

Protection of Personal Information Act 2013 (POPIA)

What is POPIA?

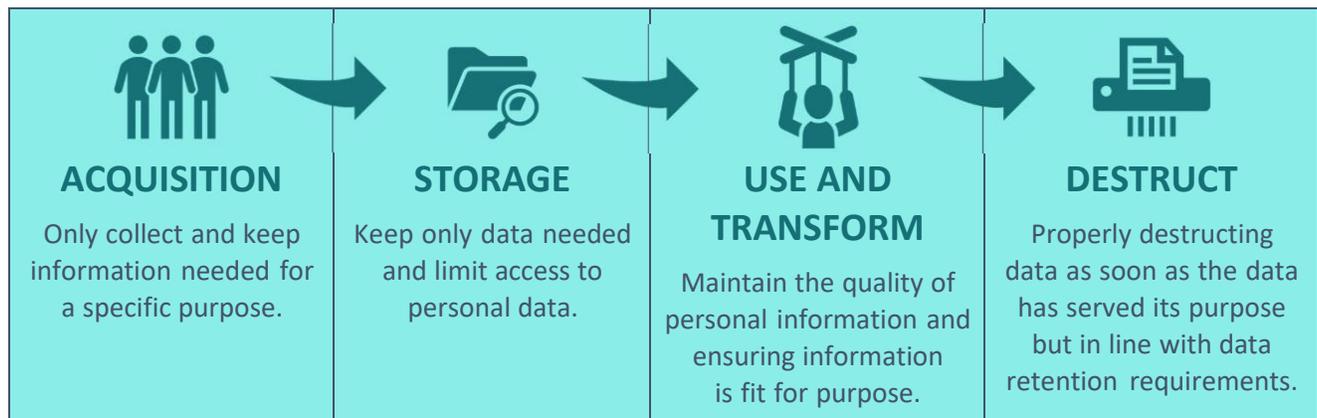
Serious change is happening in the world of privacy compliance, and at the forefront is POPIA (Protection of Personal Information Act) and GDPR (General Data Protection Regulation).

	<p>You say POPI. I say POPIA.</p> <p>POPI is short for the Protection of Personal Information and is a broad topic. POPIA, which is short for the Protection of Personal Information Act, refers to the actual Act. POPI and POPIA are often used interchangeably, although it is better to use POPIA when referring to the Act.</p>
---	---

How do these changes apply to your business in particular?

The Protection of Personal Information Act 2013 (POPIA) is South Africa's primary legislation dealing with personal information processing. POPIA is a law that applies to individuals and companies who process the personal information of other people. The Act intends to protect personal information and ensure its confidentiality.

POPIA is concerned with how personal information is used within an organisation. It deals with how personal information is acquired, transformed, used, stored, shared and destroyed.



What is Personal Information?

'Personal information' means any information relating to a **person**.

According to Section 1 of POPIA 2013 (POPIA, c2021), a **person** means an identifiable, living, **natural person** and an identifiable, existing **juristic person**, such as a registered company, closed corporation or trust.

PERSONAL DATA



- Name
- Date of Birth
- Marital Status
- Phone Number
- Email Address
- Residential Address
- Hair Colour
- Eye Colour
- Weigh
- Height
- Defining Characteristics
- Salary
- Education
- Tax Information
- Photographs
- IP Addresses
- Browser Cookies
- Geo-tracking Data
- Number of Sick Days
- Number of Holidays
- Bank Account Number

The list on the left is not exhaustive, the regulation defines **PERSONAL DATA** as any information which can directly or indirectly identify and individual. This wide scope could cover much more in your organisation.

Non-compliance can result in significant penalties – up to 10 years' imprisonment and/or ZAR 10 million in administrative fines.

POPIA prohibits the processing of special personal information.

SPECIAL CATEGORIES OF PERSONAL DATA



- Ethnic or Racial Origin
- Political Opinion
- Religious Beliefs
- Philosophical Beliefs
- Trade Union Membership
- Genetic Data
- Bio-metric Data
- Sex Life
- Sexual Orientation

Specific conditions of processing special categories of personal information must be met; for example, explicit consent from the data subject or processing is needed to meet the obligation.

What is expected of me to comply with the Act?

Lawful processing of personal information will be achieved by complying with the eight conditions set out in POPIA.

A Responsible Party must comply with all 8 conditions for lawful processing, namely:

ACCOUNTABILITY

You will be responsible for ensuring POPIA compliance.

PROCESSING LIMITATION

You must only process the information that you require.

PURPOSE SPECIFICATION

Personal information must be collected for a specific purpose.

FURTHER PROCESSING LIMITATION

Further processing of personal information (i.e., outside its original purpose) must be compatible with the original purpose of collection.

INFORMATION QUALITY

You must keep personal records accurate and up to date.

OPENNESS

You must disclose certain information to Data Subjects (i.e., that their information is being collected, where it is collected from and how it will be used.

SECURITY SAFEGUARDS

You must secure the integrity and confidentiality of personal information.

DATA SUBJECT PARTICIPATION

You must allow Data Subjects to access their personal information.

What are the POPIA roles?

There are several role players involved in the processing of personal information.

2. The Responsible Party is that public body, private body or any other person that either alone or together determine the purpose and means of processing personal information.

4. The Operator is that person or organisation that processes personal Information for a Responsible Party in terms of a contract or mandate, without falling under that party's direct authority.

1. The Data Subject is the person or organisation to whom the personal information belongs.

3. The Information Officer is the head of the Responsible Party and responsible for ensuring or encouraging all persons to comply with POPIA.

5. The Information Regulator (South Africa) is an independent body established in POPIA that can monitor and enforce POPIA AND PAIA compliance.

As an SMME, What are the three quick things you need to do to get closer to compliance?

From an employment perspective, employers should take the following steps to ensure POPIA compliance:

1

Appoint and register your **Information Officer** on the **Information Regulator Website**. If you are small, this can be yourself.

2

Speak to a legal advisor to draft relevant **internal data protection policies** and implement them across your organization.

3

Identify **training** for your team and yourself. Make sure everyone in your organization is **POPIA aware**.

Remember that to make it stick, compliance has to become part of your culture.



Make sure that everyone is aware of and understand their roles.



Make sure that complying is not a choice but a way of doing business in your organisation.



Communicate about POPIA often, even when things are going right!



Celebrate the small wins, all the time!