Update on POPIA and the Information Regulator (South Africa)

South Africa's information regulator is getting tough on companies found to have been negligent in safeguarding the personal information of consumers, which lands in the wrong hands through data breaches.

The Information Regulator South Africa is a watchdog that monitors compliance with information protection legislation by private and public sector companies to prevent, among other incidents, data breaches.

The spate of high-profile data breaches in South Africa in recent months has jolted the regulator to launch a unit within its office — supported by forensic investigation and IT skills — that will investigate and impose sanctions against errant companies. Companies in the regulator's firing line would ordinarily have weak control systems that fail to protect sensitive information belonging to consumers or fail to even take corrective measures once there is a data breach.

The regulator was launched in 2016, but its powers were limited because the Protection of Personal Information Act (Popia) wasn't operational at the time. Popia became fully operational on 1 July 2021, on which date the 12-month grace period for company compliance ended, paving the way for the regulator to impose sanctions.

The unit that will investigate data breaches — the Security Compromise Unit — may now make findings and recommendations against companies entrusted to safeguard the personal information of consumers. The recommendations might include the regulator slapping negligent companies with sanctions including fines of up to R10-million or company directors facing imprisonment for up to 10 years.

Data breach incidents

Data breaches have worsened in recent months, with the regulator receiving more than 330 reports or complaints since July 2021 against companies. These complaints were lodged by people whose personal information had been compromised.

Companies that have reported suspected breaches in recent months include Liberty, Standard Bank, Absa, Dis-Chem, Shoprite, Experian and TransUnion (consumer credit bureaus), and others that don't usually grab headlines. In some cases, the personal information of consumers (such as their names, surnames, cellphone numbers and email addresses) was exposed.

No fines or other sanctions were imposed against companies that suffered data breaches, with the regulator saying during a press briefing on Wednesday that Popia is still new in South Africa. The information regulator's chair, Pansy Tlakula, says her office prefers to engage with errant companies and allow them to remedy a suspected data breach before imposing fines.

"But we are prepared to take the route of fines and demonstrate the regulator's bite," she says.

The regulator is still willing to show grace to companies that proactively inform it about suspected data breaches, immediately inform affected consumers (and do this publicly), and take demonstrable steps to protect sensitive information.

Protection of Personal Information Act Regulations 2018

Did you now that the POPI Regulations 2018 were gazetted last December? They add weight to the requirements of the POPI Act. In this news item we want to focus in particular on the Responsibilities of information Officers which were covered in the POPI Regulations.

Responsibilities of information Officers

The POPI Regulations 2018 include a section on the responsibilities of the Information Office role. The Regulations provide a summarised description of the role. We recommend than an Information Officer appointment letter, which includes the designation and delegation of Deputy Information Officers, is established in order to formalise these roles. Key points relating to the responsibilities of the Information Officer contained in the Regulations are:

- A compliance framework is developed, implemented, monitored and maintained
- A personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information
- A manual (a PAIA manual) is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) (aka PAIA)
- The Information Officer shall upon request by any person, provide copies of the manual to any person upon the payment of a fee to be determined by the Regulator from time to time
- Internal measures are developed together with adequate systems to process requests for information or access thereto
- Internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
- These requirements in the Regulations are intended to complement and not replace the provisions in the POPI Act concerning the Information Officer (see section 54 to 56).

Effective date

Please note that at the time of publication of the Regulations in the Government Gazette in December 2018 the effective date had not yet been announced.

For a full copy of the Government Gazette announcing these regulations and for further information please visit the Information Regulator South Africa web site at http://www.justice.gov.za/inforeg/

Correct as at February 2019

Please note this document is not legal advice but a practical interpretation to help Responsible Parties and their Information Officers and Data Subjects to make best use of the Regulations

For further information regarding this document

Please contact Dr Peter Tobin petert@iact-africa.com or John Cato johnc@iact-africa.com