POPI

Are You Ready?

ALL YOU NEED TO KNOW ABOUT THE POPI ACT AND HOW TO BE COMPLIANT

FREE E-BOOK

What is POPI?

POPI refers to South Africa's Protection of Personal Information Act which seeks to regulate the Processing of Personal Information.

Personal Information broadly means any information relating to an identifiable, living natural person or juristic person (companies, CC's etc.) and includes, but is not limited to:

- contact details: email, telephone, address etc
- demographic information: age, sex, race, birth date, ethnicity
- history: employment, financial, educational, criminal, medical history
- biometric information: blood type etc.
- opinions of and about the person
- private correspondence etc.

Processing means broadly anything that can be done with the Personal Information, including collection, usage, storage, dissemination, modification or destruction (whether such processing is automated or not).

Some of the obligations under POPI are to:

- only collect information that you need for a specific purpose.
- apply reasonable security measures to protect it.
- ensure it is relevant and up to date.
- only hold as much as you need, and only for as long as you need it

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.

Accountability for compliance rests with a Responsible Party, meaning a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

This applies to:

- All Sole Proprietorships
- All Partnership Companies
- All Private Incorporations
- All Non-profits, Trade Unions etc
- All Public Bodies

Exclusions include:

- purely household or personal activity.
- some state functions including criminal prosecutions, national security etc.
- journalism under a code of ethics.
- judiciary functions.

Know Your Consumer Rights

- Direct Marketing (Opt in & Opt out)
- Right to Access Data (PAIA)
- Right to know what data is on record
- Right to correct data
- Right to delete data
- Right to object to processing of data
- Right to appeal rejection to access

Why Should You Comply?

POPI promotes transparency with regard to what information is collected and how it is to be processed. This openness is likely to increase customer confidence in the organisation. Protect and maintain your reputation and Brand.

POPI compliance involves capturing the minimum required data, ensuring accuracy, and removing data that is no longer required. These measures are likely to improve the overall reliability of the organisation databases.

Compliance demands identifying Personal Information and taking reasonable measures to protect the data. This will likely reduce the risk of data breaches and the associated public relations and legal ramifications for the organisation.

Non-compliance with the Act could expose the Responsible Party to a penalty of a fine and / or imprisonment of up to 12 months. Avoid risk and abide by the law.

8 Conditions of Lawful Processing

POPI refers to the 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.

These include:

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

1. 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.

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.

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.

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

5. Information Quality

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

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.

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.

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 behavior.

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.

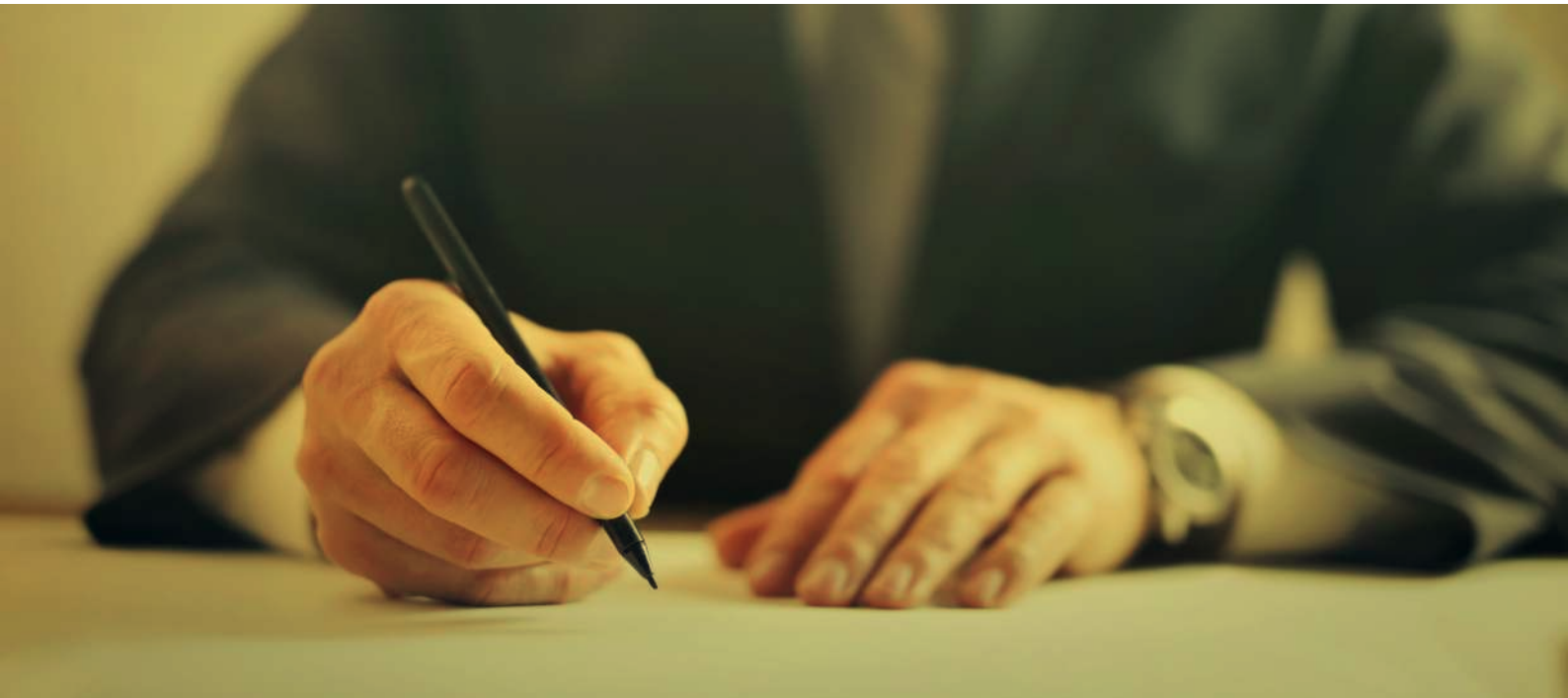
How to Comply with the POPI Act

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

Examine. Prep. Act. Maintain.

- Examine what personal information you collect, why and how it is processed, stored and secured. Impact Assessment.
- Nominate and Register a Dedicated Information Officer & Deputy Officer/s.
- Perform a gap analysis and risk assessments in line with POPI requirements and your unique organization/ industry needs.
- Prepare and update existing/ new policies & documents in line with POPI requirements.
- Create and maintain a platform for query management and reporting.



Consequences of Non-Compliance

Fines and/or Imprisonment...

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.

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

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

Ultimately, if you process data fairly, ethically, and safely, then POPI is unlikely to require dramatic changes to your business.