Introduction to Protection of Personal Information Act no 4 of 2013

‘POPIA’

RMG Newsletter Editon
6 May 2021

www.rmgforensics.com

INSTITUTE OF DIRECTORS SOUTHERN AFRICA

UNASHAMEDLYETHICAL

ACFE SOUTH AFRICA
ACFE
Association of Certified Fraud Examiners
CORPORATE SPONSOR

RMG
FORENSIC SERVICES (Pty) Ltd.

Contents

Foreword

In this month's fraud newsletter edition 6 / 2021 we cover the subject at hand: POPIA in the South African context.

In the next edition, newsletter edition 7 / 2021 in the second quarter of the year we will define how IT must conform to POPIA.

How POPIA will assist in mitigating Fraud?

Essentially, the purpose of the Protection of Personal Information Act (POPIA) is to protect people from harm by protecting their personal information. To stop their money being stolen, to stop their identity being stolen, and generally to protect their privacy, which is a fundamental human right.

Only through diligent and ongoing effort can an organisation protect itself against significant acts of fraud. Key principles for proactively establishing an environment to effectively manage an organisation's fraud risk include:

Principle 1: As part of an organisation's governance structure, a fraud risk management program should be in place, including a written policy (or policies) to convey the expectations of the board of directors and senior management regarding managing fraud risk.

Principle 2: Fraud risk exposure should be assessed periodically by the organization to identify specific potential schemes and events that the organization needs to mitigate.

Principle 3: Prevention techniques to avoid potential key fraud risk events should be established, where feasible, to mitigate possible impacts on the organization.

Principle 4: Detection techniques should be established to uncover fraud events when preventive measures fail, or unmitigated risks are realized.

Principle 5: A reporting process should be in place to solicit input on potential fraud, and a coordinated approach to investigation and corrective action should be used to help ensure potential fraud is addressed appropriately and timely.

Protection of Personal Information Act (POPIA) Implementation is now the focus

The Protection of Personal Information Act no 4 of 2013 ('POPIA') has been with us from November 2013. The POPIA Regulations was published on the 14th of December 2018. It has been 10 years since the first POPIA bill was issued in 2009. At last there is a final date when the main provisions of POPIA will be effective.

The main provisions of POPIA commenced from 1 July 2020. This mean that organisations need to understand and implement the requirements of POPIA and the POPIA regulations. Organisations need to focus on aligning their business to comply with the POPIA requirements. This will take some time as it might involve changing business processes to comply.

Organisations should do the following as soon as possible:

Governance

- Identify and appoint Information Officers and where applicable Deputy Information Officers.

Regulator indicated that a portal will be available from May 2021 to register them.

- Ensure that Information Management is a discussion point at the Board of Directors, EXCO and MANCO.
- Draft a POPIA Compliance Policy and Framework to guide the implementation within the organisation.

People

- Do POPIA awareness training for their management and employees;

Process

- Perform a Personal Information Impact Assessment (PIIA) to understand where personal information is processed (including storage) in the organisation;
- Draft, review and update all the policies and procedures that relate to POPIA (this includes privacy and information security).

Technology

- Review Information Security as a whole and align it with POPIA requirements.

There is a grace period of 12 months from 1 July 2020 before fines can be issued by the Information Regulator. All the POPIA requirements that relate to the Protection of Personal Information will be effective from 1 July 2021. There is thus two (2) months left to be fully compliant with POPIA. The clock is ticking and organisations should not wait any longer to continue with the POPIA implementation.

South Africa: The role and responsibilities of the information officer under POPIA

Who is the information officer?

In terms of South African law, the role of the information officer stems from the Promotion of Access to Information Act No. 3 of 2000 ('PAIA') which, at its core, aims to uphold the right to access information (Section 32) as enshrined in the Constitution of the Republic of South Africa, 1996 ('the Constitution'). POPIA, on the other hand, promotes and aims to protect the right to privacy as set out in the Constitution (Section 14). Therefore, these two pieces of legislation aim to coincide and find a balance between the right of any person to have access to information (PAIA) versus the right of a person to have their own personal information and privacy protected (POPIA).

No matter the turnover, number of employees, or type of body (public or private), every organisation is required to appoint and register an information officer. Information officers are appointed automatically in terms of PAIA. What this means is that every public body (e.g. national department, provincial body, and municipality) and every private body (e.g. a company, a trust, or a close corporation) has an information officer by default and no one is exempt.

POPIA defines an information officer as follows (Section 1 of POPIA):

- in relation to a public body: an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of POPIA; or
- in relation to a private body: the head of a private body as contemplated in Section 1 of PAIA.

PAIA provides that a 'head' of a private body means:

- in the case of a natural person: that natural person or any person duly authorised by that natural person;
- in the case of a partnership: any partner of the partnership or any person duly authorised by the partnership; or
- in the case of a juristic person: the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or the person who is acting as such or any person duly authorised by such acting person.

The information officer of a public body is the head of that public body. This means that for a national or provincial government department it is the Director-General or the equivalent official of that department who is the information officer. For a municipality, the municipal manager is the information officer. In the case of any other public body, the CEO is the information officer. In the case of a private body, the information officer is by default the owner of the business. Therefore, based on the type of private body, the information officer may be the sole trader, a partner in a partnership, or the CEO (or equivalent) in a company or close corporation.

The duties and responsibilities of the information officer

In general, the role of the information officer is to ensure the responsible party's compliance with both POPIA and PAIA. Therefore, like any compliance project that may require that a leader, the information officer, in this instance, plays this leadership role and is tasked, in general, to ensure that the responsible party (i.e. the body/organisation) meets its processing compliance obligations under both POPIA and PAIA.
In terms of PAIA, an information officer of a responsible party is in essence tasked with:

- encouraging and ensuring compliance with PAIA;
- developing, updating and monitoring a PAIA manual for the body (that is if the organisation is required to have such a manual and does not fall under the current exemptions);
- assessing and providing outcomes, within the applicable time periods, to application requests which are received by the organisation, on the grounds of PAIA, to be given access to information held by the organisation.

In terms of Section 55 of POPIA, an information officer has the duty and responsibility to:

- encourage compliance by the body with the conditions for the lawful processing of personal information in terms of POPIA;
- deal with requests made to the body in terms of POPIA;
- work with the Information Regulator in relation to investigations conducted in relation to the body; and
- otherwise ensure compliance by the body with the provisions of POPIA.

Regulation 4 of the published Regulations Relating to the Protection of Personal Information (14 December 2018) ('the POPIA Regulations') further shed light on what the duties and responsibilities of an information officer are and provide that the information officer is responsible for ensuring that:

- a compliance framework is developed, implemented, monitored, and maintained by the responsible party;
- 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;
- (subject to the aforementioned exemptions) a manual is developed, monitored, maintained, and made available as prescribed in terms of POPIA and PAIA;
- internal measures are developed together with adequate systems to process requests for information or access thereto; and
- internal awareness sessions are conducted regarding the provisions of POPIA.

What are the qualifications, if any, that the information officer is required to have?

Neither POPIA nor PAIA specifically provide for the qualifications that a person should have to hold the position of information officer. However, from the afore listed duties and responsibilities it is evident that such a person is bestowed with great responsibility and duty to ensure that the body, whether private or public, fulfils its POPIA and PAIA mandate.

Must we register our information officer and with who?

An Information Officer is required to be registered with the Information Regulator, prior to the person formally commencing his or her duties in terms of POPIA (Section 55(2)). The due date to register an organisations Information Officer is the 30th of June 2021. There are two methods to register an organisations Information Officer and where applicable Deputy Information Officers. The one method is manual and the other is through an online portal. The online portal method is recommended, this should only be available in the latter part of May 2021.

As from 1 April 2021 it is possible to register on organisations Information Officer and where applicable Deputy Information Officers with the Information Regulator. The application for the manual registration of Information Officers and Deputy Information Officers can be found on the following link:
https://www.justice.gov.za/inforeg/docs/InfoRegSA-eForm-InformationOfficersRegistration-2021.pdf

After completing the application it can be send to one of the following channels:

1. **Email:** registration.ir@justice.org.za

2. **Post:** PO Box 31 533
   Braamfontein
   Johannesburg
   2017

3. **Physical Address:**
   Information Regulator
   JD House
   Braamfontein
   Johannesburg
   2001

There will however be an online portal to register an organisations Information Officer and Deputy Information Officer. This will be available during May 2021. We suggest that the online method is preferable and we expect the portal to be available from the 3rd week in May 2021.

Becoming POPIA Compliant

Even if an organisation fall victim to a data breach it is important to prove to the Information Regulator that reasonable measures have been put in place to comply with POPIA. This should go a long way to minimise the fines and penalties and also the reputational risk that exist.

Compliance means that organisations must put measures in place to comply with the conditions of lawful processing that include:

- Taking accountability for processing personal information in the organisation
- Processing personal information lawfully
- Processing personal information so that it doesn't infringe on data subject's privacy
- Processing personal information for a specific, explicitly defined and lawful purpose

- Considering the retention and restriction of records that contain personal information
- Not using personal information collected for another purpose (Further Processing)
- Ensure that personal information us complete, accurate, not misleading and updated where necessary
- Be open when collecting information directly from a data subject
- Have the generally accepted security practices and measures in place to protect personal information
- Have a system in place to provide a data subject with their personal information and get it corrected or delated where applicable.