JUTA
POPIA PORTAL

ISSUE NO 54 • DATA PRIVACY ROUNDUP FOR 2025 Q2 • MAY 2025

DATA PRIVACY ROUNDUP FOR 2025 Q2

1. OVERVIEW

In this issue of our Data Privacy Roundup, we discuss what is happening in South Africa and abroad to bring you the latest data privacy and protection news.

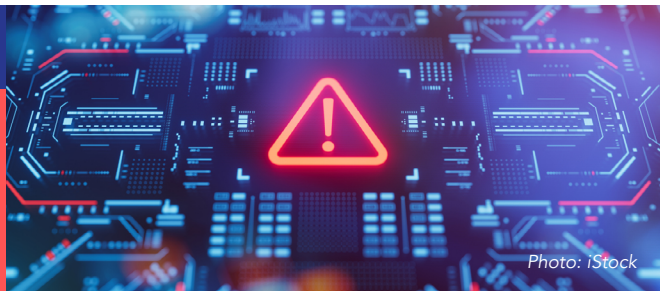
Photo: iStock

2. WHAT HAS BEEN HAPPENING AT HOME

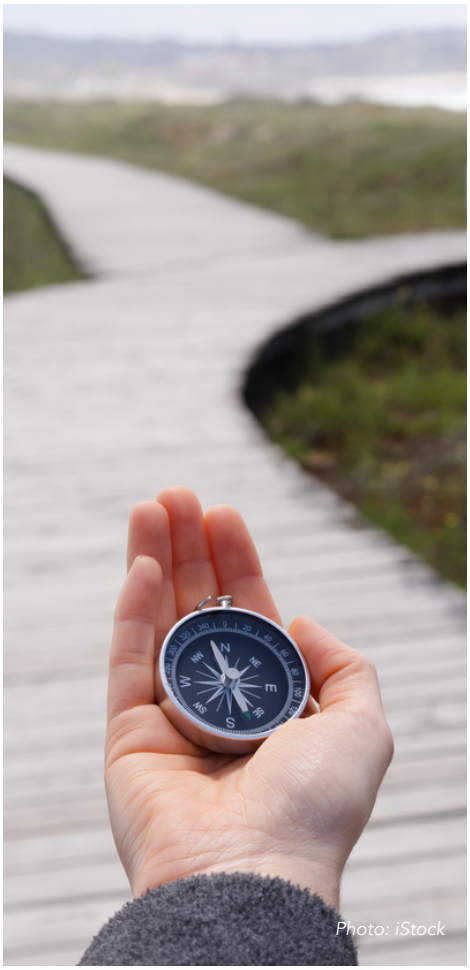
Photo: iStock

2.1. The Information Regulator held a stakeholder consultation session

On 5 March, the Information Regulator held a consultative session to discuss its annual performance plan and address key issues. Some of its plans are to:

- resolve 85% of simple complaints within three months, using mediation and quick resolution strategies
- publish revised draft regulations for the processing of health information or sex life 'very, very soon'
- develop a Code of Conduct specifically for processing personal information in gated communities
- conduct at least 80 PAIA compliance assessments before 31 March 2026
- take action to enforce the guidance note on direct marketing
- be involved in regulating AI governance, especially when personal information is being processed in the AI system; and
- publish an annual assessment report highlighting the assessments conducted and their outcomes.

2.2. Annual reports of Public and Private companies must be submitted in terms of PAIA

The Information Regulator invited public and private bodies to submit annual PAIA reports by 30 June. Information officers must log into the eServices portal and upload their documents between 1 April and 30 June 2025.

2.3. CPA Regulations on the opt-out registry

The Department of Trade and Industry recently published amended CPA Regulations on the national 'Do Not Contact Me' list and asked interested parties to submit their comments. This concept is not new, but it raises many questions and potential conflicts with POPIA and the Information Regulator. For instance, who has jurisdiction over direct marketing complaints? The IR or the NCC?

2.4. Pam Golding data breach

A third party accessed Pam Golding's customer relationship management (CRM) system on 7 March. Pam Golding took immediate action to secure their systems and contain the incident. They notified the affected clients, reported it to the Information Regulator, and reported it to SAPS. No banking or financial details were compromised.

3. WHAT HAS BEEN HAPPENING ABROAD

3.1. EU Commission will withdraw the e-Privacy Regulation

The e-Privacy Regulation was a proposed European Union law meant to improve privacy and confidentiality in electronic communications. It was originally proposed in 2017 to replace the e-Privacy Directive and align it with the GDPR.
As of February 2025, the Commission has decided to withdraw the proposal. Many disagreements and resistance from European lawmakers led to the proposal stalling. The Commission also said that it is now outdated.

3.2. European Data Protection Board publishes a statement on age assurance

The EDPB issued a statement that outlines ten principles to guide the proper handling of personal data when verifying an individual's age or age range. They are:

- Ensure age checks uphold all individual rights, prioritising children's best interests.
- Implement age verification measures appropriate to the associated risks and do not infringe on individual rights.
- Avoid unnecessary data collection that could lead to identifying, profiling, or tracking individuals.
- Only process essential age-related information for explicit, legitimate purposes.
- Use reliable methods that accurately verify age.
- Process personal data legally and fairly and inform users clearly about its use.
- If using automated systems, comply with regulations and protect individual rights.
- Incorporate privacy measures into age verification systems from the outset.
- Implement appropriate technical and organisational measures to protect personal data during age verification.
- Implement governance methods that hold service providers accountable for their age verification methods and demonstrate compliance with data protection laws.

3.3. ICO publishes guidance for employers

The UK Information Commissioner's Office (ICO) published guidance for employers on managing employment records in compliance with data protection laws.[1] They provide practical guidance as well as checklists for employers to use. Key points include:

- Relying on employee consent as a lawful basis for processing is discouraged due to power imbalances. Instead, processing should be justified by:
  - fulfilling employment contracts
  - complying with laws and regulations; or
  - the employer's legitimate interests.
- Collecting and keeping employment records:
  - What lawful basis can apply to employment records?
  - How do you keep records accurate and up-to-date?
- When an employer can use employment records:
  - Sharing with other people or organisations; and
  - What to consider when providing references.

4. WHAT'S NEXT?

Our roundups will keep giving you data privacy updates from local and abroad. If you are interested in reading more about the topics covered in this article, refer to these chapters under the 'Understand the Law' tab:

- Chapter 5: Information Security Management
- Chapter 16: Direct Marketing

Photo: iStock