POPI ACT

HANDBOOK

SOUTH AFRICA'S POPI ACT

The privacy legislation conversation largely revolves around the **General Data Protection Regulation (GDPR)** recently put in place by the European Union. Although it's the most comprehensive and sweeping regulation in place, it is far from the only one.

If you live or operate a business in South Africa, you will soon have your own legislation to contend with. And a survey conducted in early 2019 suggests that only 34 percent of South African organizations are ready for it.

In 2013, South Africa passed the Protection of Personal Information Act (POPI). Although it predates the GDPR, it's often referred to as South Africa's GDPR equivalent. **The goal of the POPI Act is to protect data subjects from security breaches, theft, and discrimination**. To accomplish this, it outlines eight principles that South African data processors must follow.

Each principle encourages responsibility, security, and consent. It also provides special protections for distinct categories of data as well as the data of children.

What is POPI, and what does it mean for South African institutions and data processors? Keep reading to learn what POPI includes and learn how to comply with the law.

WHAT IS POPI?

POPI is shorthand for the **Protection of Personal Information Act No. 4 of 2013**. Signed into law on November 19, 2013, parts of the law became effective on April 11, 2014. The rest of the law was still on the books but inactive in 2019.

The Act includes a grace period of 12 months for businesses to update their systems after the regulator becomes fully operational. The regulator, Advocate Pansy Tlakula was appointed 1st July 2020. Therefore, the Act becomes formal law from the 1 July 2021. However, given that it takes six months to two years to implement a POPI-compliant plan, the Information Regulator says businesses should already be preparing - even without a formal launch date.

In essence, POPI applies conditions for the lawful processing of personal data of South Africans (both South African citizens and those living in South Africa). It includes eight general conditions and three less descript conditions.

Like the GDPR, POPI makes responsible parties culpable for failures among those who process data on their behalf.

It also provides South Africans with rights regarding unsolicited electronic communications.

POPI differs from other privacy laws in several ways, but the biggest difference lies in **consent**. POPI does not require you to get consent from data subjects before processing their data. The only case in which consent is required is when processing special types of data and the data of children.

For most South African companies, the biggest change was the introduction of restrictions for processing special types of personal information (including children's data). Marketing, healthcare, and the financial industry are among the most affected because they deal with the largest amount of personal information.

WHO DOES POPI APPLY TO?

POPI applies to data processors or responsible parties who are either domiciled in the Republic of South Africa or who are domiciled elsewhere but "makes use of automated or non-automated means" in South Africa.

"Automated" refers to using equipment that processes information automatically according to a data processor's instructions.

POPI regulates your business's use of personal information. According to the text, personal information is:

"*information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person*."

WHO IS EXEMPT FROM POPI?

POPI largely applies to people or groups in South Africa who process data for commercial purposes. The law cites exclusions from coverage, including:

Data processed for personal reasons.

Data that is de-identified and cannot be reinstated.

Data process by (or for) a public body relating to national security, law enforcement, or the justice system.

Data processed by a province's Cabinet and committees or Executive Council.

The data also includes any processing completed for literary or artistic expression or for the purposes of journalism. POPI deems processing for these purposes to be a matter of public interest and any limits on the processing could be seen as an infringement on freedom of expression.

THE POPI ACT'S EIGHT CONDITIONS FOR LAWFUL PROCESSING

POPI issues its rules for using South African data in Chapter three. It refers to these rules as conditions, and they largely cover what data you collect, what you can do with the data, and how you protect both the data and the data subject.

POPI includes eight conditions for lawful processing including:

1. Accountability
2. Processing limitation
3. Purpose specification
4. Further processing limitation
5. Information quality
6. Openness
7. Security safeguards
8. Data subject participation

We provide an overview of all the conditions below. For a full expression of the conditions, read Chapter 3 of the act.

- Condition 1: Accountability

Condition 1 refers to Accountability.

It stipulates that the responsible party has the responsibility of ensuring the rest of the conditions are in place before processing data. The responsible party must also ensure compliance both when deciding to process data and during the processing of the data.

Effectively, the first condition places the blame squarely on the shoulders of the data processor and no one else. Doing so makes it easier to investigate, cite, and punish violations of the law.

- Condition 2: Processing Limitation

The second condition - Processing Limitation - places strict controls on what it means to lawfully process data. To meet the condition, data processors must:

- Process data in a way that doesn't risk the data subject's privacy.
- Process only relevant data with a given purpose.
- Obtain consent from the data subject before processing (and keep proof of consent)
- Protect the legitimate interest of the data subject.
- Allow data subjects to object to processing and/or withdraw consent at any time.
- Stop processing data after an objection or withdrawal of consent.

Condition 2 also provides a unique stipulation: "Personal information must be collected directly from the data subject" except for in specific circumstances.

The only time you can collect data from a third-party source is if the data is public record or is deliberately made public or if you have the consent to do so or if doing so does not violate the legitimate interest of the data subject.

There are also exceptions for those working in court proceedings, law enforcement or public bodies.

- Condition 3: Purpose Specification

Where Condition 2 limits the data you can collect, Condition 3 - Purpose Specification - details your reasons for collecting data.

The idea that you must collect information only for a "specific, explicitly defined and lawful purpose" related to one of your normal activities is at the heart of the law. Moreover, you must ensure that data subjects are aware of that purpose.

Additionally, you can't hold onto records forever. Once you no longer need them for the processing purpose, you no longer have a right to keep them unless required by law (civil, penal, contract, or other law).

Once you no longer have a right to hold onto the file, you must "destroy or delete...or de-identify" the record as soon as practical. The process should render the data irretrievable.

- Condition 4: Further Processing Limitation

Conditions 2 and 3 aren't the only processing limitations. Condition 4 - Further Processing Limitation - continues to elaborate on how you can and can't process data.

The main point noted here says that you must only process data in ways compatible with the purpose you stated.

How do you know if you can process data further? POPI requires you to consider the relationship between further processing and the original purpose, the nature of the information, potential consequences of further processing, how you collected the data, and any contractual rights.

You can always further process data if:

- The data subject consented.
- The information came from the public record.
- The law requires further processing.
- The processing is related to national security.

- Condition 5: Information Quality

Condition 5 says that you must take steps to ensure the data you collect and subsequently process is accurate and complete.

- Condition 6: Openness

Openness refers to your responsibility under the Promotion of Access to Information Act. Essentially, you must maintain strict documentation of all the processing activities you undertake.

Additionally, you need to let data subjects know when you collect information. They should know:

- Where you collect information
- Where you don't collect information
- The source of your information
- Your company's name and address
- Why you collect the data (your purpose)
- Whether the collection is voluntary or mandatory
- What happens if the data subject doesn't provide their data?
- Laws that allow data collection
- If and when you intend to send the data to a third country

These must all be shared before you collect information from the data subject.

Condition 6 requires you to have a Privacy Policy that shares your data processing practices in detail.

- Condition 7: Security Safeguards

Condition 7 details the security measures POPI requires for personal information.

It says that the responsible party must employ "appropriate, reasonable technical and organizational measures" designed to prevent both unlawful access and the loss or damage of the personal information.

To meet these obligations, you must perform a risk assessment test, ensure the maintenance of safeguards, verify the effectiveness of the safeguards, and ensure new updates are provided to prevent new deficiencies or risks.

The law also says that anyone processing personal information must also only first gain the knowledge of authorization of the responsible party and consider the information to be confidential. Any other (third) parties who process information on behalf of the responsible party must sign a written contract and notify the responsible party if there is a breach.

Condition 7 also provides a long list of requirements if a responsible party believes its security is compromised. First, they must notify the Regulator and the data subject (when possible) and they must do so as soon as reasonably possible.

Data subjects must be notified in writing by email, letter, a news article, or by publishing an alert on a prominent part of the website. The Regulator may also direct the notification efforts as they see fit.

The notification must include enough information for the data subject so that they know what measures to take to protect themselves against further breaches.

Finally, the Regulator may require the responsible party to publicize the breach if the Regulator believes doing so is reasonable.

- Condition 8: Data Subject Participation

Condition 8 lays out the rights of the data subject. Under the law, they have access to their personal information, including learning what information the responsible party has the option to ask for a description or record.

The data subject also has the right to request corrections to their record when the data is out of date, incomplete, inaccurate, excessive, or obtained unlawfully. Upon receiving the request, the responsible party must complete the request within a reasonable timeframe.

Responsible parties have the option to decline when it falls within their rights as stated in Chapter 4 of the law.

Condition 8 also has several parts. Part B refers to the prohibition of processing of special personal information (including religious beliefs, health information, biometric information, etc.) or criminal behaviour. The only exceptions that apply include:

- If the data subject provided consent
- If processing is necessary for establishing a defense of a right
- If processing is required for fulfilling obligations under international public law
- If processing is in the public interest
- If the data is already public (through the data subject correctly)
- If processing involves historical research, or statistical purposes (within the public interest or if asking consent is impossible or close to impossible)

POPI puts significant emphasis on these special categories of information and each type of data has a list of exemptions. If you need to process a protected type of data, refer directly to the law, and seek legal advice.

Finally, Part C deals with the data of children. Responsible parties may not process children's personal information unless:

- You have the consent of a "competent person".
- It is necessary for obligations under the law.
- It is required for upholding international public law.
- It is necessary for research purposes.

The Regulator may also grant permission if it is in the public interest and you agree to use the appropriate safeguards. In addition, the Regulator may also impose further conditions related to the nature of the data, the amount of information, and the method of processing.

HOW TO COMPLY WITH SOUTH AFRICA'S POPI ACT

If you process data in South Africa, then you have an obligation to comply with POPI. But what does that mean in practical terms.

The principles of compliance mean you must:

- Obtain consent before collecting data (or processing, storing, or sharing it)
- Be sure to only collect data needed for legitimate purposes.
- Use the information in a way that matches the purpose of collection.
- Take reasonable security steps to protect the integrity of the information.
- Store the information only as long as required.
- Uphold data subjects' rights by providing access and corrections to information.
- Create policies to notify the Regulator about your processing activities, such as a Privacy Policy.

The South African government says it can take up to two years to fully prepare for POPI compliance. Here is what you will need to do in the meantime.

EXAMINE THE IMPACT ON YOUR BUSINESS

How will POPI impact your business? The first step towards reaching compliance is understanding of what personal information you collect, how you process it, and how POPI impacts your essential business processes.

As per Condition 4, you need to know the purpose of the personal information you collect and the purpose of processing. If you need to undergo further processing, then you need to ensure it is also compatible with the initial collection.

NOMINATE A DEDICATED INFORMATION OFFICER

Complying with POPI usually means you need someone who fully understands the law and your data practices.

If you do not already have an Information Officer, then your CEO/Owner fills the role by default. However, CEOs rarely have time to complete their existing duties and POPI compliance, so it is best to find someone who can encourage compliance, deal with requests, work with the Regulator, and actively monitor compliance.

PERFORM A POPI GAP ANALYSIS

Responsible businesses already take care when processing data. However, you'll need to identify what areas of POPI compliance you already meet and where you are deficient.

Each gap analysis is unique to the organization. But as a baseline, you should know that your IT infrastructure and personnel resources should allow you to engage in best practices for your industry.

COMPLETE RISK ASSESSMENTS

POPI's security requirements require you to take necessary measures for protecting your information. The request is broad, but it is meant to be. You need to take further steps to protect banking details and protected personal information than of a database consisting of only email addresses.

A risk assessment is an opportunity to identify your security strengths, weaknesses, and be sure that you can cope with the threats your business faces.

DRAFT NEW POLICIES AND UPDATE EXISTING DOCUMENTS

POPI requires you to update your existing policies and create new ones. You'll need documents such as:

- Privacy Policies
- Information Security Procedures
- Incident Response
- Information Manuals
- Reporting procedures

You must also share these policies with your staff and third-party partners so that everyone knows what to do to comply with POPI.

CREATE A COMPLIANCE MANAGEMENT SYSTEM

Compliance is not a one-and-done event. It's an ongoing and active process that requires management.

You should have an active compliance plan that provides you with a systematic way to review and update your processing standards.

IF I'M GDPR COMPLIANT, AM I ALSO POPI COMPLIANT?

Although there are differences between POPI and the GDPR, it is generally recognized that being compliant with the GDPR makes you largely ready for POPI.

You need to know two major differences between the GDPR and POPI.

First, the GDPR relates to the personal information of individuals. It does not protect businesses. POPI, however, extends its protections to legal entities, which means it protects information collected about companies and corporations as well as the data of individuals. That means complying with POPI requires you to add the same protection to your suppliers' or partners' data in addition to your customers.

The second biggest difference lies in the development of privacy programs. The GDPR advocates for "privacy by design" rather than privacy as a function. POPI recommends best practice options for privacy and security, which means that POPI's privacy requirements are slightly less stringent - at least in theory.

Thought leadership thus far considers POPI compliance to be a steppingstone to GDPR compliance, but you should be sure that your systems do meet POPI requirements within a year after POPI becomes active law.

WHAT HAPPENS IF YOU DON'T COMPLY: FINES AND PUNISHMENTS?

Failing to comply with POPI will be an offense. However, failure to comply isn't the only way to violate the law. Interfering (hindering, obstructing, or influencing) with the Regulator is also an offense as is failing to attend hearings or lying under oath.

Chapter 10 and 11 of the law cover the enforcement and punishments for non-compliance of POPI, respectively. In this case, non-compliance refers to the "interference with the protection of personal information of data subject," which includes:

- Breaches of the conditions required for lawful processing.
- Failure to comply with sections 22,54,69,70,71, or 72 of the law.
- Breaches of section 60 (code of function)

The penalties for anyone convicted of violating the terms of POPI (an offense) include a fine or imprisonment (or both).

Prison time could be as long as 10 years for violations of section 100, 103(1), (104(2), 105(1), (106(1)(3)(4). A lesser sentence of up to 12 months is applied to convictions related to section 59, 101, 102, 103(2) and 104(1).

The Regulator may apply administrative fines not to exceed R10 million. The total fine is subject to the Regulator's discretion and may depend on:

Type of personal information involved:

- Number of data subjects affected (or possibly affected)
- Duration of the violation
- Likelihood of damage to data subjects
- Failure to carry out a risk assessment
- Previous offenses
- Preventability of the violation
- Whether the issue is a matter of public importance

ARE YOU READY FOR POPI?

Ultimately, if you process data fairly, ethically, and safely, then POPI is unlikely to require dramatic changes to your business. But a gap assessment and risk assessment will tell you what comes next and direct the policies your write for your organization.