JUTA
POPIA PORTAL

ISSUE NO 32 • DATA PRIVACY ROUNDUP FOR Q3 2023 - Q1 2024 • MAY 2024

DATA PRIVACY ROUNDUP FOR Q3 2023 - Q1 2024

1. OVERVIEW

In this issue of our Data Privacy Roundup, we uncover the significant improvements made by the Information Regulator in enforcing data privacy regulations in South Africa and explore the latest developments in data privacy and protection worldwide.


Photo: stock.adobe.com

2. WHAT HAS BEEN HAPPENING AT HOME ...

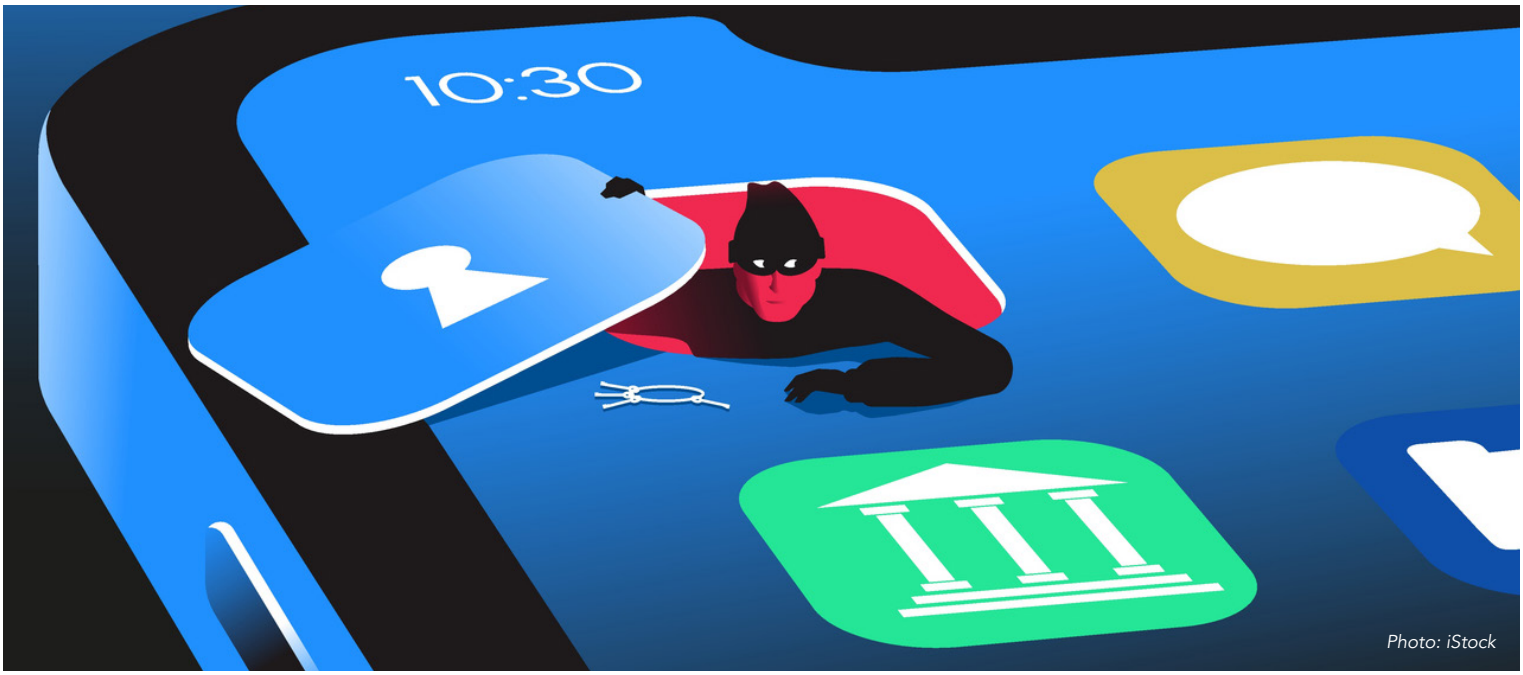

Photo: iStock

2.1. Outcomes of various investigations relating to PAIA and POPIA

The Information Regulator held a press briefing on 26 March 2024, during which it shared the outcomes of high-profile investigations relating to the Promotion of Access to Information Act 2 of 2002 (PAIA) and the Protection of Personal Information Act 4 of 2013 (POPIA). The briefing covered the outcomes of PAIA complaints, updates on enforcement notices, and compliance assessments on political parties and government departments.

The Regulator provided the following updates on POPIA investigations and enforcement notices:

• **TransUnion**

The Information Regulator issued an enforcement notice to TransUnion regarding its breach of personal information. TransUnion failed to secure the confidentiality of its customer's personal information, implement appropriate technical measures, prevent unlawful access, and follow its information security policies. The Regulator ordered TransUnion to develop security measures, conduct an audit, and perform a Personal Information Impact Assessment (PIIA) by 26 May 2024.

• **Dis-Chem**

Dis-Chem was issued with an enforcement notice in September 2023 after being targeted by a brute force attack that compromised their customers' personal information. Dis-Chem has complied with the recommendations and requirements stated in the notice, and the Regulator has closed its file on Dis-Chem.

• **SAPS**

The SAPS was issued an enforcement notice following a breach of personal information regarding sexual assault victims in Krugersdorp. The SAPS complied with the enforcement notice, resulting in the closure of the matter. However, a new investigation is pending due to another breach involving the personal information of victims shared on WhatsApp groups.

• **Companies and Intellectual Property Commission (CIPC)**

The Information Regulator is conducting a new investigation involving a data breach at CIPC that allegedly started in 2021 when hackers gained unauthorised access to CIPC's database.

Photo: iStock

2.2. Information Regulator issued its first enforcement notice on direct marketing

The Information Regulator issued an enforcement notice in response to a direct marketing complaint against F.T. Rams Consulting, a training institution. The Regulator provided further information in a media statement on 27 February 2024. Despite numerous requests from a data subject to opt out of marketing emails, F.T. Rams Consulting continued to send unsolicited messages, violating various sections of POPIA. The Regulator found the company in breach of conditions for the lawful processing of personal information and section 69 of POPIA regarding direct marketing via electronic communication.

Chairperson Adv Pansy Tlakula emphasised the Regulator's commitment to enforcing regulations on direct marketing. The Regulator ordered F.T. Rams Consulting to cease unsolicited marketing, obtain consent before sending such communications, comply with other prescribed procedures within 90 days, or face penalties for non-compliance, including fines up to R10 million or imprisonment.

Various industries eagerly await guidance from the Information Regulator on whether telephone calls should be considered electronic communication.

3. WHAT HAS BEEN HAPPENING ABROAD ...

3.1. UK ICO publishes new guidance for organisations using biometric data

The ICO released a guidance note that aims to help organisations and providers of recognition systems understand how data protection laws apply to biometric data. The guidance note covers biometric data, its special category status, its use in recognition systems, and what organisations should, must, and could do to comply with the law and good practice.

3.2. EU-US Privacy Framework update

Efforts have been ongoing in the EU-US Data Privacy Framework to establish a new framework following the invalidation of the EU-US Privacy Shield by the CCJEU's Schrems II ruling in 2020. Despite initial setbacks, including concerns raised by the European Parliament's Committee on Civil Liberties and Home Affairs regarding the adequacy of safeguards, the European Commission ultimately made an adequacy decision on 10 July 2023.

This decision confirms that the United States offers a level of protection for personal data comparable with that of the EU under the new framework. The framework incorporates new binding measures to address concerns raised by the CJEU, such as restricting U.S. intelligence services' access to EU data to what is deemed necessary and proportionate.

3.3. One of the most significant data breaches in US history

Real Estate Wealth Network, a New York-based online real estate education platform, experienced a massive data breach in December 2023, with over 1.5 billion records exposed. The leaked data, totaling 1.16 TB, included sensitive information such as names, addresses, phone numbers, property history, court judgments, mortgage details, homeowner association liens, obituary information, bankruptcy details, and tax information. The breach also revealed property ownership data of significant celebrities like Kylie Jenner, Britney Spears, and Floyd Mayweather, raising concerns about potential social engineering attacks and financial fraud.