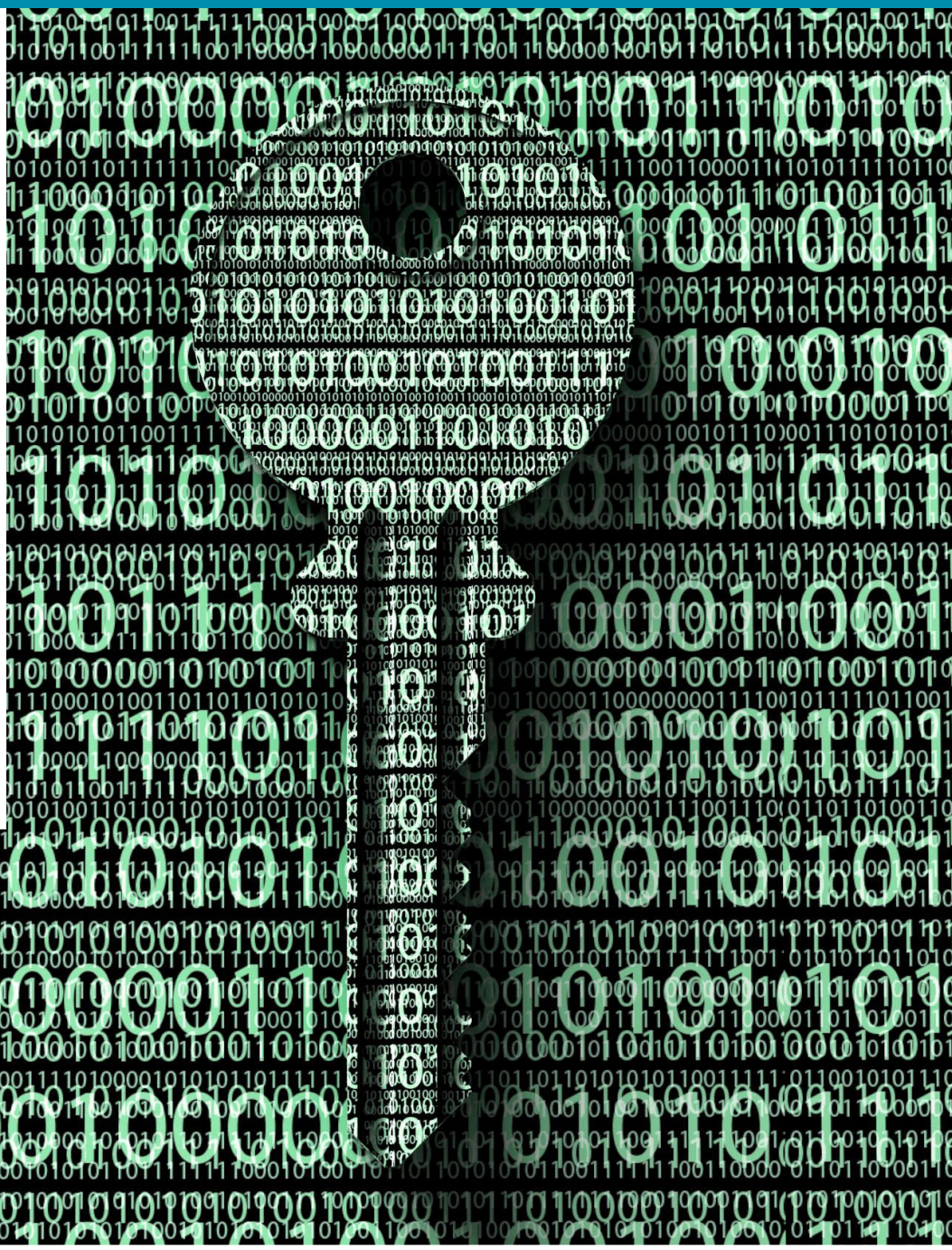
Introduction to Protection of Personal Information Act no 4 of 2013

‘POPIA’



RMG Newsletter Edition 7
June 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 7 / 2021 we cover the subject at hand: PoPIA and the impact on the IT industry.

In the next edition, newsletter edition 8 / 2021 in the third quarter of the year we will discuss internal financial control and fraud preventative measures in that sector.

PoPIA and the impact on the IT industry

On 1 July 2021 South Africa will have reached a milestone in the development of the systems in place against fraud prevention. South Africans can officially welcome the Protection of Personal Information Act (PoPIA). But the question that arises is how this new development affects the IT industry and the new responsibilities that companies and individuals will be tasked with in this trying period in human history.

The PoPIA will be much like EU's General Data Protection Regulation (GDPR) will outline the policies and procedures South African organizations need to adopt to collect, process and store personal information.

In addition to giving guidelines on the safeguarding of information, PoPIA will also outline and define the security regulations that a company must comply with in order to be able to collect and store personal information. The act requires clear, specific consent from the data subject and will also help to define the roles and responsibilities of the data subjects themselves.

The IT industry will be put at the forefront of the security for personal information.

Why was it necessary to implement the PoPIA

According to TransUnion's information, identity theft is one of the fastest growing crimes in the world. To such an extent that a someone's identity is stolen every two seconds. In addition to the financial problems that come to light once the physical crime is exposed it is particularly asinine in the regard that it is a "silent" crime. This means that identity theft can go undetected for an exceptionally long time and can have enormous debts run up in their name.

Many cases of identity theft only come to light when the victim starts receiving accounts and letters of demand which they know nothing about or when application for credit is refused because their credit record has been left in tatters by the syndicates that prey on the unwary.

Because of this evidence the South African needed to decide to protect its citizens from the forces that would gladly do them harm. The Act was signed into law on the 19th of November 2013 and on the 1st July 2020, President Ramaphosa, by way of Proclamation implemented the remaining provisions namely ss 2 to 38; ss 55 to 109; s 111; and s 114 (1), (2) and (3). Ss 110 and 114(4) shall commence on 30 June 2021. According to s 114(1) all forms of processing of personal information must, "within one year after the commencement of the section", be made to conform to the Act.

The information regulator has also made available the PoPIA Regulations that will allow some clarity and assistance for organizations to reach full compliance regarding their code of conduct which must first be submitted and approved by the information regulator. The purpose of the guidelines and checklist published by the information regulator is to outline how all the conditions for the lawful processing of personal information should be applied or complied with by the organization applying for the code, by providing the minimum criteria to develop a code (of conduct). The guidelines will contain a framework for ensuring that codes are evaluated in a standard manner to foster transparency.

This will mean that all organizations that require personal information to function will be forced to comply with PoPIA by enforcing some level of IT security and that the information to safeguard oneself in interest of the many must be made more freely available, which will put a strain on a small business in the current darkness that has enveloped the economic future.

How does PoPIA affect the business

Under PoPia an organization is required by law to appoint an information officer, this will be the individual who is responsible for ensuring that the organization will have to comply with PoPIA as well as PoPIA regulations. This is nothing new as the Promotion of Access to Information Act (PAIA) had contemplated the imposition of information officers for business in 2000.

PoPIA regulations, which will define the responsibilities of the information officer. The information officer (as well as the deputy information officer) must be registered with the information regulator before they can commence their duties as of 1 May 2021 as defined by the regulations.

In order to understand the threat of cyberattack, the information officer must have the necessary IT security restrictions in place. For the individual, these same guidelines must be followed to ensure the safety of information that is processed by an organization.

The information officer is also tasked with ensuring that only the most necessary details are given to an operator to use the data, and that the data is safely disposed of when it has served it purpose. Government has made it clear that small business will not be exempt from PoPIA and will also have to adhere to the guidelines imposed on larger corporations. There is an application system in place which will grant exemption from PoPIA but this is only after the Information Regulator is satisfied that the public interest outweighs any interference with the privacy of the data subject, or the processing involves a clear benefit to the data subject or a third party, and that benefit outweighs any interference with the privacy of the data subject.

Organizations that will not be able to comply with these security regulations defined by PoPIA will suffer terribly, as not only will the organization be charged by the Information Regulator, but they will also be exposed to the syndicated that target the weak and unprepared.

In most companies the Information Officer will be a director or owner of the organization, but the task can be delegated to other parties as well. Parties tasked with handling information within the organization will have to comply to the code of conduct that is enforced by the information officer in response to use and disposal of personal information.

Understanding the responsibilities defined by PoPIA

The data subject can be either a person or a juristic entity who is the personal information belongs too or is about. Because of these measures must be put in place in order to protect the personal information of both individuals and juristic entities. The personal information must be garnered from consenting subjects who have received clarity on what their information will be used for. We will discuss the security measures that subjects can take to protect both themselves and the legal entities they represent.

The responsible party is the person or entity that determines the purpose of and means for processing personal information garnered. In most cases this will be the person who is responsible for the implementation of security measures. It is the responsible party who bears the onus and obligation to report any security compromise or data breach to the Information Regulator and affected data subjects, the responsible party also liable to data subjects for civil claims for damages and/or to the Information Regulator for enforcement action if it fails to comply with the regulations that are set out in PoPIA Regulations.

However there seems to be some confusion when it comes to a party determining whether they identify in the Responsible Party bracket or the Operator bracket. An operator is defined in PoPIA as a person who processes personal information for a responsible party in terms of a contract or mandate without coming under the direct authority of that party. PoPIA has made accommodations for this in terms of joint responsibility, as it implies that parties can be joint responsible parties, that they will be processing personal information in conjunction with one another.

We can use the definitions used in the GDPR regulations, for a Responsible Party or Controller is a body that decides certain key areas of the processing, whereas an operator or a processor will process personal data on behalf of the responsible party.

Each of these units has a key aspect in terms of IT security and has the responsibilities to comply with PoPIA in terms of personal security and asset security with regards to personal information.

If the Responsible Party does not have the correct infrastructure in place to both store the data that is used by either internal or third-party operators, then they will be liable to losses if they are targeted by cyberattacks. Data that is no longer relevant must be disposed of properly in order to attain anonymity amongst the data subjects once the relevance of the data has expired. In the same regard it would be the responsibility of the operator to ensure that the data is used only for the prespecified manner as set out by the controller. That however is left to the operators' discretion and training to determine the efficacy of the level of security with which they would handle, process and store data about data subjects.

In terms of PoPIA, the Responsible Party must secure the integrity and confidentiality of personal information in its possession or under its control by taking the appropriate technical and organizational measures to prevent loss, damage or unauthorized access or destruction of personal information.

With regards to how the operator can be motivated to better safeguard their work environ, and to assert the most secure processing center for personal information the Responsible Party can assume joint or partial responsibility by imposing contractual agreements which would hold the operator as a responsible party in special terms as predetermined by the contract. But it remains the responsibility of the Responsible Party to both enforce and educate the operator to conform to these standards.

The Responsible Party retains the discretion to use a third party to ensure security for both itself and an internal operator. The IT security which some companies must now adopt will be unknown to the involved parties, thus the parties will be forced to outsource in order comply with the act. This will require IT companies to continuously update and regulate the interests of the client, alternatively the internal IT technicians would have to ensure that the company is aware of and updated on the latest software available to secure the companies interests.

Defining Cybercrime

→ **Financial** This form of cybercrime allows perpetrators to steal financial information to disrupt the running of a financial institution.

→ **Hacking** This consists of unauthorized access to a computer system

Cybercrime has several definitions but in South Africa the biggest cause for concern is the identity theft that is then used to generate debts in the victims' names. Institutions which have large client data bases sometimes have "data leaks" when they have been the victims of a cyberattack. A data leak at a law firm or a medical aid would have catastrophic consequences if the information from its clients or members is leaked to cyber criminals.

With the rise of machine learning and artificial intelligences that are designed to ensure cybersecurity the criminals who take part in these campaigns of cyber terror are also constantly getting smarter and more efficient. Cybercriminals can use complex systems to fool unsuspecting individuals to give over sensitive information.

It is the responsibility, within PoPIA Regulations, of the Responsible Party to determine the extent of liability to the personal information in their possession. This will also include to ensure the security of the information as it gets processed by the operator and where the information is stored.

How will a business have to conform with the eight conditions set out in PoPIA

→ **Accountability**

The Responsible Party is accountable for the personal information it processes and stays accountable for that personal information even if it is passed onto a third party. Thus, it is the responsibility of the Responsible Party to ensure that all information gathered has a "why" and "how" if the data subject wishes for clarity on what their information can be used.

Information technology is a useful function for the business to network, this allows the users to trust the integrity of the organization that they can state to users via either personalized responses or a multimedia interface to relay the information to the data subject as to what the personal information gathered will be used for.

→ **Process Limitation**

Personal information must be processed lawfully and in a manner that does not infringe upon the data subject's privacy in any way. This requires that the Responsible party must ensure that the information is processed safely and conveyed between responsible parties without threat of a data breach. Organizations should not collect or process more information than it needs to achieve the purpose that it is being collected for. The responsible party can set about limitations to the information by applying security applications on the devices used within the organization framework to discourage any behavior that could negatively implicate the subject's personal information.

→ **Purpose Specification**

Personal information must be collected for a specific, explicitly defined and lawful purpose. This ties in with being accountable for the information collected. Organizations will be forced to utilize the ITC sector to accurately convey the purpose of the collection of personal data to the subject. The subject also has the freedom to question any data collected as the data subject must understand the conditions on which the personal information is collected.

→ **Further Processing Limitation**

PoPIA states that information can only be processed for the purpose that it was collected for and no other purpose. If an organization wishes to repurpose that information for another process it would have to generate a new consent form from the data subject for the additional or new processing activity. The Responsible Party would have to put in place infrastructures to ensure that the data subjects are aware that the personal information that they had submitted would be repurposed to ensure compliance with PoPIA.

→ **Information Quality**
In order to comply with this condition, the organization must take practicable steps to ensure that personal information is complete, accurate, not misleading of purpose and updated where necessary. This will mean that the systems in place for the processing and storage of personal information within an organization will have to be updated to the best of the organizations abilities to comply with PoPIA. In order to give feedback on data that is lawfully collected the collection process must be made as simplistic as practical for the organization.

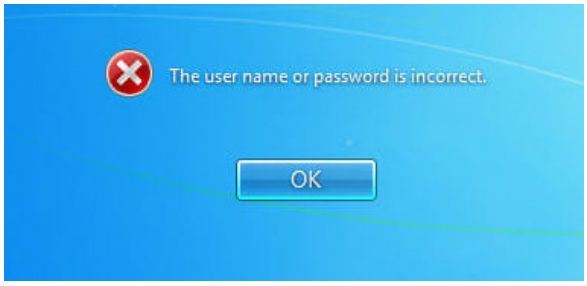
→ **Openness**
This condition requires business to be open about why they need the personal information from the data subject. When data is being collected the subject must be aware which information is mandatory or voluntary as well as any implications that the data would be used for in either storage or processing. Businesses can simplify this function by detailing these conditions in their privacy policy which will then in turn be available to the data subject at any time, or these conditions would be detailed in PoPIA consent form.

→ **Security Safeguards**
Organizations must take appropriate, reasonable, technical, and organizational measures to secure the integrity and confidentiality of the personal information it processes and to prevent the loss, damage, unauthorized access or unauthorized destruction to personal information. This is not limited to IT as organizations would have to implement the safeguard and security of both electronic and hard copy records of personal information. The Responsible Party must ensure that generally accepted information security practices and procedures apply to the organization across all fields of its industry.

→ **Data Subject Participation**
Under PoPIA, a data subject has the right to ask whether the Responsible party holds any personal information about the data subject, and to request the details of what personal information is being held, a copy of their personal information record and details of all third parties who have access to this information. In this regard the systems and processes that house that information should be simplified for the organization in order to convey the personal information that it holds to the correct data subject. Having proper administrative and information technology systems in place would be seen as a condition for PoPIA as the data subject should have the freedom to ask for this information at any time.

How can the common worker protect themselves?

The Responsible Party will be tasked with assigning sober practices in terms of securing the personal information of data subjects under PoPIA. Organizations are sometimes very lax in their cyber security and that is why it is such a big risk. But building from the foundational level with these simple steps the organization will be able to improve its IT security by teaching the following practices as prescribed by TransUnion:



→ do not use obvious passwords, criminals will try admin1 or 123456 the first chance they can get the personal information of a data subject. Or when they would try to bypass a laptop or phone that has company details on the internal cache.
→ be random with spelling, do not use just words and numbers. Most passwords support characters that allow an additional level of security. For example, rather replace Adele1944 with @dele1944 in order to secure the information that is being protected by that password
→ when devices are not in use to take them “offline” as to discourage any cyber-attacks.
→ That operators who use emails can identify and discard “spam” or phishing mails that would be a risk once the attachment is opened.

Operators are just as at risk as the Responsible Party; thus, the operator must be made aware of how to verify if they have been hacked or if they had been subject to a data breach. There must also be a framework and policies in place in order to make provisions for such a scenario

An organization is only as strong as its weakest member, if that member does not receive proper training or is compromising to the organizations processing or personal information then steps must be taken to either ensure that training is provided to safeguard against threats or to ensure that persons who would be a threat are eliminated early on before a larger problem can occur.

THE SILVER LINING: CONCLUSION

PoPIA will bring about a new era of data security and processing as South Africa leans more towards taking part in the global community. This new dawn will allow many skilled South Africans to assist with the networks and infrastructure that will be in place for future generations. With the assistance of government, the IT industry will be benefitted by PoPIA, it will not be without sacrifice as there are still many grey areas that will need to be defined within PoPIA but for the security of all South Africans it will be a necessary task.