Compliance Declaration

By

CLAASSEN AURET (PTY) LTD

In terms of

The Protection of Personal Information Act no. 4 2013, (POPIA)

OVERVIEW

POPIA came fully into effect on 1st July 2020, with a 12-month grace period; therefore, all South African companies need to comply with the requirements by **30th June 2021**.

POPIA demands that companies operating within South Africa which collect, process and store Personal Information in respect of natural persons (individuals) and juristic persons (other businesses), ensuring that they take sufficient precautions to protect that information from being stolen through hacking, or loss through ransomware or theft of IT hardware.

The purpose of the law is to ensure all South African businesses conduct themselves in a responsible manner by holding them accountable should they fail to protect or compromise Personal Information in any way.

The supervisory authority known as the **Information Regulator (IR)**, Advocate Pansy Tlakula and her team, will investigate any data breaches reported to the IR's office, which will show either compliance, or prove non-compliance.

The situation is therefore, that any business that experiences a data breach is expected to report the breach to the IR's office. Alternatively, a Data Subject (either a natural person or juristic person) who/that has been negatively affected by a data breach, can also report this to the IR's office, but it is expected that the business will be proactive and report it first.

It is the IR team's job to investigate breaches that have been reported, looking at how and why the breach occurred, how many Data Subjects have been potentially affected and if the business reporting the breach **has taken reasonable steps to avoid such breaches taking place**.

It is this type of investigation that poses the biggest threat to any business, in terms of penalties, if no effort has been made to become POPIA compliant. All businesses are held to the same security and compliance standards, irrespective of size. Business size and activities will dictate the complexity of the implementation plan and processes to be followed.

POPIA DEFINITIONS

- A **Data Breach** is a release/exposure/loss/leak/spill of private Personal Information in respect of Data Subjects, to an untrusted environment.
- **Data Subjects** are natural (human) or juristic persons to whom gathered/processed/stored Personal Information relates.
- **Juristic Persons** are legal entities such a companies, close corporations or any other legally-formed entity.
- **Operators** are individuals and/or businesses that process Personal Information of Data Subjects on behalf of the Responsible Party.
- **Processing** means collection, use, storage, dissemination, modification or destruction.
- **Responsible Party** is the person or organisation who requires the information to be gathered and processed.

Undertaking by Claassen Auret (Pty) Ltd

Currently there is no independent measurement for POPIA compliance, but the onus is on us to report any data breach we experience to the Information Regulator, proving that we **have not acted** negligently or disregarded the need for robust protection measures.

We hereby confirm that our company are POPIA compliant, by way of having taken all reasonable measures, to protect and keep private, the Personal Information of our Data Subjects.

Our compliance goals are:

- To avoid as much as possible, any data breaches from happening;
- To protect clients and other Data Subjects by processing their Personal Information lawfully;
- To protect the company brand and build trust with clients and other Data Subjects;
- To be able to prove to the Information Regulator, if required to do so, that the company had made every reasonable effort to prevent data breaches from occurring.

The processes we are following include:

- Conducting a business impact assessment and IT hardware assessment
- Identifying data flows within the business
- Reviewing company data processing and data storage systems
- Destruction of old data and client information, with reference to requirements by other South African laws
- Reviewing access to data and company login permissions
- Implementation of updated policies containing POPIA requirements
- Implementation of procedures for reporting of data breaches, both internally and to the Information Regulator
- Updating existing contracts with our Data Subjects
- Updating contracts with authorised Operators
- Registration and appointment of an Information Officer and Deputy Information Officer
- Awareness training for all company employees
- Training for the Information Officer / Deputy Information Officer

Signed at Ormonde, on today, 1 July 2021.

SAREL CRAUSE – Director

Information Officer