



POPI

PROTECTION OF PERSONAL INFORMATION



ABSOLUTE AVIATION



WHAT IS THE POPI ACT?

POPIA aims to regulate the collection and processing of Personal Information.

POPIA seeks to protect and prevent the abuse and misuse of Personal Information owned by individuals and companies in South Africa.

TO WHOM DOES POPI APPLY?

Any 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.

Any person who processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of the Responsible Party.

POPI also apply to personal information of companies.

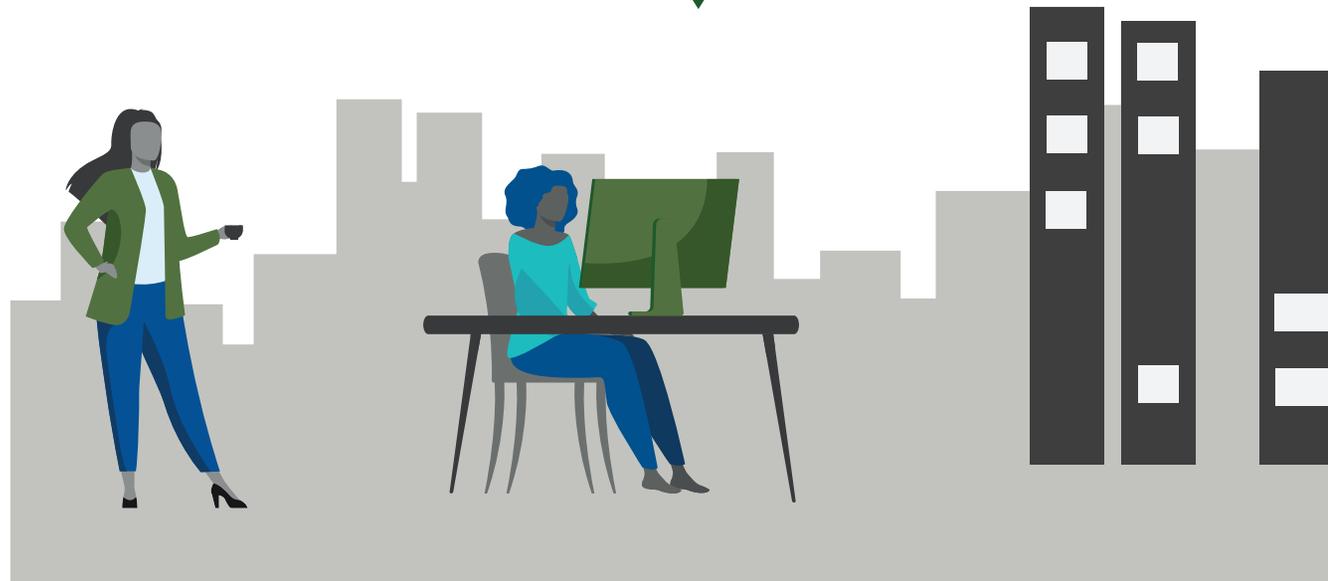
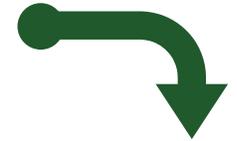
RESPONSIBLE PARTY



OPERATOR

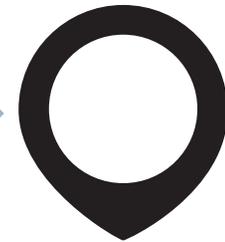
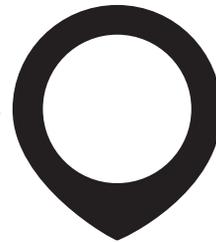
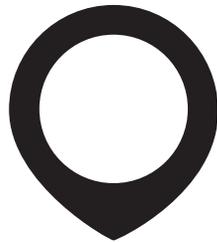
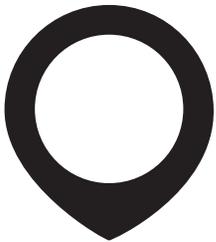


COMPANY INFO





IMPORTANT POPI CONCEPTS:



RESPONSIBLE PARTY

The person that collects and uses any individual or legal entity's Personal Information.

DATA SUBJECT

The individual or company, whose Personal Information is being collected, used and processed.

PERSONAL INFO

Any information that can identify a person or company including but not limited to:



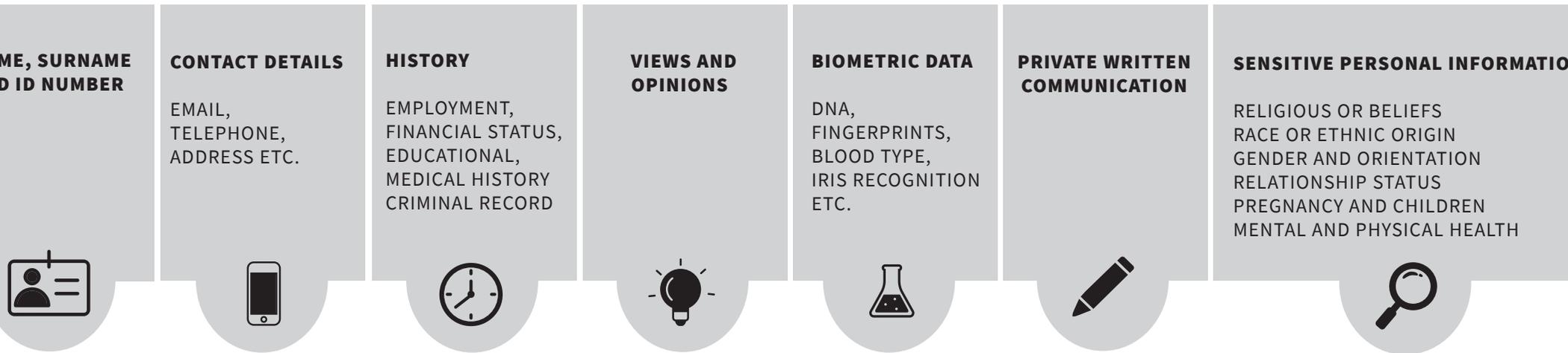
PROCESSING

Collecting information, receiving it, storing it, updating it, modifying it, distributing/viewing and destroying the data.

RECORD

Any digital or physical recorded information that is in the possession or control of a person in its capacity as a Responsible Party, irrespective of whether or not it created it.

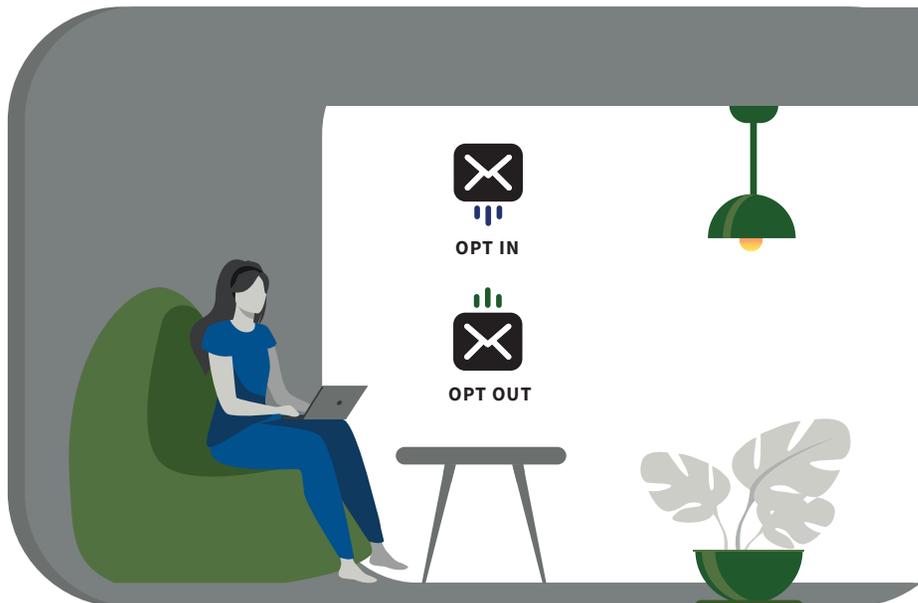
WHAT IS PERSONAL INFORMATION? (let's call it PI)



DOES POPI APPLY TO DIRECT MARKETING?

POPIA provides that the Responsible Party **CANNOT** process Personal Information for the purposes of direct marketing unless:

- The Data Subject is a **current customer** and the direct marketing is in respect of similar products or services as previously sold to the Data Subject and the Data Subject has given its **express permission (opt in)** to use the PI for the purposes of direct marketing;
- Where **not a current customer**, such Data Subject has to **“opt in”** to the use of its PI for the purposes of direct marketing; Finally note that all communications sent to the Data Subject must feature the Responsible Party’s identity, contact details and an **opportunity to “opt out”**.





INFORMATION PROTECTION PRINCIPLES

PROCESSING LIMITATION

1

Personal Information must be collected directly from the Data Subject and may only be processed with the consent of the Data Subject, or in the absence of consent where it is necessary to comply with a legal obligation, public law duty, or a contractual obligation.

INFORMATION QUALITY

4

The person or company in its capacity as the Responsible Party that processes PI should ensure that the PI is complete, not misleading, up to date, and accurate.

SECURITY SAFEGUARDS

6

The implementation of measures to secure the integrity of PI, and to guard against the risk of loss, damage or destruction thereto. PI must be protected against any unauthorised or unlawful access or processing.

SPECIFIC PURPOSE

2

PI must be collected for a specific, explicitly defined, and legitimate purpose. The Data Subject should be made aware of the purpose for which the PI is collected, and whom the likely recipients of the PI will be.

OPENNESS

5

Where PI of a Data Subject is collected, the Responsible Party must ensure that the Data Subject is made aware of:

- The fact that the information is being collected.
- The name and address of the person or company collecting the information.
- Whether or not the supply of the PI by that Data Subject is voluntary or mandatory and the consequences of not providing the PI.
- Where the collection of PI is authorised or required under any law, the particular law to which the collection is subject.

INDIVIDUAL PARTICIPATION

7

A Data Subject is entitled to the details of its PI held by any company or person, and to the identity of any person that had access to its PI. The Data Subject is entitled to require the correction of any incorrect PI held by a party or to have the PI destroyed.

FURTHER PROCESSING LIMITATION

3

PI may not be processed further in a way that is incompatible with the purpose for which the information was collected initially.

ACCOUNTABILITY

8

The Responsible Party i.e. the party or institution that holds Personal Information must give effect to the principles/conditions for the protection of Personal Information as set out under POPIA.



WHO REGULATES THE POPI ACT?



INFORMATION REGULATOR SOUTH AFRICA

POPIA creates an “Information Regulator” which is a supervisory body. The Regulator, will be independent and subject only to the Constitution.



RISK AND CONSEQUENCES OF NON-COMPLIANCE

Non-compliance with the Act could expose the Responsible Party to a penalty of a fine of R10 million and/or imprisonment of up to 10 years.



OPERATIONAL DATE → 1 JULY 2020



WHAT ABOUT TRANS-BORDER INFORMATION FLOWS?



Note that POPIA not only regulates Personal Information held in South Africa. It also seeks to regulate the transfer of PI to parties outside RSA.

THE RESPONSIBLE PARTY MAY NOT TRANSFER PI ABROAD UNLESS:

- The recipient is subject to a law, binding corporate rules, binding agreement or memorandum of understanding which provide an adequate level of protection that is substantially similar to the conditions for the processing of PI as set out in POPIA.
- The Data Subject has consented to the transfer.
- The transfer is necessary for the performance of a contract; or the transfer is for the benefit of the Data Subject and it was not reasonably practicable to get their consent.



HERE ARE A FEW EASY TIPS TO COMPLY: (the REALLY important stuff!)

Get the Personal Information directly from the Data Subject.

Make sure that the PI obtained is accurate and give the Data Subject the opportunity to rectify and update their PI.

Safeguard the PI and ensure that it does not fall into the wrong hands.

Only use PI for as long as the purpose for its collection exists. Once the purpose expires the PI must be permanently destroyed or de-identified.

