JUTA
POPIA PORTAL

ISSUE NO 35 • DATA PRIVACY ROUNDUP FOR 2024 Q2 • JULY 2024

DATA PRIVACY ROUNDUP FOR 2024 Q2

1. OVERVIEW

In this issue of our Data Privacy Roundup, we highlight the Information Regulator's new eServices portal, and their updates to the guidance note for political parties and independent candidates ahead of the elections. We also look at the EU AI Act, privacy concerns about WorldCoin's iris scanning, and the $22 million ransom paid by UnitedHealth.

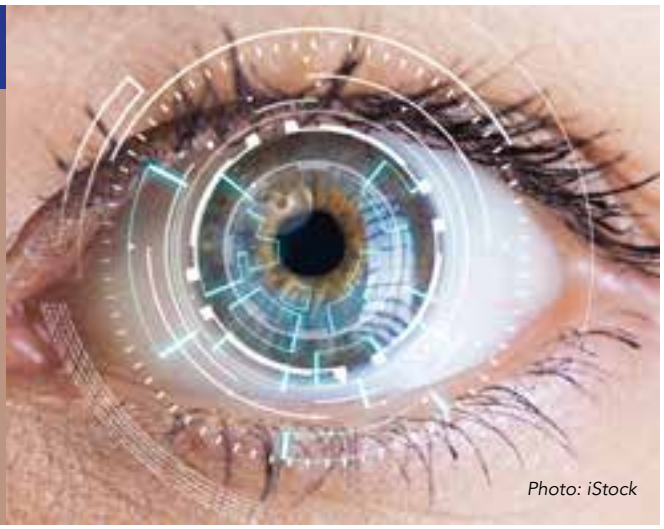

Photo: iStock

2. WHAT HAS BEEN HAPPENING AT HOME

Photo: stock.adobe.com

2.1. Regulator launches new Information Officer portal

The Information Regulator has launched a new eServices portal where Information Officers and Deputy Information Officers must register, and where organisations can submit their PAIA annual reporting. If your Information Officer was registered previously, you have to migrate your user profile to the new eServices Portal.

Why an eServices portal? According to the Regulator:

'Our commitment to modernisation drives our provision of innovative eServices at the Regulator. Embracing the digital age, we're streamlining and automating our services progressively, initiating a transformative journey. The eServices platform offers automated solutions to simplify intricate processes. From digitalising conventional paperwork to optimising operational tasks, our goal is to revolutionise and expedite your experience. Stay tuned as we progressively introduce automated services aimed at replacing traditional manual forms. Your efficiency and convenience are at the core of our endeavor.'

2.2. New guidance note on political parties and independent candidates

The regulator published a new guidance note on the processing of personal information of voters and the countering of misinformation and disinformation during elections.

These are some of the key takeaways:

- Political parties and independent candidates may process a data subject's political persuasion, a type of special personal information, in terms of section 31 of POPIA for the purposes of forming a political party, participating in its activities, recruiting members, canvassing supporters and for campaigning. You can read more about this in paragraph 7.4.4.
- Political parties and independent candidates may not obtain the personal information of voters from data brokers, lead generators or through applications that generate personal information such as telephone numbers automatically. They may however, collect the personal information directly from the voter, from a public record such as the voter's roll, or if a voter deliberately made their personal information public. Read more about the direct collection rule in chapter 10.
- Campaigning for votes does not constitute direct marketing.
- Requests for donations are direct marketing and any unsolicited electronic direct marketing must comply with the requirements in section 69 of POPIA. Read more about direct marketing in chapter 16.
- Where a data subject's consent is required for direct marketing via fax, SMS or email, the words 'opt in' or 'yes' must be used to obtain consent, and 'opt out' or 'no' to withhold consent. Where consent is obtained by telephone or automatic calling machine, the data subject's response must be recorded.

3. WHAT HAS BEEN HAPPENING ABROAD

Photo: iStock

3.1. European Council approves first worldwide rules on AI

The Council of the EU approved a ground-breaking law aiming to harmonise rules on artificial intelligence, the Artificial Intelligence Act.

'The adoption of the AI act is a significant milestone for the European Union. This landmark law, the first of its kind in the world, addresses a global technological challenge that also creates opportunities for our societies and economies. With the AI act, Europe emphasizes the importance of trust, transparency and accountability when dealing with new technologies while at the same time ensuring this fast-changing technology can flourish and boost European innovation.' - Mathieu Michel, Belgian secretary of state for digitisation, administrative simplification, privacy protection, and building regulation.

Photo: iStock

3.2. UnitedHealth paid hackers a $22 million ransom

The UnitedHealth Group CEO confirmed that he authorised the payment of a $22 million ransom to hackers during a hearing before a US Senate committee on Finance. Cybercriminals obtained access to systems that provide payment, revenue management and e-prescriptions to healthcare providers. The system was not protected by two-factor or multi-factor authentication, which are the bare basics for protecting personal data.

3.3. Privacy concerns: WorldCoin's use of biometrics

According to their website, WorldCoin has done 5,4 million ID verifications in more than 160 countries. The ID verification requires people to have their irises scanned in exchange for a digital ID and free cryptocurrency. The Office of the Privacy Commissioner for Personal Data in Hong Kong served an enforcement notice on WorldCoin in May, claiming that the personal data collection is unnecessary and excessive. This follows earlier bans in Spain and Kenya.

8. WHAT'S NEXT?

Photo: stock.adobe.com

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:

- Read chapter 7 for more about special personal information including political persuasion, health, and biometric information.
- Chapter 16 covers direct marketing, but keep in mind that the Regulator recently changed their earlier approach to telemarketing. Read more about this controversial issue here.