JUTA
POPIA PORTAL

ISSUE NO 39 • DATA PRIVACY ROUNDUP FOR 2024 Q3 • SEPTEMBER 2024

DATA PRIVACY ROUNDUP FOR 2024 Q3

1. OVERVIEW

In this issue of our Data Privacy Roundup, we chat about some of the data breaches that have happened in South Africa and their impact on South Africans. We also look abroad and discuss some regulatory developments, such as the CNIL's updated AI Guidelines and Rhode Island's Data Transparency and Privacy Protection Act.

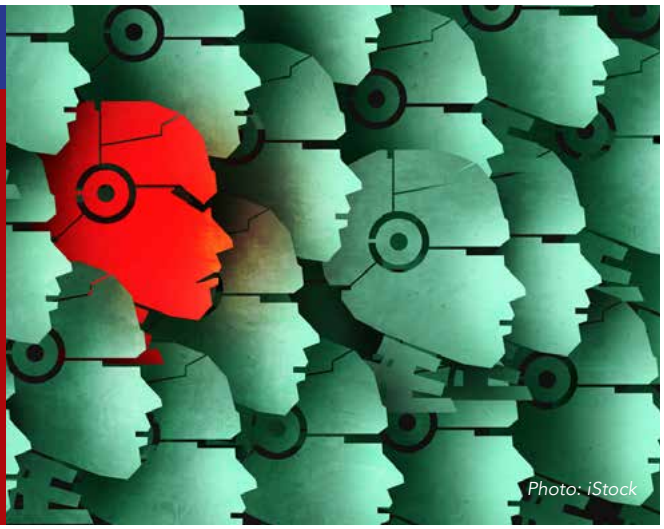
Photo: iStock

2. WHAT HAS BEEN HAPPENING AT HOME

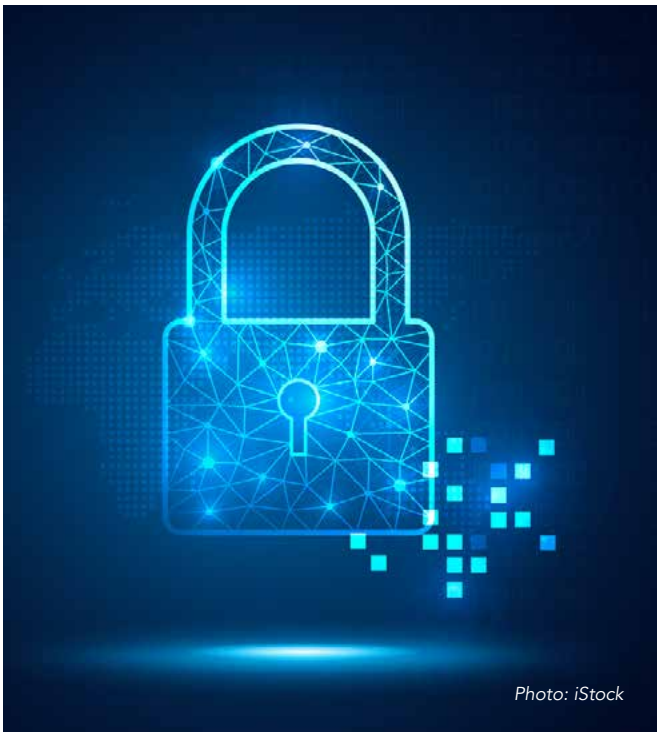
Photo: iStock

2.1. Ransomware attack on South Africa's National Health Laboratory Service (NHLS)

On 22 June, ransomware targeted the NHLS, effectively blocking communication between the labs and the information system.

'It has been established that sections of our system have been deleted, including in our backup server and this will require rebuilding the affected parts. Unfortunately, this will take time and investigations thus far have not advanced enough for us to give a timeframe toward the restoration of our systems and full service. …

All patient data is safe. The investigation indicated that a ransomware virus was utilised to target selected points in the NHLS IT systems, rendering them inaccessible and blocking communication from the LIS and other databases to and from users.' [1]

2.2. Sibanye-Stillwater's global IT systems under attack

Sibanye-Stillwater suffered a cyber attack. They implemented containment measures to isolate affected systems. This is ongoing, and their IT experts are still investigating the extent of the attack.

3. WHAT HAS BEEN HAPPENING ABROAD


Photo: iStock

3.1. Rhode Island General Assembly passed State Privacy Bill

The Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA) will be in effect on 1 January 2026.

'While the RIDTPPA resembles the existing comprehensive state privacy laws in many ways, the Act contains some notable drafting ambiguities, such as the use of multiple terms to refer to covered data, particularly with respect to certain exemptions (e.g., "personal data" is defined, but "personally identifiable information" is not). The drafting ambiguities bring a new layer of complexity to interpreting the law as the list of comprehensive state privacy laws continues to grow.'[2] – Hunton Andrews Kurth

3.2. EU AI Act published in the Official Journal. Will enter into force on 1 August 2024.

The Act has been published in the Official Journal of the European Union, which means that we now have dates!

- 1 August 2024: The EU AI Act will be in force.
- 1 February 2025: Chapter 1 (General provisions) and Chapter II (Prohibited AI practices) come into effect.
- 1 May 2025: The codes of Practice for General Purpose (GPAI) will be finalised.
- 1 August 2025: Additional rules will apply. Chapter III Section 4 (Notifying Authorities), Chapter V (General Purpose AI Models), Chapter VII (Governance), Chapter XII (Confidentiality and Penalties), and Article 78 (Confidentiality) will apply, except for Article 101 (fines for General Purpose AI providers).
- 1 February 2026: The Commission will issue guidelines.
- 1 August 2026: The whole Act (except for Article 6(1) and its corresponding obligations) will be in force (this is one of the categories of high-risk AI systems).
- 1 August 2027: Article 6(1) and corresponding obligations will be in force. The whole Act will now be in force.

3.3.The French Data Protection Authority (CNIL) published new guidelines on AI

The CNIL published the final version of its guidelines after a round of public consultations.

The guidelines 'help professionals reconcile innovation with respect for people's rights for the innovative and responsible development of their AI systems.' [3]- CNIL Press release.

An English version of the AI how-to sheets is available here.

3.4.RockYou2024 leak: 10 billion passwords shared

A hacker uploaded billions of login details in early July on BreachForums (a popular hacking site). It is mainly a collection of existing leaked passwords. The 2024 leak built on from RockYou2021 when it released 1.5 billion passwords. Users who reuse passwords are in danger as threat actors will likely target them again even though most of the data is old.

'The Cybernews team believes that attackers can utilize the ten-billion-strong RockYou2024 compilation to target any system that isn't protected against brute-force attacks. This includes everything from online and offline services to internet-facing cameras and industrial hardware.

… combined with other leaked databases on hacker forums and marketplaces, which, for example, contain user email addresses and other credentials, RockYou2024 can contribute to a cascade of data breaches, financial frauds, and identity thefts.'[4] - Cybernews

4. WHAT'S NEXT?

Our newsletters will keep giving you data privacy updates from home 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 2.4: Considering international guidelines and foreign law
- Read our ISM tips for SMEs – Byte 9 to see what you should have in place if a breach occurs.

Photo: iStock