JUTA
POPIA PORTAL

ISSUE NO 70 • DATA PRIVACY ROUNDUP FOR 2026 Q2 • JULY 2026

DATA PRIVACY ROUNDUP FOR 2026 Q2

1. OVERVIEW

POPIA enforcement is becoming more assertive, with the Information Regulator increasingly moving beyond guidance and enforcement notices. In this roundup, we look at recent enforcement actions, what they signal for compliance, and what organisations can learn from them.

We also look at recent EU developments, including changes to the AI Act and proposed updates to the GDPR and ePrivacy rules, which may affect South African organisations processing the personal data of people in the EU.

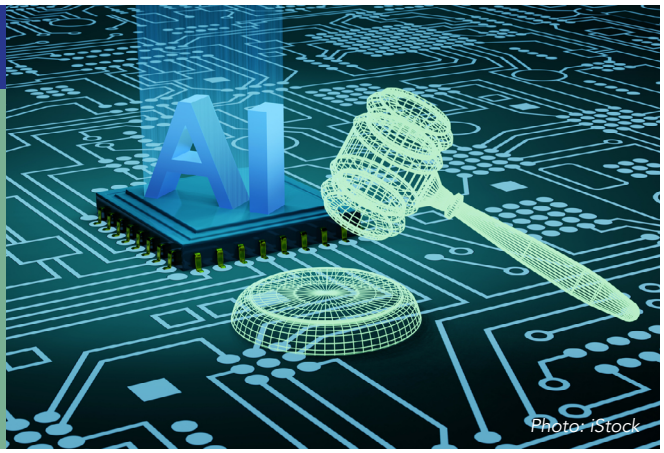

Photo: iStock

2. LATEST ENFORCEMENT ACTIONS AND FINES BY THE INFORMATION REGULATOR

Photo: iStock

The Information Regulator is increasingly willing to move from guidance and enforcement notices to infringement notices, administrative fines and court proceedings. In many cases, the biggest risk is not the original POPIA breach, but what happens after the Regulator intervenes. The fines imposed so far have generally followed failures to comply with enforcement notices.

2.1. Blouberg Local Municipality: R500 000 reduced to R250 000

In the Blouberg Local Municipality matter, personal information about a staff member was published on the municipality's website. The Regulator issued an enforcement notice and, after non-compliance, imposed a **R500 000 administrative fine**.

The Regulator then approached the Polokwane High Court to have the fine confirmed. The court reduced it to **R250 000**, noting that only one data subject was affected, the municipality had taken corrective steps, and this was its first POPIA violation.

The case shows that courts may scrutinise the proportionality of POPIA fines and reduce them where appropriate.

2.2. Department of Basic Education: R5 million fine under appeal

The Regulator issued a **R5 million fine** against the Department of Basic Education after it allegedly failed to comply with an enforcement notice relating to the publication of matric results in newspapers.

Photo: iStock

The Pretoria High Court later set aside both the enforcement notice and the infringement notice. The Regulator has applied for leave to appeal and says this suspends the court order pending the appeal.

This matter is significant because it tests the boundaries of POPIA enforcement, public interest, publication of examination results and the Regulator's powers.

2.3. Lancet Laboratories: R100 000 fine paid

Lancet Laboratories was fined **R100 000** after failing to comply with an enforcement notice relating to security compromise notifications. The Regulator found that Lancet had not notified either the Regulator or affected data subjects as required by section 22 of POPIA.

Lancet paid the fine. The case confirms that breach notification failures are not treated as technical oversights. The Regulator expects timely notification and clear evidence of compliance.

2.4. FT Rams Consulting: R100 000 fine for direct marketing

FT Rams Consulting received an enforcement notice after repeated unsolicited marketing emails were sent despite opt-out requests. The Regulator found that FT Rams had contravened section 69 of POPIA.

After FT Rams failed to comply with the enforcement notice, the Regulator issued a **R100 000** fine and later started court proceedings to recover the unpaid amount.

This matter shows that direct marketing is now a real enforcement risk. Consent, opt-outs and objection management must be properly recorded and honoured.

2.5. What we can learn from these findings

The Regulator is not yet imposing GDPR-style mega-fines, but POPIA fines are now a real risk. The penalty landscape is still developing, and several major matters remain before the courts.

The biggest risk is often not the initial POPIA breach, but the organisation's response after the Regulator intervenes. A responsible party that ignores an enforcement notice, fails to keep evidence of corrective action, or does not appeal properly is far more exposed to an infringement notice and fine.

The Regulator's message is becoming clear: **comply, prove compliance, or face escalation**.

3. EU DIGITAL OMNIBUS: CHANGES MOVE AHEAD, WHILE GDPR AMENDMENTS REMAIN UNDER DEBATE

Photo: iStock

The EU's Digital Omnibus package is part of a broader simplification agenda aimed at reducing regulatory overlap and administrative burden. But the package is moving on two different tracks, and they have not progressed at the same pace.

The first track is the **Digital Omnibus on AI**, which makes targeted changes to the EU AI Act. The second is the broader **Digital Omnibus Regulation Proposal**, which includes proposed changes to the GDPR, ePrivacy rules, the Data Act, cybersecurity incident reporting and other parts of the EU digital framework.

The AI Act track has moved ahead. On **7 May 2026**, the Council presidency and European Parliament negotiators reached a **provisional agreement** on a proposal to simplify certain AI Act rules. This is a major political step, but it is not yet final and still requires formal approval.

The broader Digital Omnibus Regulation Proposal, which includes the proposed GDPR amendments, remains further back in the process. The European Commission tabled it on **19 November 2025**, but it has not reached the same provisional agreement stage as the AI Act amendments.

3.1. What has moved on the AI Act?

The AI Act amendments are mainly about implementation, timing and simplification. The provisional agreement introduces new application dates for high-risk AI systems: **2 December 2027** for stand-alone high-risk AI systems and **2 August 2028** for high-risk AI systems embedded in products. It also postpones the deadline for member-state AI regulatory sandboxes until **2 August 2027**.

The agreement also makes a few substantive changes. It adds a new prohibition on AI practices involving the generation of non-consensual intimate content or child sexual abuse material. It also keeps the 'strict necessity' standard for processing special categories of personal data for bias detection and correction.

In short, the AI Act part of the package is no longer just an early-stage proposal. It now has political agreement between the co-legislators, although formal adoption is still required.

3.2.What about the GDPR changes?

The GDPR changes are different. They remain proposed amendments under the broader Digital Omnibus Regulation Proposal.

The proposal would amend the GDPR in several significant ways. One of the most important is a proposed clarification of personal data: pseudonymised data would not be treated as **personal data** for an entity that does not have the means to re-identify the individual. This is intended to support data sharing and AI development, but it is also one of the proposal's most controversial features.

The proposal would also clarify that organisations may, in some cases, rely on **legitimate interests** to process personal data for developing, training, deploying and operating AI systems and models. The EDPB and EDPS have questioned whether a new

GDPR provision is necessary and have recommended clearer safeguards if lawmakers proceed.

The proposal would also reshape cookie and tracking rules. It would move certain consent rules from the ePrivacy Directive into the GDPR, expand some consent exemptions, and allow users to express preferences through one-click choices or browser or system-level settings. It also proposes that, where a user refuses consent, a controller may not ask again for six months.

Other proposed changes include streamlined data breach reporting, harmonised data protection impact assessment requirements, and a single reporting point for certain cybersecurity and data incidents. The aim is to reduce fragmentation and make compliance more consistent across the EU.

3.3. What organisations should do now

For now, controllers and processors should treat the GDPR amendments as a watch item, not as current law. Existing GDPR obligations still apply.

However, organisations should use this period to prepare.

- Those developing or deploying AI systems should map where personal data is used, identify lawful bases, and document legitimate interest assessments where relevant.
- Organisations using pseudonymised datasets should assess who can re-identify individuals and under what circumstances.
- Marketing and digital teams should monitor the cookie proposals but should not dismantle current consent mechanisms yet.
- Privacy and security teams should also track the proposed changes to breach reporting and DPIA requirements.

The Digital Omnibus is best understood as a simplification package in motion. The AI Act amendments have reached provisional political agreement, while the GDPR amendments remain proposals and are still open to negotiation. For privacy teams, the task now is not to rewrite the compliance manual overnight, but to watch the process closely, understand the likely direction of travel, and be ready to adapt when the final text is adopted.

4. FURTHER READING

Photo: iStock

- Chapter 19: Enforcement of POPIA
- Information Regulator's Annual Performance Plan 2026/2027
- European Commission Digital Omnibus Regulation Proposal
- NOYB: Digital Omnibus Report V3: Analysis of Select GDPR and ePrivacy Proposals by the Commission