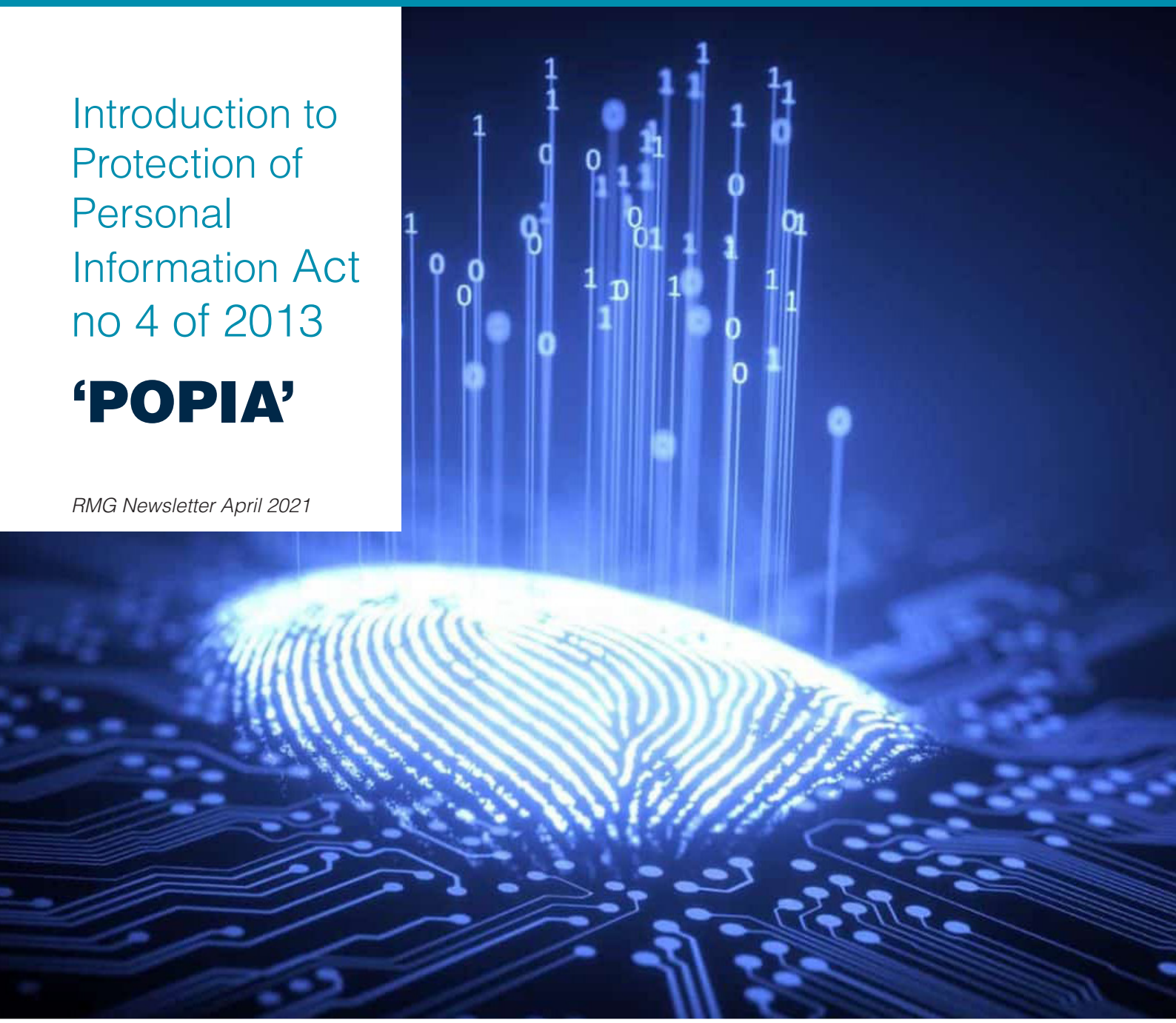
Introduction to Protection of Personal Information Act no 4 of 2013

‘POPIA’

RMG Newsletter April 2021



www.rmgforensics.com

INSTITUTE OF DIRECTORS SOUTHERN AFRICA

UNASHAMEDLYETHICAL

RMG
FORENSIC SERVICES (Pty) Ltd.

Contents

Foreword

As part of the Fraud Awareness initiative of the MRG Group to its members this monthly Fraud newsletter would assist with the most current Fraud Trends detected in the industry as well as practical advice to proactively remedy this.

In this month's fraud newsletter edition 5 / 2021 we cover the subject at hand: the protection of personal information act (POPIA) and how it will affect businesses in South Africa.

In the next edition, newsletter edition 6 / 2021 in the second quarter of the year we will define POPIA in the South Arican context.

Introduction to Protection of Personal Information Act no 4 of 2013 (*'POPIA'*)

On the morning of 22nd June 2020, the Presidency announced dates for compliance to the Protection of Personal Information Act no 4 of 2013 (POPIA). The dates are as follows:

- Sections 2 to 38; sections 55 to 109; section 111; and section 114 (1), (2) and (3) shall commence on 1 July 2020.
- Sections 110 and 114(4) shall commence on 30 June 2021.
  POPIA or POPI was promulgated on 26 November 2013. The final POPIA Regulations was published on the 14th of December 2021. POPIA is intended to promote the right to privacy in the Constitution, while at the same time protecting the flow of information and advancing the right of access to and protection of information.

  POPIA establishes the rights and duties that are designed to safeguard personal data. In terms of POPIA, the legitimate needs of organisations to collect and use personal data for business and other purposes are balanced against the right of individuals to have their right of privacy, in the form of their personal details, respected.

  POPIA applies to a particular activity, i.e. the processing of personal data, rather than a particular person or organisation. Therefore, if you process personal data then you must comply with POPIA and you must handle personal data in accordance with POPIA's data protection principles.

Therefore, if you collect or hold information about an identifiable individual or if you use, disclose, retain, or destroy that information, you are likely to be processing personal data. The scope of POPIA is very wide and it applies to almost everything you might do with an individual's personal details including details of your employees.

POPIA Framework

Essentially, POPIA:

- sets out the rules and practices which must be followed when processing information about individuals and juristic persons;
- grants rights to individuals in respect of their information;
- and creates an independent regulator to enforce these rules, rights, and practices.

It should be noted that POPIA applies to:

- information that is processed automatically;
- information recorded on paper as well as electronic;
- and health records and certain public authority records.

Section 114(1) is of particular importance as it states that all forms of processing of personal information must, within one year after the commencement of the section, be made to conform to the POPI Act.

This means that entities (both in the form of private and public bodies) will have to ensure compliance with the Act by 1 July 2021. However, it stands to reason that private and public bodies should attempt to comply with the provisions of the Act as soon as possible to give effect to the rights of individuals.

Entities which process personal information must ensure that it is done in a lawful way, the presidency said.

The POPI Act is fundamental in safeguarding persons' personal information and thus protecting them against data breaches and theft of personal information.

Pansy Tlakula, the chairperson of the Information Regulator of South Africa, says that POPIA will give serious enforcement powers to the regulator including the ability to levy fines of over R10 million and the ability to pursue criminal prosecution

She added that the POPIA will ensure that companies have adequate security measures as well as other measures when dealing with your private information. Privacy can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.

Compliance is an imperative, she stressed. "It does not in any way stifle innovation. In conclusion, I want to address those who collect our personal information. I say to them: Those who process personal information for business purposes must always remember that our personal information is our privacy. And it is a fundamental part of our human dignity. If you cannot protect our personnel information, don't collect it."

Finally, she cited the dangers of falling foul of the regulator.

"Non-compliance will damage the brand and reputation of a company through bad publicity as well as investigation by the regulator. It can lead to decline in financial wellbeing through, among other things, avoidable fines for non-compliance, which have to be explained to shareholders."

The Act makes provision for fines of up to R10 million and a jail sentence of up to 10 years, depending on the seriousness of the breach.

Whether such processing involves personal information of your employees, prospective employees, part-time workers, contractors, clients, members, consumers, customers or third-parties or anybody else whose personal information you collect, use, share, retain, store, archive, delete or destroy – you, as a processing entity, will have to ensure that you, or anybody that processes personal information on your behalf, complies with the POPI Act.

POPIA gives consumers specific rights in respect of organisations handling their personal information and it gives consumers greater control over their personal information. Consumers are informed about what personal information is collected, by who and why so that consumers can make informed decisions.

It is also important to take note of the General Data Protection Regulation (GDPR) that came into effect on the 25th of May 2018. Where your organisation deals with European Citizens information you should the regulation from the European Parliament also applies. The fines are much higher than in the case of POPIA.

Organisations should expect to see an active Information Regulator and enforcement of the provisions of the Protection of Personal Information (POPI) Act (POPIA) after 1 July 2021. This is according to Leishen Pillay, associate director within the risk advisory at Deloitte, speaking during the recent ITWeb Governance, Risk and Compliance 2021 virtual conference. Pillay, however, pointed out that whether this will result in several fines, compliance notices or otherwise come 1 July 2021, will be determined by a number of factors.

Impact on HR teams

From an employment perspective, a significant amount of personal information of a business' employees is processed by the HR function. This includes sensitive information.

Often, HR functions rely on third parties to assist them in carrying out certain HR functions. These third parties include outsourced HR payroll functions, third parties assisting with carrying out background checks, undertaking psychometric assessments, assisting with forensic investigations involving employees, assisting with the recruitment process and the like.

POPIA covers all personal and special personal information that all employers might collect, retain, or archive on previous, prospective, and current employees.

Generally, extensive special personal information (including health information, trade union membership, race, and ethnic origination information and in some cases, biometric information, and certain types of criminal information) as well as children's information, is also processed by a business in relation to its employees.

Traversing the requirements of POPIA can be challenging and it is important to note that POPIA creates various criminal offences for non- compliance and fines may be imposed of up to R10 million. Some offences also attract imprisonment.

All employers should ensure compliance having regard to the harsh penalties imposed. POPIA also places an obligation on the information officer of each business (as a responsible party under POPIA) to ensure that data processing activities are properly documented, and impact assessments and staff awareness and training are regularly undertaken.

Preparing for POPIA

In October 2020, the KnowBe4 and ITWeb online data protection survey found that when it comes to the preparedness of their organization for POPIA compliance, just under one-third (30%) indicated they were well prepared, while 39% said they were "somewhat" ready, but more work needs to be done.

Anna Collard, SVP Content Strategy and Evangelist KnowBe4 Africa shares six things that can be done to improve your POPIA readiness:

- **"Education and awareness should be a top priority for organizations** as we approach the POPIA deadline," she adds. "This is critical at every level of the business, from top management down to every person who works at the organization. Everyone has to be aware of their responsibilities with regards to handling personal information and their roles when it comes to the safeguarding of personal information." People unfortunately are also the ones who react to phishing with emotion and make mistakes that can cost the business money and reputation, and that can put critical data systems at risk. "People play a massive role in ensuring that the organization remains POPIA compliant, and the organization remains secure and safeguarded," says Collard. "They need consistent training and education so that their understanding of the threats can translate to ongoing protection of information within the organization. And to their own security hygiene practices as well."

- Secondly, organizations can really benefit from **implementing the role of a dedicated information officer** – a role that should be created specifically for the task of ensuring compliance and understanding. The duties of the information officer include, amongst others, to attend to the development and implementation of a compliance framework, ensure that internal POPIA awareness sessions are conducted, and conduct assessments to identify any risks and necessary safeguards to the personal information processed.
- Thirdly, **conduct a data mapping exercise** that identifies what type of personal information the organization collects, who this information is shared with and where it is stored. This is immensely valuable, as it not only highlights areas of vulnerability that may not have previously been identified, but it also identifies potential risks that can be alleviated prior to POPIA coming into effect. "This exercise can also be used to raise awareness and form part of an overall education drive, as it typically involves interviews with all major department heads," says Collard. "Once this is done, **it should be followed with a privacy impact assessment** (PIA), that identifies the risks and what could possibly go wrong in an environment. It is a practical step that plays a pivotal role in embedding a more robust security foundation into the organization." Part of the PIA would require a review of the security controls. This will help refine the controls that are in place and identify what has to be improved on. For organizations that do not have these skills or systems in place, they can collaborate with a third party that can help conduct these types of risk assessments and reviews.
- "Speaking of third parties, **make sure you unpack who you share the personal information with, how compliant they are and what controls they have in place**," adds Collard. "They are as much a target as the business, so if they have any vulnerabilities, they can put your organization at risk. Just make sure that the boxes are ticked with every service provider, platform and system so you are secured and compliant."
- **Consider hiring a consultant** who can go through contracts and online privacy notices, and every other space where information is collected, to ensure that the right notices have been put in place. These notices must be written in plain English and specify why the information is collected and how it is used so that consumers are informed and aware.
- "The last thing that you should consider is to **define the processes that make up your compliance programme and data breach processes**," concludes Collard. "If there is a breach, who will notify the regulator, who will notify the customers and the media and what will employees be allowed to say – these are just some of the considerations that should be unpacked in advance to ensure the organization is absolutely ready for whatever may be ahead."