JUTA
POPIA PORTAL

ISSUE NO 64 • DATA PRIVACY ROUNDUP 2026 EDITION 2 • MARCH 2026

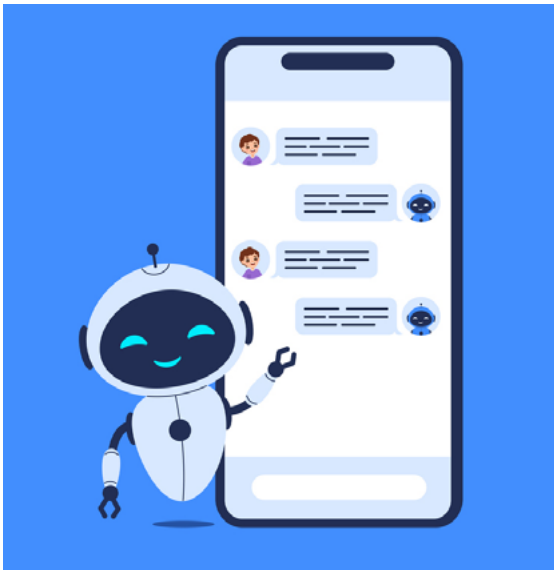
# DATA PRIVACY ROUNDUP 2026 EDITION 2

## 1. OVERVIEW

In this edition, we look at developments in South Africa and abroad that continue to influence how organisations manage personal information and risk. Recent enforcement activity, new guidance trends, and high-profile incidents highlight the need for proactive governance, transparent practices and strong vendor oversight.

Photo: iStock

# 2. WHAT HAS BEEN HAPPENING AT HOME



### 2.1. Chatbot governance takes centre stage

A recent analysis by local commentators has reignited a reminder that your chatbot is not a separate legal entity under POPIA. Any privacy breach, misleading disclosure, or unauthorised data processing carried out 'by the chatbot' is in fact carried out by the responsible party behind it.

The discussion follows increased regulatory scrutiny of AI-driven engagement tools and the risk they pose when they collect customers' personal information without proper purpose specifications, retention rules or human oversight.

Important things for organisations to remember when using chatbots include:

- ensure privacy notices cover chatbot interactions explicitly
- confirm that scripts, data logs and escalation rules minimise unnecessary collection; and
- incorporate chatbot deployments into your POPIA risk assessments and security controls.

As more organisations use AI-powered support channels, regulators are signalling that the technology does not lessen accountability, but rather heightens it.

### 2.2. Continued focus on vendor risk after recent breaches

- Following high-profile breaches such as the **Pepkor Lifestyle/Mobiz incident** previously reported, the Information Regulator continues to emphasise third-party risk management.

Themes emerging from recent engagements include:

- stronger due diligence requirements before onboarding marketing and analytics providers
- contractual controls over data-hosting arrangements and sub-processors; and
- clearer incident-reporting timelines from service providers.

# 3. WHAT HAS BEEN HAPPENING ABROAD

Photo: iStock

**3.1. Europe sees an uptick in large GDPR fines**

November 2025 was marked by several significant enforcement actions, which include the following:

- Croatia issued its **highest recorded GDPR penalty to date**, related to unlawful disclosure and inadequate organisational controls; and
- EU regulators are issuing substantial fines for failures in consent, security safeguards and DSAR response times.

Trends from these cases include:

- regulators prioritising transparency failures, especially around behavioural tracking and automated decision-making
- increased penalties for recidivism, where organisations repeat previously flagged non-compliance; and
- a growing expectation that large entities implement risk-based controls, not 'paper compliance'.

For South African businesses operating internationally, these decisions serve as a reminder that extraterritorial regulators are tightening their approach, particularly in cases involving cross-border processing.

**3.2. EU procedural reforms to speed up cross-border enforcement**

The EU's adoption of the new GDPR Procedural Regulation aims to reduce delays that have historically hampered multi-country investigations. Standard investigations should be closed within 15 months, while simplified matters are targeted for 12 months.

This means organisations can expect:

- shorter timelines from complaint to decision
- faster determinations in cases involving multiple supervisory authorities; and
- more harmonised enforcement across the EU.

**3.3. India's new privacy framework becomes fully operational**

India's Digital Personal Data Protection Act continues its phased rollout, with the 2025 DPDP Rules now in force. Highlights include:

- an 18-month compliance runway
- new duties for Significant Data Fiduciaries, including audits and DPIAs
- strict timelines for data-subject responses; and
- penalty ceilings of up to ₹250 crore for security-safeguard failures.

Multinationals processing Indian data should ensure they understand the new obligations, especially around cross-border transfers and accountability frameworks.

## 4. WANT TO READ MORE?

- **Chapter 4**: For accountability for compliance, including responsibility for chatbots, AI tools and operators.
- **Chapter 5**: For information security management, including safeguards, vendor risk and breach prevention.
- **Chapter 11**: For notification duties, privacy notices and transparency towards data subjects.
- **Chapter 19**: For enforcement, investigations and regulatory consequences of non-compliance.

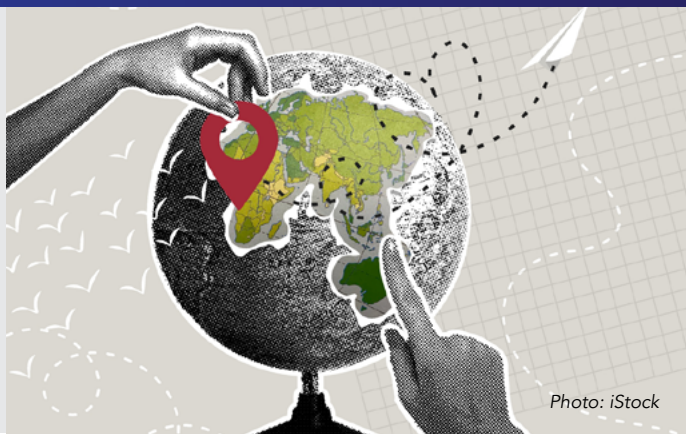


*Photo: iStock*

## 5. WHAT'S NEXT?

Data privacy enforcement is accelerating, both locally and globally, with regulators placing an increasing emphasis on transparency, vendor governance, AI-driven processing, and prompt incident reporting. Organisations should review their internal POPIA controls and align international operations with evolving compliance expectations.