JUTA
POPIA PORTAL

ISSUE NO 56 • DATA PRIVACY ROUNDUP FOR 2025 Q3 • JULY 2025

DATA PRIVACY ROUNDUP FOR 2025 Q3

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. Amendments to POPIA Regulations

The Information Regulator published major amendments to the POPIA Regulations on 17 April 2025. Improving the rights of individuals and imposing stricter obligations on organisations processing personal information. These changes clarify definitions such as "complainant," "complaint," "day," "office hours," and "relevant body," providing clearer guidance for compliance.

Data subjects now have expanded avenues to object to the processing of their personal information and to request corrections or deletions. These requests can be made free of charge through various channels. Organisations are mandated to inform individuals of these rights at the point of data collection and must respond to such requests within 30 days. Please click here for the full article on the amended Regulations.

2.2. SAA data breach

South African Airways (SAA) experienced a significant cyberattack on 3 May 2025, which temporarily disrupted its website, mobile app, and several internal systems. The airline's disaster management and business continuity protocols were activated promptly, allowing core flight operations and essential customer service channels to continue functioning. All affected systems were restored later the same day.

SAA published a media statement confirming that it launched a forensic investigation to determine if any personal information was compromised and reported the incident to the State Security Agency, SAPS, and the Information Regulator. The airline has committed to notifying affected individuals if a data breach is confirmed and is taking steps to strengthen its cybersecurity measures.

3. WHAT HAS BEEN HAPPENING ABROAD


Photo: iStock

3.1. EU AI Act Code of Practice soon to be released

On 22 April 2025, the European Union Artificial Intelligence Office released preliminary guidelines to clarify the responsibilities of general-purpose AI (GPAI) model providers under the new EU AI Act. These draft guidelines identify seven key areas that will be elaborated on in the final version and offer initial interpretations to help stakeholders prepare.

The guidance is particularly important because the EU AI Act assigns distinct legal obligations to GPAI model providers, separate from those developing or deploying AI systems that incorporate these models. Given the complexity of the AI value chain, the guidelines are intended to help organisations understand their role and determine whether they fall into the GPAI model provider category.

3.2. An increase in data breaches in the US

The healthcare, education, and financial sectors have seen some of the most severe breaches since the end of last year.

Healthcare sector:

- UnitedHealth recently confirmed that up to 190 million Americans' personal and medical information was compromised in a data breach last year, making it one of the largest breaches in U.S. history.
- Frederick Health Medical Group reported a ransomware attack on 27 January 2025 that affected over 934,000 individuals and exposed medical records, Social Security numbers, and insurance details.

Education sector:

- PowerSchool, a major provider of education management software, suffered a breach that affected data from more than 62 million students and teachers across North America.
- In New York, cyberattacks on multiple Long Island school districts compromised student data from over 10,000 individuals.

Financial and public sectors:

- TD Bank disclosed an insider threat in which an employee exposed the personal banking details of 43 clients, including their Social Security numbers.
- Insight Partners, a leading venture capital firm, suffered a breach that revealed sensitive investor information, such as tax and banking records.
- Berkeley Research Group involved in legal cases with the Catholic Church, was targeted in an attack that potentially exposed sensitive data tied to sexual abuse victims.
- U.S. Customs and Border Protection acknowledged using a compromised messaging app, raising concerns over national security and internal communications.

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 in the Understand the Law tab:

- Chapter 5 – Information Security Management
- Chapter 18 – Data subject rights

Photo: iStock