JUTA
POPIA PORTAL

ISSUE NO 43 • DATA PRIVACY ROUNDUP FOR 2024 Q4 • NOVEMBER 2024

DATA PRIVACY ROUNDUP FOR 2024 Q4

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. National Policy on Data and Cloud

On 31 May 2024, the Department of Communications and Digital Technologies published the National Policy on Data and Cloud. The Policy applies to National and Provincial Government, Organs of State, and the private sector.

It aims to promote cloud services and improve data management and protection. The policy recognises that sharing data across borders is essential, especially for businesses and international companies, and it warns against unnecessary restrictions that could harm trade.

It focuses on creating a safe and secure online environment to allow data to be shared internationally in compliance with legislation. The policy supports economic growth by encouraging innovation and securing data use across sectors.

Photo: iStock

2.2. Information Regulator update

The Information Regulator held a briefing session on 11 September 2024, where Adv Pansy Tlakula gave an update on their activities over the past few months. They have issued quite a few enforcement notices in the last few months to:

- Blouberg Municipality;
- Lancet Laboratories;
- Electoral Commission; and
- WhatsApp LLC.

They also mentioned sharing a draft guidance note on direct marketing with key stakeholders. The Regulator held a stakeholder engagement session on 25 September 2024 to discuss the final version of the guidance note, which should be published shortly after. The full briefing can be read here.

2.3. Legal Practitioners Fidelity Fund (LPFF) hack

The LPFF sent a letter to its stakeholders on 25 June 2024 saying that some of its systems had been affected.
'Preliminary investigations suggest that an entity with administrative rights successfully breached our security protocols and accessed certain sensitive data.'

The letter recommends security safeguards but does not elaborate on the 'sensitive data'. Considering their primary purpose is to compensate attorneys' clients who suffer losses due to theft of money or property entrusted to the attorney, this could be banking details.

3. WHAT HAS BEEN HAPPENING ABROAD

Photo: iStock

3.1. Botswana published Data Protection Bill

The 2024 Data Protection Bill will repeal the current Data Protection Act of 2001. The original Data Protection Act was delayed many times due to criticism that it did not adequately address many data privacy issues.

3.2. Noyb filed nine complaints against X

X (previously Twitter) started using European users' data in their AI 'Grok' without informing them or asking for their consent. Noyb (Max Schrems' brainchild) came to the rescue and filed complaints with the Irish Data Protection Commission (DPC). It appears that the DPC was concerned with mitigation measures, so Noyb pushed for a full investigation. In a recent Noyb article, Schrems said:

> 'We have seen countless instances of inefficient and partial enforcement by the DPC in the past years. We want to ensure that Twitter fully complies with EU law, which – at a bare minimum – requires to ask users for consent in this case.

The Noyb article continues:

> 'In addition to the lack of a valid legal basis, it's highly unlikely that Twitter properly distinguishes between data from users in the EU/EEA and other countries where people don't enjoy GDPR protection. The same goes for sensitive data under Article 9 GDPR (for which the "legitimate interest" argument is not available under the law), such as data revealing ethnicity, political opinions and religious beliefs, as well as other data for which a "legitimate interest" could theoretically be claimed. With the introduction of its AI technology, Twitter appears to have breached a number of other GDPR provisions.' [1]

[1] 'Twitter's AI plans hit with 9 more GDPR complaints', available at https://noyb.eu/en/twitters-ai-plans-hit-9-more-gdpr-complaints.

3.3. Uber fined 290 million Euro

The Dutch Data Protection Authority fined Ube servers in the United States without adequate security measures. Sensitive data such as location data, payment details, and criminal and medical records were involved.[2]

> 'For a period of over 2 years, Uber transferred those data to Uber's headquarters in the US, without using transfer tools. Because of this, the protection of personal data was not sufficient. The Court of Justice of the EU invalidated the EU-US Privacy Shield in 2020.
> According to the Court, Standard Contractual Clauses could still provide a valid basis for transferring data to countries outside the EU, but only if an equivalent level of protection can be guaranteed in practice. Because Uber no longer used Standard Contractual Clauses from August 2021, the data of drivers from the EU were insufficiently protected, according to the Dutch DPA. Since the end of last year, Uber has used the successor to the Privacy Shield.
> This is the third fine that the Dutch DPA imposed on Uber. The Dutch DPA imposed a fine of 600,000 euro on Uber in 2018, and a fine of 10 million euro in 2023. Uber has objected to this last fine.' [3]

3.4. The Information and Privacy Commission (IPC) of New South Wales published a guide on PIAs on AI systems for comment

The IPC has published guidelines and asked privacy practitioners to give their feedback on whether the guide is helpful.
'The Guide has been developed to support agencies in understanding, assessing and mitigating privacy risks in relation to the use of AI systems and projects when undertaking Privacy Impact Assessments (PIAs). It also supports agencies in undertaking privacy related assessments under the NSW AI Assessment Framework (AIAF) and the National framework for the assurance of artificial intelligence in government'. [4]

4. WHAT'S NEXT?

Photo: iStock

These roundups will continue to provide you with 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
- Chapter 14: Transborder information flows and extraterritorial application
- Read our ISM tips for SMEs – Byte 9 to see what you should have in place if a breach occurs.