PoPI

Most people have heard of the Protection of Personal Information Act (PoPI), which was signed in to South African law in late 2013.

The focus, for many, has been the security implications of ensuring that personal data is not accessed without authorisation. PoPI, however, goes much further than simply defining how personal data may be captured and used. *The Act governs the end to end life cycle of personal data within any company, irrespective of the size*.

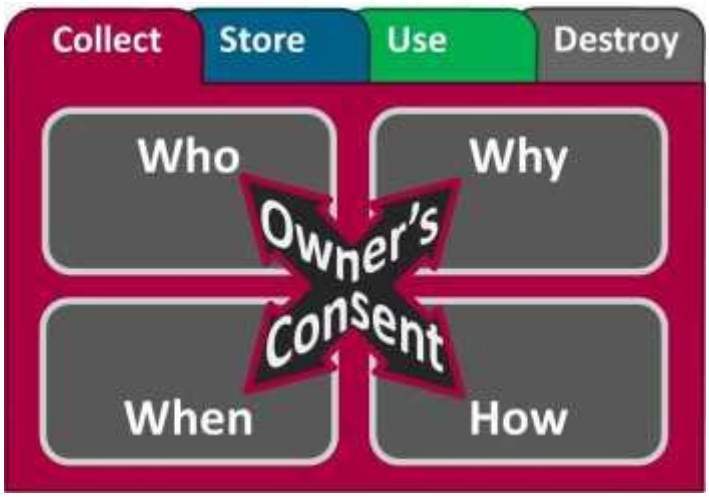
The Act provides for fines of up to R10 million, or jail terms of up to ten years, for non-compliance.

What is Personal Information?

PoPI defines personal information as any data that may identify a natural, legal or juristic person, or distinguish that person from another. This includes aspects as diverse as religion, medical history, bio-metrics, online screen names, or even opinions of, or about, a third party.

PoPI applies to the data of any legal entity – from a natural person, to a company, trust or non-profit institution. As such PoPI extends beyond customer data, and governs the use of other party's data, such as data related to customers, employees, suppliers and partners.

Data management principles are woven directly into the Act.



What does PoPI require?

Broadly speaking, PoPI controls how personal information is used within an organisation, from data capture to destruction.

Some of the requirements for PoPI include:

- Only collecting and keeping information you need for a specific purpose
- Limiting access to personal data
- Ensuring the quality of personal information
- Allowing the subject of the data to see it upon request

Non-compliance… why take the risk?

30 May 2019Myra Knoesen

The Information Regulator in SA published the final Protection of Personal Information (POPI) regulations on 14 December 2018.

Although a commencement date for the POPI Act has not yet been announced, many organisations are operating as if it is already in force.

FAnews spoke to Nadia Verappen, Compliance Officer at Compli-Serve SA, about how POPI will affect businesses and the best principles and practices to adopt.

The right thing to do

"The POPI Act sets out the rules regarding the way businesses will manage, handle and use information. It compels businesses to recognise the importance of data privacy, as well as to establish the delicate balance between safeguarding personal information, and at the same time allowing for the free flow of information as required in business processes," said Verappen.

"By recognising the importance of data privacy, not only is South Africa positioned in line with global standards, but also remains lucrative for foreign investment. This in turn provides an opportunity for businesses to exhibit good governance and grow market share by demonstrating commitment to data privacy. Trying to become POPI compliant seems like a daunting task at this time but businesses should bear in mind that not only is data protection the right thing to do for clients in terms of good governance, but it will also result in efficiencies and strengthen client and stakeholder relationships," continued Verappen.

Punitive measures of non-compliance

"Some of the possible punitive measures for non-compliance will include a fine or imprisonment – either charging between R1 million and R10 million, or one to ten years in jail. The Information Regulator may order financial compensation to data subjects for any damages they may suffer as a result of a breach. Businesses may also suffer reputational damage for breaches or non-compliance, the cost of which cannot be precisely measured, and the effects thereafter may linger long into the future," said Verappen.

“However, all attempts are not futile as the Act focuses largely on the concept of reasonability and practicality. That means that while it will be impossible to keep all information secure all of the time, one is required to take all reasonable measures to ensure that data is protected and handled in accordance with legislative requirements,” emphasised Verappen.

Governance into the pillars of POPI

“POPI should be viewed as an opportunity to drive behavioural change within your business. The success of that change relies not only on the risk and compliance teams, but also on synergy between senior management, IT, HR and the operational teams,” stated Verappen.

“It should be viewed not so much as; ‘how do I tie this into my governance policy?’ but rather, ‘how do I incorporate protection of personal information into our culture?’ As a collective, businesses need to evaluate what the business goals are and how the processing of personal information ties into it,” continued Verappen.

“A thorough review of the personal information life cycle is required. Some points for consideration are; how is personal information handled within the business, and what processes and policies can be implemented to ensure that due care is exercised when collecting, storing, sharing as well as destroying it. There must be a dissection of the data to assess its quality, as well as its purpose and safeguards. Furthermore, to satisfy the principle of data subject participation, if clients query the use of information, how quickly and efficiently are they able to receive it?” added Verappen.

“In brief, is the data accurate, safe-guarded and how is it discarded when no longer required? There should also be an enhanced focus on legacy data, which will prove to be the most problematic and time consuming. Lastly, an important and often overlooked aspect is the socialisation of POPI within a business. **In all likelihood, a breach will occur as the result of human error, due to negligence or a general lack of understanding. To mitigate this, management and training needs to take place, and then be repeated. Correct data, stored in the correct place, for the correct reasons, accessible by the correct people, is a mantra to follow when dealing with personal information,” continued Verappen.**

A POPI implementation roadmap

“Accountability is imperative. There must be ownership for data governance and a driving force for adherence from the leadership within the organisation. This should include the Information Officer who will be responsible for ensuring compliance and liaising with the Information Regulator when required. Ultimately, it is everyone’s responsibility,” said Verappen.

According to Verappen the best principles and practices to adopt are:

1. Implementation of policies and processes: Important policies like your Privacy Notice, Cookie Policy and Data Protection Policies should be in place to protect personal information and ensure accordance with regulations. Bearing in mind the intertwining relationship with other data privacy legislation like PAIA and GDPR.
2. Data Quality Standards and Transparency: Data needs to be of a high quality and a high standard of reliability. The way personal information is used and by whom should be clear to any stakeholders, customers and auditors. This will offer a business protection in the event of a breach.
3. Training: There needs to be structured training in place that clearly lets employees know who is responsible, how to handle data and what to do in the event of a breach.

“The rapidly changing landscape of regulation and information technology has resulted in a complicated relationship with data, and it requires a robust and fluid compliance programme. By knowing your legal responsibilities and what the practical implications are on your business, you will be well equipped to mitigate the risks thereof,” concluded Verappen.

Where do we start?

“The first step to POPI compliance is understanding what personal information your organisation has” says Crawford. “Remember that personal information doesn’t only apply to your individual customers or employees. Personal information is BREAK any information relating to an identifiable individual, or an identifiable juristic person such as a company. Every organisation handles personal information of various parties on a daily basis, including suppliers, corporate customers, shareholders and group companies.”

“You need to identify and document the life-cycle of personal information through your organisation - where you collect it from, why you have it, what you use it for, how you store it, who you share it with and when you get rid of it” continues Crawford. Only once this is done will you be able to conduct a gap analysis of your organisation’s personal information handling practices. Crawford says some things to consider are:

- Do we have personal information that we don’t need, or are not lawfully allowed to keep?
- Do the people whose personal information we have know that we have it and what we do with it?
- How do we secure personal information?
- When and how do we get rid of personal information?
- What policies and procedures are in place regarding personal information? Do we monitor compliance with these?
- Are our employees trained in how to handle personal information?”

“Proper awareness and training is one of the most critical components of data protection compliance” notes Crawford. “Comprehensive policies and watertight security protocols are useless if they are not followed.”