South Africa POPI Act as at 03 February 2020

Robert Bateman, Legal writer.
https://www.termsfeed.com/blog/south-african-popi-act/

South Africa's **Protection of Personal Information (POPI) Act** sets new standards for data protection and privacy in South Africa. South African businesses have been waiting a long time for the Act to come into full force. When it does, probably at some point in 2019, those who are already compliant could have a **significant competitive advantage**.

The POPI Act represents a comprehensive and progressive data protection framework that is likely to bring significant changes to the state of consumer privacy in South Africa. Some parts of the Act are reminiscent of laws that have passed in the EU and California in recent years.

Contents

Let's take a look at what the POPI Act requires, and **how your business can prepare** for the day when the law finally comes into force.

What is the POPI Act?

The POPI Act is a comprehensive data protection law that regulates the processing of personal information in South Africa. It's designed to **protect people from data breaches** and cybercrime, and to **prevent intrusive marketing** practices.

The right to privacy has long been recognized under Article 14 of the South African Constitution. The POPI Act will put some meat on the bones of this fundamental principle by providing **clear rules** and a **means of enforcement**.

The POPI Act became law on November 19, 2013 but hasn't yet come fully into force.

What's the Hold-Up?

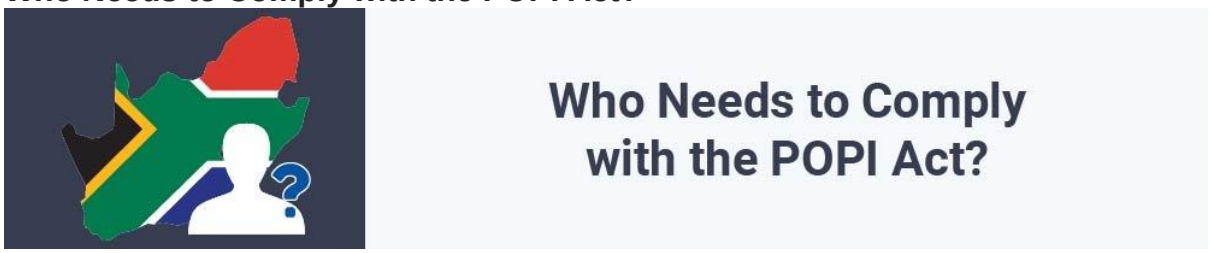
Despite having passed into law over half a decade ago, it's still unclear when the POPI Act will take full effect.

One of the few parts of the Act that has come into force is Section 39, which establishes the Information Regulator. The Information Regulator is an independent body charged with the monitoring and enforcement of data protection throughout South Africa. It can be compared with a Data Protection Authority in the EU.

Conflicts with government departments and apparent contradictions between the POPI Act and other national laws have apparently prevented the Regulator from properly establishing the scope of its work. Once this is all resolved, the President will finally announce the date on which the Act finally becomes fully effective.

While this uncertainty might be frustrating, it's also a great opportunity to familiarize yourself with the Act and **start preparing** for its enforcement.

Who Needs to Comply with the POPI Act?



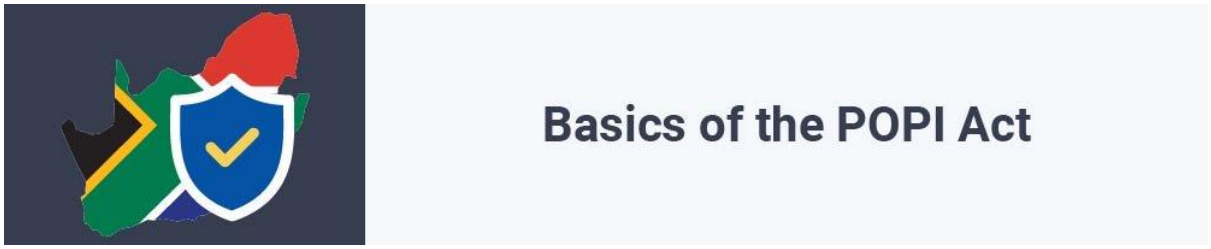
The POPI Act is **very broad** in scope and applies to just about every business and public body operating in South Africa. And to be clear, **this includes foreign companies** that are not based in the country.
According to Section 3.1, the POPI Act applies to any "responsible party" that is

- Based in South Africa, **or**
- Based outside of South Africa, so long as it **processes personal information inside South Africa** (unless it is merely "*forwarding personal information through South Africa*")

This means that **non-South African companies** will need to comply with the POPI Act if they have customers (or prospective customers) in South Africa.

POPI Act vs GDPR
The POPI Act is a fairly comprehensive law and is often compared to the **EU General Data Protection Regulation** (GDPR).
Like many modern data protection laws, the POPI Act shares certain terminology and concepts with EU laws.
You'll be at an advantage if you're already familiar or compliant with the GDPR or its predecessor, the **Data Protection Directive**.

Basics of the POPI Act



Before we get into the **practical steps** you can take to comply with the POPI Act, you'll need a basic understanding of that Act's **purpose** and **terminology**.
Objectives of the POPI Act
The POPI Act lists several objectives, including:

- **Promoting** the **protection** of **personal information**
- **Establishing standards** for data protection
- **Bringing about new personal rights** around direct marketing and automated decision-making

Personal Information
The POPI Act defines **personal information** by providing a non-exhaustive list of examples, including:

- Information about a person's **identity or beliefs** (e.g. age, race, religion, disability)
- Information about a person's **educational, medical, financial, criminal** or **employment history**
- **Identifiers** such as name, ID number, contact information, or online identifier (e.g. cookies)
- **Personal views**
- **Private correspondence**

Processing

Processing means, in effect, doing something with the data. Again, the POPI Act defines this similarly to the GDPR (see our article What Activities Count as Processing Under the GDPR?).

Examples of activities that constitute the processing of personal data include:

- Collecting an email address via a web form
- Storing a list of customers' addresses
- Sending a person marketing communications

Responsible Parties

Responsible parties are the main subject of the POPI Act. Responsible parties **determine the purposes and means** of the processing of personal information. Under the GDPR, responsible parties are known as data controllers.

Your business can act as a responsible party in a number of scenarios, for example when it:

- Collects a person's address in order to mail them a product
- Shares a person's email address with an email marketing company
- Stores the resumes of job applicants in a filing cabinet.

A responsible party decides **how and why** to process personal information.

Conditions for Lawful Processing

The POPI Act provides **eight conditions for lawful processing**. Think of these as legally-binding principles that must underpin all processing of personal information within your company.

The conditions for lawful processing can be summarized as follows:

1. **Accountability** - The responsible party must **ensure compliance** with the POPI Act
2. **Lawfulness** - The collection of personal information must **not be excessive**, it must **be legally justifiable**, and it must not be collected from **third parties without good reason**
3. **Purpose limitation** - Personal information must only be collected in connection with a **specific purpose** and must not be stored for **longer than necessary**
4. **Restriction on further processing** - Personal information may only be processed for a purpose other than that for which it was collected under **specific conditions**
5. **Information quality** - Personal information must be **complete and accurate**
6. **Openness** - Personal information must be processed in a **transparent** manner
7. **Security safeguards** - Personal information must be processed **securely** and the responsible party must provide **notification of any data breaches**

8. **Data subject participation** - People must be allowed to **access** their personal information and **request that it is corrected or deleted** if it is inaccurate

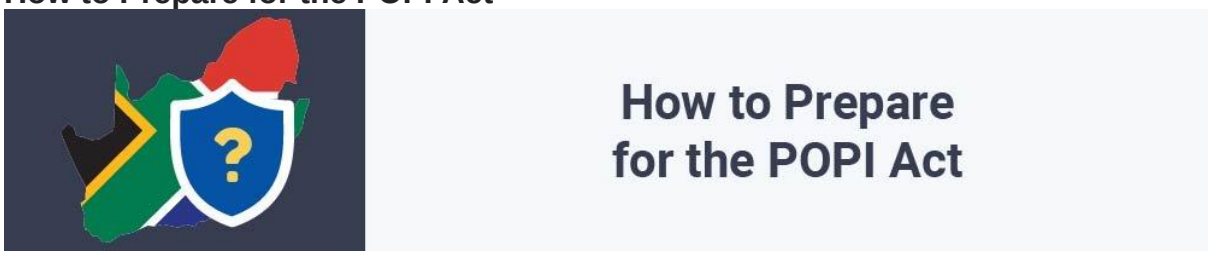
Penalties for Non-Compliance

The POPI Act provides **new powers** to penalize people and businesses who fail to comply with the Act. Such penalties vary in severity depending on the nature and seriousness of the offence.

Penalties for violating the POPI Act include:

- **Administrative fines** of up to 10 million South African Rand
- **Prison sentences** up to 10 years

How to Prepare for the POPI Act



All companies operating in South Africa should start preparing for the enforcement of the POPI Act. Here are some **practical steps** you can take toward compliance.

Conduct a Personal Information Audit

Your company probably handles a lot of personal information.

- You may be **storing** personal information in paper files, on hard disks, on web servers
- You might be **collecting** personal information via web forms, cookies, and mail
- You could be **sharing** personal information with marketing companies, analytics providers, and mail carriers

These are just a few examples. Think carefully about **personal information flows** within your company.

You can't comply with the rules in the POPI Act unless you know what personal information is in your control.

Designate an Information Officer

All organizations, public or private, are required to designate an **Information Officer** under the POPIA.

This role is comparable to that of a Data Protection Officer under the GDPR. However, whereas a Data Protection Officer is not always required under EU law, the requirement to appoint an Information Officer falls on **all South African companies**.

The Information Officer can be anyone within your company, but their appointment must be approved by the head of your company.

An Information Officer's duties include:

- Ensuring the company complies with the POPI Act
- Dealing with data subject rights requests (see below)
- Working with the Information Regulator

Facilitate Data Subject Rights

The POPI Act provides **new rights for data subjects**. A data subject is a person whose personal information has been processed. To put this in context, if you hold someone's personal data on file, that person is a data subject, and you must respect their data subject rights.

The POPI Act provides three data subject rights: **access, correction**, and **deletion**. These rights are only available under limited circumstances.
It's important that staff in your company know how to recognize such a request. You should provide a means of making such a request, for example your Information Officer's email address or a secure web form.

Access to Personal Data
If a data subject requests **access** to their personal information, you must provide them with a copy of any personal information you hold on them. You must also let them know which **third parties** have had access to their personal information (if any).
You must supply this information:

- Within a reasonable time
- In a reasonable manner
- In a generally understandable form

You **may** charge a fee for this service. The data subject must provide proof of their identity.

Correction and Deletion of Personal Data
The rights of **correction and deletion** apply only to personal information that is:

- Inaccurate
- Irrelevant
- Excessive
- Out of date
- Incomplete
- Misleading
- Obtained unlawfully

If you hold such personal information regarding a data subject then you must correct or delete it on request.
Implement Security Measures
One of the most important aspects of data protection law is the requirement to **store and transfer personal information in a secure way**.
You can think of your security responsibilities under the POPI Act as a three-part process:

1. Risk assessment
2. Technical measures
3. Breach notification

Risk Assessment
Section 19.2 (a) of the POPI Act requires the responsible party to "*identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control.*"
Consider the following questions in relation to each set of personal information in your possession:

- Do we **need** to collect this personal information?
- How long do we need to **retain** it?
- Who else needs **access** to it?
- How might someone **illegally** gain access to it?

Technical Measures

There are many ways to secure personal information in transit and storage. At the broadest level, these consist of:

- **De-identification** (anonymization) - Scrubbing personal information of all identifiers. This is the most effective way to secure personal information, but will be appropriate only if you'll never need to re-associate it with an individual data subject.
- **Pseudonymization** - Swapping out identifying details in a set of personal information, which can then be re-identified with reference to additional information, stored separately.
- **Encryption** - Scrambling the entire contents of a set of information using mathematical techniques. This can be performed on a single file, in transit (via TLS/SSL protocols), or on an entire hard disk.

Breach Notification

Section 22.1 of the POPI Act imposes an obligation on responsible parties to **notify the Information Regulator** of data breaches "*as soon as reasonably possible.*" Under certain conditions, you must also **notify the individuals** who have been affected by the breach.

This topic will be on the mind of many South Africans following the high-profile Liberty Holdings data breach.

To ensure you can mitigate the damage caused by a data breach, you should consider creating a Data Breach Policy. This will enable all staff to quickly and effectively identify and respond if the worst happens.

Review Your Direct Marketing Methods

The POPI Act builds upon existing direct marketing rules under South African legislation such as the **Consumer Protection Act (CPA)** privacy law.

Chapter 8 of the POPI Act sets out the conditions under which you may send a person marketing communications. The recipient of marketing communications must either:

- Give their **consent**, **or**
- Be an **existing customer**

In either case, there must be a clear way to withdraw from receiving marketing communications. This could be, for example, an **unsubscribe** link in an email.

Consent

The POPI Act defines consent as a "*voluntary, specific and informed expression of will.*"

Let's break that down:

- **Voluntary** - Consent must be "opt-in" or "express." You cannot assume that a person has consented. This precludes the use of pre-checked boxes that make statements such as "yes, subscribe me to your newsletter."
- **Specific** - Requests for direct marketing consent must be made **separately from other requests**. There is arguably an exception to this rule in the context of making a sale (see below).
- **Informed** - You must be upfront with people about the implications of providing consent. Don't pretend that you will only be sending "news" if you're planning to send ads. Present a link to your Privacy Policy at the point of collecting any personal information.

This is very similar to the model of consent under the GDPR.

Existing Customers
You don't need consent to send direct marketing to your **existing customers**, so long as:

- You received their contact details in the context of **making a sale**,
- You're marketing something relevant to a product or service they've **already bought, and**
- You offer the person a **clear means to opt out**

Create a Privacy Policy
A Privacy Policy is a public-facing document that tells your customers (or anyone else) how you process personal information. A Privacy Policy should be written in clear, plain language and made available via your company's website.
The Privacy Policy requirements under the POPI Act are very extensive. If your company has a GDPR Privacy Policy then it will likely be close to being compliant with the POPI Act.
Here are some examples of the sorts of information that you're required to include in your Privacy Policy under the POPI Act:

- The **name** and **contact details** of your company
- The **source** and **nature** of the personal information you collect
- Your **purpose** for collecting personal information
- What will happen if people **fail to provide** personal information in a given situation
- Information about the **rights of access and correction**

Summary
The POPI Act is a big step forward for privacy in South Africa. It brings the country closer to the data protection standards of other large economies, such as those in the EU.
Whilst compliance with the Act may seem daunting, it's important that your business **takes the necessary steps now** to avoid legal issues in future.
Some first steps toward compliance with the POPI Act include:

- Understanding your **legal obligations** under the Act
- Conducting a **personal information audit**
- Designating an **Information Officer**
- Preparing to facilitate **data subject rights**
- Implementing information **security measures**
- Reviewing your **direct marketing** practices
- Creating a **Privacy Policy**

https://www.termsfeed.com/blog/south-african-popi-act/