



The POPI Compliance Guide, is designed to help the companies understand all the privacy initiatives that will need to be implemented across the organisation so that you comply with the new Protection of Personal Information Act (“the Act”). This guide will aid in highlighting the risk areas applicable to our business and the documents and procedures required to help you implement your compliance measures.

This guide is applicable to to below diversified entities:

1. EBM Steel and Manufacturing Pty Ltd
2. Simrox Property Holdings Pty Ltd
3. Esheshayo Trading Pty Ltd
4. Simrox Steel and Pipe Pty Ltd

WHAT IS THE POPI ACT?

The aim of the POPI Act is to control the way in which personal information is handled and to regulate how that personal information should be processed, to ensure it is done in a responsible way. This would include the methods of collection, usage, storage, dissemination, alteration and destruction of any personal data and information.

The POPI Act headlines this process by asking you to identify a “processor of information” in your organisation and then to hold them accountable should any information be abused or compromised in any way.

For the most part, the requirements of POPI compliance are self-explanatory and easily implemented. The impending POPI compliance deadlines provide your organisation with an ideal opportunity to review the sort of information and data that you collect to manage all your client interactions, and store and use data for marketing purposes, among other tasks.

STEP 1: UNDERSTAND THE POPI GUIDELINES

The principles of POPI can be divided into eight practical guidelines that help us understand how we must legally process personal information. Every company that processes personal information, will need to comply with all eight of the requirements. In turn, each section has its own unique set of requirements.



ACCOUNTABILITY:

Your company will need to determine who will be responsible to ensure compliance with the POPI Act. This person will normally be the director of the company or an Information Officer that is appointed by the company, depending on the size of the business.

The natural person responsible for compliance with the POPI Act is known as the Information Officer. Your company can appoint the Information Officer by way of a Director's Resolution.

PURPOSE SPECIFICATION:

A company should only collect the information that is necessary for them to fulfill a specific purpose, and it must only be used for lawful purposes. The Information Officer will need to ensure all information is relevant and up to date and should only keep personal information for as long as it is necessary. The company should have limited access to personal information long enough for them to perform the purpose of that data.

INFORMATION QUALITY:

The company that processed the information, has a duty to ensure the information is kept up to date, complete and correct. This duty can be transferred to the data subject (owner, client or employee) providing the personal information.

The Terms & Conditions or agreements entered into must expressly communicate that it is the data subject's duty to ensure their personal information remains updated and they should communicate any changes on to the relevant party within the company.

SECURITY SAFEGUARDS:

The POPI Act states that processors of information are responsible for protecting all the personal information they have in their possession. As such, your Information Officer will need to be able to provide proof that they have taken all reasonable steps to ensure that all personal information held is safeguarded.

The company should also identify all reasonable and foreseeable internal and external risks to data abuse, theft or loss, and establish and maintain appropriate safeguards.

PROCESSING LIMITATION:

Any Personal Information that you collect must be processed lawfully in a reasonable manner that does not infringe on the privacy of a data subject such as your client or marketing database. The personal information may only be collected and processed if it is adequate, relevant, and not excessive. And most importantly, personal information can further only be collected if the data subject consented to it! You can only collect data directly from the data subject.

FURTHER PROCESSING LIMITATION AND DATA SUBJECT PARTICIPATION:

The further processing or use of personal information is expressly prohibited by the POPI Act unless that processing is compatible with the initial purpose of collecting information - or if the further processing of the information is done with the data subject's consent.

OPENNESS:

The data subject can request that the company provide them with the record, or a description of their personal information held by the company. Then, the company must provide this information to the owner of the information within a reasonable time, in a reasonable manner and in a format that is generally understandable.

It would be best that the company prepare itself for requests of information by the data subjects. They should have a procedure in place to deal with this type of request. This can be as simple as having the data subject complete and sign a form requesting certain information.

DATA SUBJECT PARTICIPATION:

Data subjects have the right to establish whether personal information is held by a responsible party and to have it corrected or destroyed if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or has been obtained unlawfully.

STEP 2: APPOINT AN INFORMATION OFFICER

In order to ensure that your organisation complies with in terms of the POPI Act, you will need to formally appoint an Information Officer.

The appointed Information Officer of the Company is entrusted with the following responsibilities:

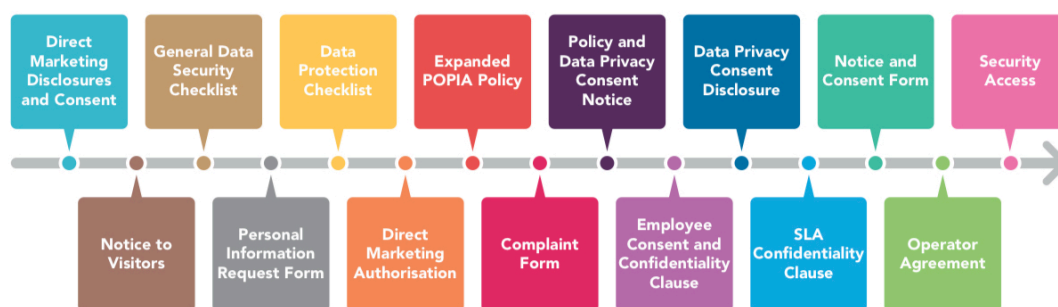


STEP 3: ESTABLISH A BASIC POPI ACT POLICY

A framework of a POPI Act Policy is provided here. This general POPI policy will assist you at a foundational level as you begin to process, analyse and manage the data and personal information you collect. It is vital that this policy is then adapted to suit your unique requirements so that it covers any potential risks. The Information Officer will provide a separate guide for the POPI Manual.

STEP 4: UNDERSTAND THE UNIQUE IMPLICATIONS OF THE POPI ACT ON YOUR ORGANISATION

Apart from understanding the POPI Act and its guidelines, there may be a number of additional requirements or necessary internal and external documents that will be unique to the type of operation or structure. These documents may include:

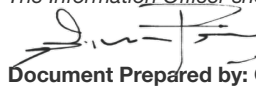


The Information Officer will compile a detailed policy for filing on or before the implementation date of the ACT. It should be noted that failure to adhere to the conditions in the ACT on 01/07/2021 will result in:

- A fine issued for up to R 10 million, or
- Imprisonment for up to 10 years, or
- A fine issued for up to R 10 million and imprisonment for up to 10 years.

** This document remains the sole property of the mentioned entities and may not be reproduced, stored or copied in any way whatsoever. Written permission must be obtained from the company to use or share this document:*

The Information Officer should approve such consent.


Document Prepared by: Q. Pelser

Document: SEES-POPI-2021-1

Revision: 0