in the POPIA landscape. The first is the Information Regulator's draft code of conduct for the processing of personal information at gated accesses. The second is the growing international focus on AI-generated imagery and the privacy risks created when realistic images or videos of identifiable individuals can be generated without their knowledge or consent. Both developments are reminders that POPIA applies just as much to everyday operational practices as it does to new technologies.


Photo: iStock

2. THE REGULATOR'S DRAFT CODE OF CONDUCT FOR GATED ACCESSES

Photo: iStock

The Information Regulator has developed a draft **Own Initiative Code of Conduct of the Information Regulator on the Processing of Personal Information at Gated Accesses in South Africa**. Its purpose is to explain how POPIA's eight conditions for lawful processing apply in controlled-access environments where access control, CCTV, guards, scanning systems, and similar security measures involve the processing of personal information.

The Regulator's **2025/2026 Strategic Plan** explains why this work was prioritised. It states that the code is being developed following public concern about over-processing at gated accesses. The plan also indicates that the project would move from a first draft to a final version to be gazetted under section 61(2) of POPIA.

Although often described as a code for 'gated communities', the draft has a wider scope. It applies to processing at gated accesses in residential estates and buildings, as well as in government and military buildings, healthcare facilities and educational institutions. The Regulator held a stakeholder session on 18 February 2026 and invited comments by 4 March 2026. The next step is expected to be publication of an amended version in the *Government Gazette*.

The draft is notable for its practical guidance. It distinguishes between minimal and excessive data collection. For visitors, it treats name, purpose of visit, vehicle registration where relevant, and time of entry and exit as necessary, while identifying ID copies or photos, home address, email address, personal phone number, and employer details as excessive. For employees, it contrasts basic access-related details with full ID numbers, home addresses, personal phone numbers, next-of-kin details, and unjustified biometric data. It also proposes retention periods for different categories of records, including 30 to 90 days for access-control logs, depending on context and operational need.

Photo: iStock

The draft also takes a firm position on consent and governance. It states that consent is not voluntary where access depends on providing personal information, and cautions against relying on implied consent where people are not properly informed. It also requires responsible parties to manage operators contractually and encourages impact assessments where higher-risk processing could expose data subjects to significant harm.

What responsible parties should know:
The draft makes it clear that access-control practices are not exempt from ordinary POPIA discipline. Responsible parties should be able to justify what they collect at the gate, explain why it is necessary, define how long it will be kept, and restrict access to it appropriately. The draft's examples make routine collection of ID copies, photographs, contact details or biometrics much harder to justify where those are collected by habit rather than necessity.

Responsible parties should also review how roles are allocated across owners, body corporates, homeowners' associations, managing agents, security companies, and technology vendors. The draft expects proper operator agreements, clear instructions, and appropriate security safeguards where third parties handle access data.

It also warns against treating consent as a shortcut. Where a person must provide information to gain entry, consent is unlikely to be truly voluntary. In this setting, responsible parties should focus on justification, necessity, openness, and minimality, rather than assuming that a signature in a register resolves the POPIA analysis.

Finally, the draft points to a more structured compliance model for access control. Privacy notices, retention rules, staff training, incident response planning and, where necessary, impact assessments are increasingly part of baseline POPIA compliance in this setting, especially where CCTV, scanning tools, biometrics or cloud-based access systems are used.

3. AI-GENERATED IMAGES AND PRIVACY RISK


Photo: iStock

On 23 February 2026, 61 data protection authorities issued a **Joint Statement on AI-Generated Imagery** and the Protection of Privacy. The statement was issued in response to concern about AI systems that generate realistic images and videos of identifiable people without their knowledge or consent. It specifically highlights non-consensual intimate imagery, exploitative content, defamatory depictions, and heightened risks to children and other vulnerable groups. The statement also makes the regulatory position clear: organisations developing or using these systems must comply with privacy and data protection laws, implement safeguards, and ensure effective reporting and takedown mechanisms.

Regulators are increasingly framing this as a privacy issue, not merely a content-moderation issue. Their concern is not limited to the final synthetic image. It extends to the use of source photographs, the modelling of a person's likeness, prompts that identify real individuals, the retention of uploads and prompts, and the creation of images that can humiliate, sexualise or exploit a person without their knowledge. The joint statement expressly links the issue to privacy, dignity, and safety and notes that the creation of non-consensual intimate imagery may also amount to criminal conduct in some jurisdictions.

The controversy around Grok on X turned these concerns into a live enforcement issue. In January 2026, Ofcom opened a **formal investigation into X** under the UK Online Safety Act to assess whether X had complied with its duties to protect users from illegal content following reports that Grok-generated sexualised imagery, including imagery involving children, was being circulated on the platform. On 3 February 2026, the UK Information Commissioner's Office opened investigations into both X Internet Unlimited Company and xAI, saying the reported use of Grok to generate non-consensual sexual imagery of individuals, including children, raised serious concerns under UK data protection law.

The EU response has also been significant. On 26 January 2026, the European Commission launched a **formal Digital Services Act investigation** into Grok and X's recommender systems, focusing on whether systemic risks linked to Grok had been properly assessed and mitigated. On 17 February 2026, Ireland's Data Protection Commission (DPC) opened a formal **GDPR inquiry** into X Internet Unlimited Company concerning the apparent creation and publication on X of harmful, non-consensual intimate or sexualised AI-generated images involving EU and European Economic Area (EEA) data subjects, including children. The DPC said it would examine compliance with core GDPR obligations, including lawfulness, the principles of processing, data protection by design and default, and data protection impact assessment (DPIA) requirements.

This issue has also started to drive law reform. In the UK, the government **announced** in February 2026 that the creation of non-consensual intimate images, including sexually explicit deepfakes, had been criminalised and that platforms would be required to remove abusive images within 48 hours under new legislation. In the EU, key lawmakers have now backed proposals to ban AI 'nudifier' systems and apps that generate unauthorised sexually explicit images of real people.

Criminal enforcement against individuals who create or possess AI-generated sexual abuse material, particularly involving children, is happening. In the US, the Department of Justice **announced** charges in 2024 against a man accused of producing, distributing and possessing AI-generated sexually explicit images of minors. The FBI has also highlighted sentencing in cases involving the use of generative AI to create child sexual abuse material from images of real children.

What responsible parties should know for POPIA compliance

For responsible parties, the key point is that AI-generated imagery does not fall outside POPIA because the output is synthetic. If a system is trained on, prompted with, or used to create depictions of identifiable people, personal information is involved. Privacy risk arises not only from the final image, but also from the collection of source images, the modelling of a person's likeness, the retention of prompts and uploads, and the ability to generate intimate or defamatory depictions without the person's knowledge or consent. The familiar POPIA questions therefore remain central: what is the lawful basis, was the person adequately informed, is the use compatible with the original purpose, is the processing proportionate, and were appropriate safeguards built in from the start?

The second lesson is that dignity and abuse risks need to sit at the centre of the compliance analysis. Regulators are increasingly treating these systems as capable of causing immediate and serious harm, especially where children are involved. Responsible parties should therefore not assess AI image tools only through an information-security or innovation lens. They should also assess whether a proposed use could facilitate humiliation, exploitation, sexualisation, impersonation, harassment or reputational harm. That is especially important where employees, customers, learners, patients or children may be affected.

The third lesson is around governance. The joint statement and the Grok investigations point toward the same expectation: privacy and safety safeguards must be designed into the system, not bolted on after public backlash. Organisations using AI tools to generate avatars, marketing visuals, simulations or personalised content should examine vendor terms, training and retention settings, misuse-prevention features, removal channels, escalation procedures, and human review controls before deployment. If a tool can realistically be used to sexualise or humiliate identifiable people, a responsible party should assume that ordinary POPIA principles such as minimality, openness, security safeguards, and accountability will be scrutinised closely.

Finally, the Grok episode shows how quickly a novelty feature can become a legal and reputational crisis. The current regulatory trend is clear: authorities are moving from abstract discussion about generative AI to concrete action where image-generation tools are used to process personal data in harmful ways. For responsible parties, AI image-generation should now be treated as a live privacy-risk area requiring active governance, rather than an experimental tool sitting outside the normal POPIA framework.

4. CONCLUSION

These two developments show POPIA operating as a practical governance framework rather than a narrow compliance checklist. The draft gated-access code is a reminder that routine security processes must still satisfy necessity, transparency, retention control, and accountability. The growing regulatory concern about AI-generated imagery is a reminder that new technologies do not displace ordinary privacy laws. In both contexts, the message is the same: know what personal information you are processing, be clear about why you are processing it, keep the processing proportionate, and make sure your systems, vendors and internal practices can withstand scrutiny.

Photo: iStock

5. WANT TO READ MORE?

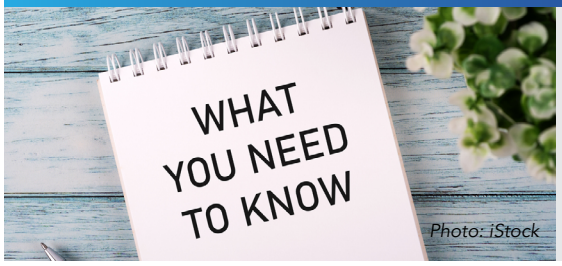

Photo: iStock

Chapter 4: Who is held accountable for POPIA compliance
Chapter 5: Information security management
Chapter 7: Special personal information and children's personal information
Chapter 9: Minimality and information quality
Chapter 10: Collecting and creating personal information

juta