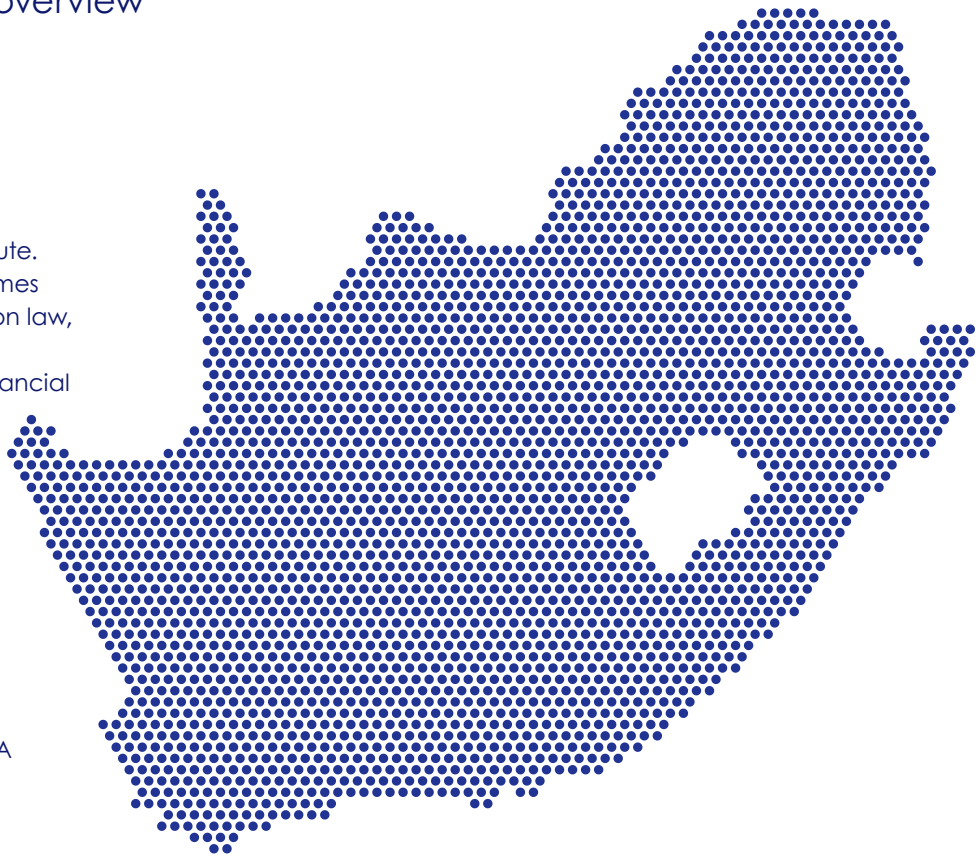


Cybersecurity regulation in South Africa

a 2026 overview



WHO IS IN SCOPE

Most organisations processing personal information. No single cybersecurity statute. The duties sit across POPIA, the Cybercrimes Act, critical infrastructure law, interception law, and electronic communications law. Designated critical infrastructure and financial services carry extra obligations.

REPORT A BREACH BY

As soon as reasonably possible.
POPIA has no fixed deadline, unlike the GDPR's 72 hours.

WHAT THEY MUST DO

Secure personal information under POPIA section 19, appoint and register an Information Officer, and ordinarily notify both the regulator and affected people when something goes wrong. Certain financial institutions also fall under Joint Standard 2, which has some DORA-style resilience features.

SUPERVISION AND PENALTIES

The Information Regulator has been increasingly active on incident response and issuing enforcement notices since 2023. Financial services are supervised separately by the conduct and prudential authorities. Fines up to R10 million, with imprisonment possible in the most serious cases.

WHAT TO WATCH NEXT

Implementation of the financial sector's new 24-hour material incident reporting process, in force since 1 September 2026. Further Information Regulator enforcement, following its R5 million fine against the Department of Justice. The Cybercrimes Act's 72-hour police reporting duty, which is not yet in force. And the National Data and Cloud Policy, which signals localisation for sensitive government data.

WHAT MAKES SOUTH AFRICA DIFFERENT

The reporting trigger is unusually broad. POPIA requires notification where there are reasonable grounds to believe personal information was accessed or acquired by an unauthorised person, with no equivalent of the GDPR's 'risk to rights and freedoms' test. A misdirected email containing personal information is ordinarily reportable if it reaches an unauthorised recipient.

FROM THE INTERVIEW

"Cybersecurity isn't just an IT department's problem. It's a board-level issue that needs to be dealt with by C-suite executives in your organisation. And that's because data has value."

"You can't decide 'this is reportable to the regulator but not to the data subject.' It's a package deal. And that's the hard pill to swallow for most organisations. They wouldn't mind telling the authorities, but they don't necessarily want to fess up to their data subjects."