POPI: Understanding Protection of Personal Information Act

By Lindsay Smith

RED EDGE Solutions

Foreword: this e-book was written on the premise that the new POPI (protection of personal information) act is a lot to digest for most organisations. That said, this book will assist in simplifying the understanding of POPI and how it will ultimately affect organisations.

Contents:

Edited by:

Etienne Herbst: Managing Director of Red Edge Solutions

Kayla Wilson: Senior Compliance Specialist at Red Edge Solutions

Chapter 1: What is the Protection of Personal Information Act (POPI)?

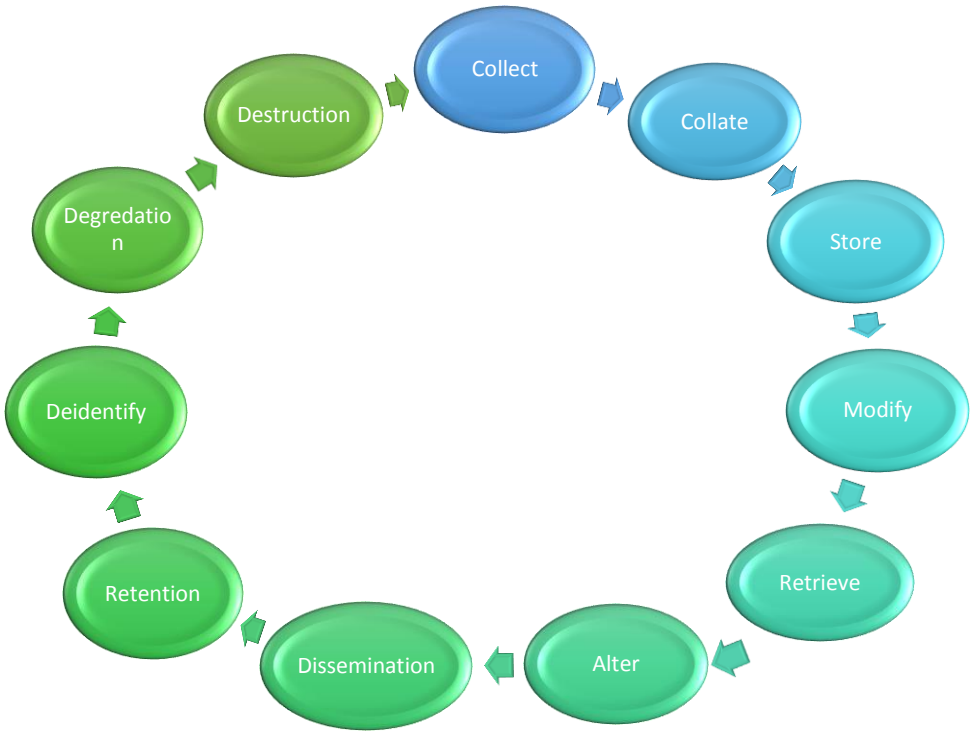
The POPI Act is in recognition and enforcement of the South African Constitution in Section 14; that subscribes to everyone's right to privacy, and the State that must respect, protect, promote and fulfil this right. The act draws from established privacy legislations such as the GDPR in the European Union as well as other international best practices that subscribes to certain principles on how one can process information.

POPI applies to all individuals and juristic persons and therefore requires an organisation to protect information of both entities. Drafted within the act are conditions that establish minimum requirements for the processing of personal information and ensure that it is enforceable by appointing a Regulator.

Though much can be said about protecting personal information and how one processes it, we need to understand what it means to "process" information first. This is critical to understanding how POPI ultimately affects every area of an organisation.

Information that is acquired, used, manipulated to the point of destruction (as indicated below in fig1) must be processed in a manner that is fair, responsible, and secured always. Processing of information can be conducted manually or automated and strict measures should be applied to ensure that no matter the structure of the information, it is kept secured.

Fig1: Information Processing Lifecycle



It is important to be aware that at every stage of processing information, organisations are expected to protect that information in any form that it is processed in.

So, what is personal information?

Personal identifiable information (PII), or Special Persons Information (SPI) as used in information security and privacy laws, is information that can be used on its own or along with other information to identify, contact,

or locate a single person, or to identify an individual in context. This includes, but is not limited to account numbers, biometric information of an individual and personal opinions and views of an individual.

The Act prescribes that we are to process information lawfully and gives rights to the data subject (an individual or juristic person) with certain exclusions.

By gaining understanding of these two concepts and how it is defined by law, we can now begin to unpack what the conditions of the law requires from an organisation in terms of protecting the information.

"Information is a significant component of most organizations' competitive strategy either by the direct collection, management, and interpretation of business information or the retention of information for day-to-day business processing. Some of the more obvious results of IS failures include reputational damage, placing the organization at a competitive disadvantage, and contractual noncompliance. These impacts should not be underestimated."

— Institute of Internal Auditors

Chapter 2: The 8 Conditions

The act provides eight conditions that guides the way in which information is processed. These conditions are:

- Accountability
- Processing limitations
- Purpose specification
- Further Processing limitation
- Information quality
- Openness
- Security safeguards
- Data subject participation

1 Accountability

Although this condition merely states that the responsible party (any organisation processing information) should ensure that they lawfully process information, it is important to note that one cannot look at accountability as a separate entity but in conjunction with Processing limitations, Information Quality, Openness, and Data subject participation. ***One can in fact not look at any of the conditions in isolation but rather approach personal information and processing along with the eight conditions as a collective.***

This section is usually managed by appointing an Information Officer who will ultimately be responsible for the compliance efforts within the company as well as the organisations representative and contact point for both the information regulator and data subjects.

2 Processing Limitations

This condition also ascribes to lawful processing within a reasonable manner that does not infringe on the ultimate privacy of the data subject. It indicates the necessity of minimality – not having more information than is necessary and requires ***consent from a data subject***. Any data subject can also object to the processing of information thus the responsible party will no longer be allowed to process their information.

3 Purpose Specification

Collection of personal information should be specified, explicitly defined and steps should be determined to ensure that the data subject is aware of the purpose of the collection of information. It requires clearly defined ***restriction and retention of records*** and how to go about dealing with the information until the information processing lifecycle is completed. This can be managed through access controls and restrictions accesses to information within an organisation.

4 Further processing limitations

Further processing of information must be in accordance or compatible with the original purpose for which it was collected. Therefore, one cannot use the information without the consent of the data subject to process information beyond what it was originally obtained for.

It accounts for the limitation to the way the information was collected, the consequences of further processing of information as well as the contractual rights agreed upon by both parties and the obligations within it.

5 Information Quality

Responsible parties need to put into place the reasonable practices where all personal information is complete, accurate, not misleading and updated where necessary. This practice should be considered throughout the data management process of an organisation, the information management requirements within and organisation as well as the other conditions within the act. It's important to reiterate that POPI compliance cannot be attempted in isolation but creates a paradigm shift within an organisation that includes a holistic view to business and its operational standards alongside other legislation such as the **Cybercrimes and Cyber Security Bill.**

6 Openness

The act prescribes that all relevant documentation be kept and maintained of all processing operations under its responsibility. This includes all organisational processes, SOP's (standard operating procedures), contracts, information flows within the organisation and understanding of your repositories for all information stored both manually and automatically.

The act requires that responsible party must take reasonable steps to ensure the data subject is aware of the collection of information that is not directly from them, the purpose of the information, the type of information collected and whether the information may be transferred. It is critical to mention that during the acquisition of the information and desire to process the information, a data subject may be allowed to exercise their rights, this determination will be discussed later.

Furthermore, for data subjects to request access to their information for amendments, the process should be made public in a ***PAIA Manual*** in accordance with the PAIA (Promotion of Access to Information Act) Section 14 for public bodies and section 51 for private bodies. Irrespective of the type of body, these manuals are expected to be updated at a ***minimum*** once a year.

7 Security Safeguards

Under this condition, the expectation is that the responsible party must secure the information in its possession through applying security safeguards, technical measures and ensuring that a risk management response is put in place. It requires that an organisation identifies internal and external risks, puts measures in place to mitigate these risks and ensure that this is constantly monitored and controlled through any risk response strategy.

It also requires that information processed by an operator (someone/company processing information on behalf of the responsible party) must be done so with the knowledge of the responsible party, meaning that the intention for them to process the information cannot be completed beyond the purpose for which they are processing the information. They are also required to treat the information confidentially and therefore cannot share the information further. Measures should be put in place to enforce this through written contracts, SLA's (service level agreements) and audits of such activities.

Under this condition, a process is required to ensure that should a breach occur, the regulator be notified of the breach. This process should be defined internally by the information officer in conjunction with the information regulator. What is critical in this instance, is that the act requires an organisation to determine through impact assessments, what the overall effect of this breach may be on the data lost, data subjects affected and identification of the root cause of the breach. These steps need to include the notification of a breach to the data subject with sufficient information regarding the breach and the measures in place to mitigate the effects of the breach on the data subject.

"Privacy as a fundamental right allows a person to prohibit, regulate, and take other actions against any actual and/or foreseeable intrusions into his privacy, and this fundamental, constitutional right will trump any statutory right or limitation unless he high standards for making exceptions are met."

— Kalyan C. Kankanala, Fun IP, Fundamentals of Intellectual Property

8 Data subject Participation

A data subject has been given rights. These rights allow them to manage and control their own personal information but also requires that an organisation be accountable to them in many ways. These include the right to confirm whether an organisation holds any information about them, including any operators and third parties associated with the organisation (this would require a process within the organisation to verify such).

A data subject may be allowed to request the correction of their information, the deletion (within legislative limitations) of data, and provide credible evidence of this process.

It is worth noting that POPI is not prescriptive but rather principle based, therefore it provides the Information Regulator with a unique view in dealing with contraventions and negotiated settlements. This is both a benefit and a risk should the regulator approach an organisation with an independent veritable outlook. Endeavouring to becoming POPI compliant, one mustn't put more emphasis on one condition than the other but rather approach it holistically including all conditions but not excluding other regulatory requirements.

Chapter 3: Direct Marketing Practices

An organisation may not process personal information from a data subject for the purposes of direct marketing by means of electronic communications (indirect marketing practices are covered in other legislation). This includes and is not limited to automatic calling machines, facsimile machines, SMS's or email without explicit consent from the data subject. The responsible party may only approach the data subject once to obtain consent who has not previously withheld consent. This would in any event require proof of the consent with the option to opt-out.

Direct marketing practices by electronic means is not only enforceable through the POPI act but has inclusions in both the Electronic Communication and Transactions Act, 2002 as wells as in the Cyber Crimes and Cybersecurity Bill. It is safe to say that Direct Marketing practices are becoming highly regulated and marketing companies and these practices are required to change tactic. It would come as a welcomed relief to consumers any way as many of these unsolicited practices are cause for much frustration and until recently with no recourse.

Chapter 4: Transborder Information Flows

This section affects organisations that has business operations beyond the borders of South Africa. The act is clear on personal information that flows outside of South African borders requires measures be put in place to ensure that the information that leaves the country is still protected. This is governed in the following manner

1. Similar laws exist and enforces that Transborder flows are limited and protected
2. It upholds principles for reasonable processing
3. Corporate binding rules with adequate protection policies exist
4. Binding Agreements exists – contractual agreements that upholds the principles of protecting the personal information during the processing of information

Further to that, a data subject must provide consent, however may be permissible should the transfer be necessary to complete contractual obligations, and the transfer is in the benefit of the data subject as stipulated within a contract or alternatively explicit consent is given.

Organisations should take precaution to note the other privacy laws beyond South African borders and how this may affect the secure flow of information between countries. Some countries laws are quite extensive (such as the GDPR) and requires effort to understand how it is applicable to your organisational operations and what the overall impact is.

Chapter 5: How does it affect my business?

Well, the short answer to this question is, completely. All businesses process information. Much of that information contains personal information. This in turn requires that no matter where in your organisation any personal information is processed, manually or automated; evidential, auditable, quantifiable measures must be put in place to ensure the protection of the personal information processed.

Policies and processes will need to be identified, updated, altered or established as guidelines for compliance, training and awareness is critical to the overall uptake and success of the impact within the business. It does not end there, it requires constant evaluation of the organisations efforts, constant interaction with the regulator should amendments to the law be enacted.

Contractual agreements would need to be amended to include the requirements of protection of personal information and how this would be measured and conformed to. Further to that, assurance would need to be provided to any organisation yours would be interacting with and this too would need to be measurable.

The assumptions exist that information systems are the only areas that needs to be protect, and yes , it most certainly does require effort to protect, but consideration for protecting accesses to manual filing systems and manual processes are generally one of the largest risks.

During the assessment stages of an organisations POPI readiness, it is significant to look at all risks in all processes that contains personal information, identify the impact of total loss of data, the impact it has on the data subject and ultimately the impact it would have on the organisation itself.

In terms of the implication of compromised data, the regulator may enforce penalties of 10 million rand per infringement, up to 10 years of imprisonment and provide for civil remedies. This does not account for the reputational damage an organisation will inevitably face which is by all accounts the biggest implication. With a reputation damaged, any organisation would suffer customer forfeiture and ultimately revenue loss. The resonating effect of this would ultimately lead to job loss, and should an organisation be strong enough to survive, it could take years of earning the trust of consumers and customers back.

It is however not all doom and gloom. The upside to tackling this compliance effort is that you address cross functional legislative requirements from other laws as well as apply principles of internationally recognised best practices.

During your assessment processes, one can use the opportunity to apply business process improvement strategies, revisit the organisations road map and remove redundancies that does benefit the organisation. It is close to impossible in this day and age separate data from any task within and organisation and thus makes managing the flow and integrity difficult but imperative.

What's important to consider when undertaking POPI compliance is the value of the data an organisation carries. Some data may be benign but some may in fact be crucial to an organisations existence. Information such as patents, new product releases etc. Therefore, it becomes imperative for an organisation to classify the types of information that circulates within it, the value that is placed on the type of information and what the impact would be should this information be compromised. This is validated through a policy such as an "Information Classification Policy" as well as an "Information Risk Policy". These policies should clearly define

Privacy by design has been advocated since the 1990's, and is an effective way to ensure privacy issues are addressed within the organisation from inception.

1. ***Proactive*** not Reactive
2. Privacy as the ***Default Setting***
3. Privacy ***Embedded*** into Design
4. Full Functionality — ***Positive-Sum***, not Zero-Sum
5. End-to-End Security — ***Full Lifecycle Protection***
6. ***Visibility*** and ***Transparency —*** Keep it ***Open***
7. ***Respect*** for User Privacy — Keep it ***User-Centric***

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

the criteria as well as the restrictions to the information, the impact assessment results and clearly outline the impact and recourse for these compromises.

Chapter 6: Training

"The great end of learning is not knowledge but action"

PETER HONEY

Training, awareness and change management is critical to the success of compliance. Our people are our greatest risk and therefore more emphasis should be placed on behavioural changes and attitudes towards protecting information whilst processing information.

Training requires that all staff understand what POPI is, what the organisations is doing with regards to compliance, what these measures do to affect change and how these changes will affect their day to day operations. Training around all policy and process changes needs to be conducted and finally the consequences of both the organisation as well as the individual as prescribed within these policies.

Chapter 7: The right to remain anonymous

In recent years, international privacy laws especially the GDPR has afforded its citizens the right to remain anonymous. What this means is that an individual has the right to request that all data relating to them be deleted which is not required to be kept under other legislations. The GDPR also affords its citizens the same rights and expectations from any other company globally dealing with their data to provide them with the same security and anonymity.

In recent years a Cambrian explosion has taken place in technology where information technology can exist on its own, but business cannot function without the convergence of information technology.

Undoubtedly, the risk of cyber threats that have taken the world by storm, and South African legislation would have to allow its citizens the same right in due time. Globally the threat on individual safety has shifted from not only physical but also to cyber threats and legislation internationally will have to evolve to maintain and keep up with the changes that will ultimately ensure adequate protection of its citizens.

What this would mean for South African organisations is that more measures would be required to protect information, and the technologies within organisations would have to evolve to ensure that maintaining security is impenetrable. Data subjects may require from an organisation to remain anonymous and therefore removal of all data pertaining to them needs to be actioned. Both internal and external customers are to be assured of efforts and the importance of maintaining protection of personal information exists within an organisation.

Finally, no organisation can go without complying to this law, nor can one ignore the resounding way the future in technology and data risk is headed. That means all organisations need to be able to keep up, maintain and compete in an ever expanding and changing world. POPI is but one of the steps that can assists in putting the right measures in place to protect individuals and provide surety that organisations behave ethically and are ultimately accountable to the way in which information is managed.

Should you require more information on POPI compliance, any compliance efforts within your organisation, or have implementation needs and training please contact Red Edge Solutions on info@popi360solutions.co.za or contact Lindsay Smith via email: Lindsay.smith@rededge.co.za. Visit our website: www.rededgesolutions.co.za

About Red Edge Solutions (Pty) Ltd

Red Edge Solutions is an ICT service provider that developed the POPI 360 Solution to address POPI compliance needs. Red Edge Solutions has a team of specialists with over 5 years of assessments and implementation experience and has been instrumental in many POPI assessments and implementations for companies both small and large. Their experience has made them acutely aware of the challenges businesses face with compliance and assist not only in POPI implementation but other compliance initiatives as well.

Written by Lindsay Smith

Profile: Head of IT Governance and Compliance at Red Edge Solutions

Lindsay specialises in IT Governance and Compliance projects and provides training and thought leadership as a subject matter expert in POPI compliance and has more than 3 years of experience in implementation of POPI in various organisations and sectors

For more information visit her linkedin page https://www.linkedin.com/in/lindsay-smith-80165486/

The book was written upon request from our partner Veld Cooper and Associates and distributed alongside both company's digital distribution platforms

Visit their website: www.veldcooper.com