Protection of Personal Information Bill (POPI)

Topic: Rights to Privacy

IN A CALABASH

Introduction

The Protection of Personal Information Bill (POPI) is set to become law shortly. When it does, it will have significant implications for both the citizens of this country whose information is processed by any number of companies and public bodies and for the companies and public bodies that process this personal information.

The POPI Bill is a dedicated law aimed at protecting personal data from abuse and misuse. Once bill becomes an Act, public and private entities will have one year from the date the Act comes into operation to ensure that they comply with the provisions of the POPI Bill.

Objectives of the Act

The POPI Bill aims to regulate the collection and processing of personal information by both private and public bodies, including the State. The Bill also seeks to protect and prevent the abuse and misuse of personal information owned by individuals and companies in South Africa, which is collected, processed and used by these private and public sectors.

The POPI Bill, however, must not been seen as a law which frustrates the operation of a business. To this end, it seeks to create a careful balance between one's constitutional right to privacy and the needs and interests of commerce, government and business.

Application of the Bill and its implication to Tourism

The POPI Bill will regulate the processing of personal information within South Africa, including the processing of personal information that is entered in a record by a company or public body that is domiciled in South Africa or a public body that is domiciled elsewhere but which uses automated or non-automated means situated in South Africa.

The POPI Bill will apply to all entities, both public and private, and to all information belonging to private and public bodies or individuals.

The POPI Bill will apply to all information belonging to private and public bodies or individuals.

The POPI Bill therefore has to be complied with by every individual or legal entity, be it public or private, that collects and processes personal information.

Compliance by an entity can and should be delegated to a duly appointed information officer.

Summary of the provisions of the Bill

POPI concepts

The POPI Bill refers to certain concepts, which have been explained below.

The company or public body that is responsible for processing the information is referred to as the 'responsible party', whereas the individual or company whose information is being processed is referred to as the 'data subject'.

'Personal information' which may be processed, collected and used will include any information related to a private or public entity and/or a natural individual including–

- name, address and ID number;
- blood type and fingerprints;
- educational, medical, criminal or employment history, as well as information pertaining to financial transactions;
- views or opinions; and
- information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.

When a person attempts to collect personal information, this will be known as 'processing' which has been defined to mean collecting, receiving, storing, updating, modifying, disseminating and destroying information.

In turn, any document or detail of a personal nature held by a responsible party will be referred to as a 'record', which has been defined to mean any recorded information in any form that is in the possession or control of a company or public body, irrespective of whether or not that company or public body created it.

Information protection principles

The POPI Bill has adopted eight core international principles which apply to the processing of personal information. Once a reader understands these principles, the provisions of the POPI Bill will make sense. The eight principles are outlined below:

Principle 1: Processing information

Personal information must be collected directly from the data subject and may be processed only with the consent of the data subject or, where it is necessary to comply with a legal obligation, a public law duty or a contractual obligation.

Principle 2: Specific purpose

Personal information must be collected for a specific, explicitly defined and legitimate purpose. The data subject should be aware of the purpose for which the information is collected and who the likely recipients of the information will be.

Principle 3: Further Processing Limitation

Personal information may not be processed in a way that is incompatible with the purpose for which the information was initially collected. Thus, if information was processed for the purpose for which it was collected, it may only be processed further if it can be shown that the purpose of the further processing is compatible with the original purpose. The POPI Bill provides guidelines to assist with such an assessment.

Principle 4: Information quality

The person or institution that determines the purpose and means for processing personal information should ensure that the information is complete, not misleading, up-to-date and accurate.

Principle 5: Openness

Where personal information of a data subject is collected, the person or institution responsible for such collection must ensure that the data subject is aware of–

- the fact that the information is being collected;
- the name and address of the person or institution collecting the information;
- whether or not the supply of the information by that data subject is voluntary or mandatory and the consequences of failure to reply; and
- the particular law to which the collection is subject, when the collection of information is authorised or required under any law.

Principle 6: Security safeguards

The POPI Bill requires the implementation of technical and organisational measures to secure the integrity of personal information and to guard against the risk of loss, damage or destruction of personal information.

Any person holding personal information must protect that information against any unauthorised or unlawful access or processing.

Principle 7: Individual participation

A data subject is entitled to the particulars of his or her personal information held by any institution or person, as well as to the identity of any person that had access to his or her personal information. The data subject is also entitled to require the correction of any information held by another party.

Principle 8: Accountability

The party or institution that holds personal information must give effect to the principles for the protection of personal information as set out under the POPI Bill.

Despite the principles set out above, the Commission may authorise the processing of personal information when it will be in the public interest or when there is a clear benefit for the people concerned.

The 'public interest' includes
- the interests of State security;
- the prevention, detection and prosecution of criminal offences;
- important economic and financial interests of the State and other public bodies; or
- scientific research and government statistics.

Trans-border information flows

It is interesting to note that the POPI Bill not only regulates information held in South Africa, but also seeks to regulate the transfer of personal information to parties outside South Africa.

No person may transfer personal information 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 personal information as set out in the POPI Bill;
- 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.

Exclusions

The POPI Bill does not affect the processing of personal information
- in the course of a purely personal or household activity;
- that has been deleted to the extent that it cannot be recovered;
- by or for the State if it involves national security, defence, public safety or the prevention of crime;
- for exclusively journalistic purposes by media companies that are subject to a code of ethics that has safeguards for the protection of personal information;
- by Cabinet, Provincial Executive Councils and Municipal Councils;
- if it relates to the exercise of judicial functions;
- if it has been specifically exempted; or
- in cases where other legislation regulates the processing of that information.

While some provisions of the POPI Bill may have little application to the corporate world, it nonetheless regulates the processing of all personal information that takes place in South Africa.

Conditions for lawful processing of personal information

The processing of personal information by a responsible party must comply strictly with the eight core processing principles.

Of these eight core principles, the following five provisions stand out and should be complied with by a responsible party at all times:
- The responsible party must obtain prior approval to process personal information directly from the data subject;

- The information must be obtained directly from the data subject;
- The responsible party must ensure that the personal information obtained is accurate and, on a regular basis, give the data subject an opportunity to rectify any inaccuracies;
- The responsible person must safeguard the personal information and ensure that it does not fall into the wrong hands; and
- The information may only be used for as long as the purpose for which it was collected exists. Once this purpose expires, the information must be destroyed.

Direct marketing

In line with a person's right to privacy, the POPI Bill will strictly control how one can engage in a direct marketing activity.

The POPI Bill provides that you cannot process personal information for the purposes of using it in direct marketing unless–

- the data subject is a customer of yours and the direct marketing is in respect of similar products or services which the responsible party has previously sold to the data subject;
- the data subject has given the responsible party express permission to use his or her personal information for the purposes of direct marketing; or
- the data subject is it at all times given the option to opt-out of such communication.

All such communications sent to the data subject must feature the sender's identity and contact details.

As POPI is currently a Bill. It still needs to be passed into law before any entity has to comply with its provisions. However, it remains very important to be aware of its provisions to prepare for when it is eventually signed into law and comes into force.

WHAT HAPPENS IF YOU DO NOT COMPLY?

Investigation and compliance order

Any person who is affected by non-compliance of any of the provisions of the POPI Bill will be known as the complainant. The complainant may submit a complaint to the Regulator in writing, detailing the acts of non-compliance pertaining to the information processing principles. If the Regulator finds the complaint to be valid, an investigation will be conducted.

There are certain instances in which a Regulator may decide not to take action. Some of these instances are–

- if the subject matter of the complaint is trivial;
- if a long period of time has elapsed;
- if a complaint is frivolous, vexatious or is not made in good faith; or
- if the person making the complaint has failed to use a complaints procedure under a code.

The Regulator may try to reach a settlement between the parties, or it can conduct a hearing at which it can summon witnesses and receive evidence. The Regulator can even ask a judge or magistrate for a warrant to enter and search premises. If the Regulator grants an order in favour of the complainant, it may serve a responsible party with an enforcement notice requiring it to take certain steps.

There is a right of appeal to the High Court.

Damages in the civil courts

A data subject or the Regulator, at the request of a data subject, may also institute a civil action for damages against a responsible party for a breach of any provision of the POPI Bill relating to interference with the protection of personal information of a data subject. It does not matter whether or not there was intent or negligence on the part of the responsible party.

Offences and penalties

A breach of the provisions of the POPI Bill may result in various criminal offences.

Any person convicted of an offence in terms of the POPI Bill may be liable to a fine or to imprisonment. The term of imprisonment will vary and will depend on the provision that was contravened.

Administrative fines

A failure to comply with a compliance notice and/or order issued by the Regulator in the case where the POPI Bill is not being complied with could result in the transgressor being slapped with an administrative fine of up to R10 million.

RECOMMENDED ACTIONS OR CONTROLS WHICH SHOULD BE IMPLEMENTED BY THE TARGET AUDIENCE TO ENSURE COMPLIANCE WITH THE BILL

To ensure compliance with the provisions of the POPI Bill, the following actions should be considered:

- Conduct training and awareness of the POPI Bill and its information principles;
- Correct the processing and retention of information in line with the provisions of the POPI Bill;
- Ensure that information is used for the purpose for which it was collected;

- Create awareness around the restrictions relating to direct marketing; and
- Create awareness around the restrictions on sending information across borders.

FURTHER INFORMATION

Regulator

The POPI Bill creates an 'Information Regulator', a supervisory body that will consist of a chairperson and four others members. The Regulator will be independent and subject only to the Constitution, and he or she will be responsible for promoting, monitoring and enforcing compliance with the provisions of the POPI Bill on a national level.

The Regulator will also have the power to investigate complaints and to draft or approve category-specific or industry-specific codes of conduct. Once a code of conduct has been created, it will regulate the processing of information within that category or industry. A failure to comply with a code will be deemed to be a breach of the conditions for the lawful processing of personal information.