TENSHO®
Securing Progress

The basis of the POPI Act

The basis of the POPI Act is that organisations need to conduct themselves responsibly - responsible corporate citizenship. Organisations should not only be responsible but should be seen to be responsible corporate citizens. Part of this responsibility is to protect the information inside the organisation and to be responsible when it comes to the process of storing and sharing personal information. Personal information is to be seen as precious goods and the act requires organisations to exercise control over these precious goods.

What constitutes personal information under the POPI act?

- Identity or passport number
- Date of birth and age
- Phone numbers
- Email address
- Online messaging identities
- Physical address
- Gender, race and ethnic origin
- Photos, voice recordings, video footage
- Marital relationship and family relations
- Criminal record
- Private correspondence
- Religious or philosophical beliefs including personal and political opinions
- Employment history and salary information
- Financial information
- Education information
- Physical and mental health information including medical history
- Membership of organisations

The impact of technology on protecting personal information

Due to technology convergence, there is an increased opportunity for attacks. Everyone with a cellphone, iPad or laptop is an aider and abettor to cybercriminals. Every device offers a hacker an opportunity to get into personal information. Social media sites like Facebook and LinkedIn also serve as a bank of personal information, which, in criminal hands, can cause serious harm to both individuals and organisations. Every person must protect him or herself, and the POPI Act cannot protect one if one doesn't care to protect oneself.

How does the act apply?

The act also applies to other than a natural person; it, therefore, includes companies or any other legally recognised organisation. All organisations are seen as data subjects and are afforded the same right of protection. The Act applies to anyone who keeps any type of records relating to the personal information of anyone unless those records are subject to other legislation which protects such information more stringently. It, therefore, sets the minimum standards for the protection of personal information. It regulates the "processing" of personal information. "Processing" includes collecting, receiving, recording, organising, retrieving, or using such information; or disseminating, distributing or making such personal information available. The Act will also relate to records which you already have in your possession.

POPI as a universal application

Most countries have a POPI Act and South Africa's POPI Act is based on UK legislation. Ignorance of the law is no excuse and companies need to update IT systems and start training and educating staff since early action is essential.

When will it come into force?

The Act came into effect on 1 July 2020. Companies had 12 months to comply with the conditions of the act. The act became enforceable on the 1st of July 2021.

What are your rights?

We all have the right to be told if someone is collecting our personal information, or if our personal information has been accessed by an unauthorised person. We have the right to access our personal information. We also have the right to require our personal information to be corrected or destroyed or to object to our personal information being processed.

The Act does not apply to personal information processed in the course of a personal or household activity, or where the processing authority is a public body involved in national security, defense, public safety, anti-money laundering, or the Cabinet or Executive Council of the province or as part of a judicial function.

Personal information can only be processed:

- with the consent of the "data subject"; or
- if it is necessary for the conclusion or performance of a contract to which the "data subject" is a party; or
- it is required by law; or
- it protects a legitimate interest of the "data subject"; or
- it is necessary to pursue your legitimate interests or the interest of a third party to whom the information is supplied.

We all have the right to object to having our personal information processed. We can withdraw our consent, or we can object if we can show legitimate grounds for our objection.

A Responsible Party has to collect personal information directly from the "data subject", unless:

- This information is contained in some public record or has been deliberately published by the data subject.
- collecting the information from another source does not prejudice the subject;
- it is necessary for some public purpose, or to protect your interests;
- obtaining the information directly from the subject would prejudice a lawful purpose or is not reasonably possible.

You can only collect personal information for a specific, explicitly defined and lawful purpose and the subject must be aware of the purpose for which the information is being collected.

Once the personal information is no longer needed for the specific purpose, it must be disposed of (the subject must be "de-identified"), unless you need to keep it (or are allowed to keep it) by law, or you need to keep the record for your lawful purpose or by the contract between yourself and the subject, or the subject has consented to you keeping the records.

You are entitled to keep records of personal information for historical, statistical or research purposes if you have established safeguards to prevent the records from being used for any other purposes.

Records must be destroyed in a way that prevents them from being reconstructed.
You can only use personal information that you have collected for the purpose which you collected it for.

When information is being collected, subjects must be made aware of:

- the information that is being collected and if the information is not being collected from the subject,
- the subject must be made aware of the source from which the information is being collected;
- the name and address of the person/organisation collecting the information;
- the purpose of the collection of information; whether the supply of the information by the subject is voluntary or mandatory;
- the consequences of failure to provide the information; whether the information is being collected under any law;
- If it is intended for the information to leave the country and what level of protection will be afforded to the information after it has left South Africa?
- who will be receiving the information;
- that the subject has access to the information and the right to rectify any details;
- that the subject has the right to object to the information being processed (if such right exists);
- that the subject has the right to complain to the Information Regulator. The contact details of the Information Regulator must also be supplied.

These requirements have to be met before the information is collected directly from the subject, or soon as reasonably practicable thereafter if the information is not collected directly from the subject

unless the subject is already aware of these rights. If you collect additional information from a subject for a different purpose, you have to go through this process again.

It is not necessary to meet these requirements if the subject has consented to non-compliance or if, by non-compliance, the rights of the subject would not be prejudiced, or if by compliance you would prejudice some public interest, or if the information is only going to be used for historical statistical research purposes, or if the subject is not going to be identified.

If we collect personal information how must we handle it?

Anybody who keeps personal information has to take steps to prevent the loss, damage, and unauthorised destruction of personal information. They also have to prevent unlawful access to or unlawful processing of this personal information.

We have to identify all risks and then establish and maintain safeguards against these identified risks. We have to regularly verify that the safeguards are being effectively implemented and update the safeguards in response to new risks or identified deficiencies in existing safeguards.

Anybody processing personal information on behalf of an employer must have the necessary authorisation from the employer to do so. They must also treat the personal information as confidential.

Such a person must have a written contract with their employer in which they are specifically obliged to maintain the integrity and confidentiality of the personal information and to implement the established safeguards against identified risks.

This employee is also obliged to notify their employer if they believe that personal information has fallen into the wrong hands.

If there has been a breach and personal information has been accessed or acquired by any unauthorised people you need to notify the Information Regulator, and the subject (if you still know who the subject was). The notification to the subject needs to provide sufficient information to allow the subject to protect themselves against the possible consequences of the personal information falling into the wrong hands.

We all have the right to enquire as to whether somebody has our personal information, all we have to do is provide proof of identity and this information must be provided free of charge. We can also find out what this information consists of and if this information has been disseminated to any third parties. For these last bits of information, however, we might have to pay a fee. Access to this information is also subject to the Promotion of Access to Information Act.

We all have the right to have our personal information corrected or deleted if it is inaccurate, irrelevant, excessive, dated or misleading, if it has been obtained unlawfully, or if the responsible party is no longer authorised to retain the information.

The Act creates a special category of personal information called “special personal information”. This relates to religious or philosophical beliefs, race or ethnic origin, trade union membership, political

persuasion, health or sex life or biometric information. Also included in this category is information relating to the alleged commission of any offence or any proceedings in respect of any offence allegedly committed and the outcome of such proceedings.

You are not allowed to process this special personal information unless it is done with consent; is necessary for law; is done for historical, statistical or research purposes; or the information has been deliberately made public by the subject.

There are also limited exceptions to the prohibition against the processing of "special personal information".

These relate to situations when this information is specifically relevant and constitutes the purpose for which the information is being collected, for example for BEE or insurance.

Special rules apply to the processing of the personal information of children.

The prohibition on processing the personal information of children does not apply if the processing is:

- carried out with the prior consent of a competent person;
- necessary for the establishment, exercise or defence of a right or obligation in law;
- necessary to comply with an obligation of international public law;
- for historical, statistical or research purposes to the extent that-
- the purpose serves a public interest and the processing is necessary for the purpose concerned; or
- it appears to be impossible or would involve a disproportionate effort to ask for consent,
- and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- of personal information which has deliberately been made public by the child with the consent of a competent person.

The Regulator may upon application by a responsible party and by notice in the Gazette, authorise a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.

The Regulator may impose reasonable conditions in respect of any authorisation, including conditions concerning how a responsible party must:

- upon request of a competent person provide a reasonable means for that person to-
- review the personal information processed; and
- refuse to permit its further processing;
- provide notice regarding the nature of the personal information of children that is processed;
- how such information is processed; and
- regarding any further processing practices;

- refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and
- establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

The Information Regulator has the power to grant exemptions to allow people to process personal information without complying with the Act if the public interest outweighs the subject's rights of privacy or where there is a clear benefit to the subject. Such exemptions may be granted upon conditions.

Exemptions may also be granted for the processing of personal information to discharge a "relevant function". A relevant function would include the processing of personal information to protect members of the public against:

- financial loss due to dishonesty of persons in the banking or financial services industry;
- and dishonesty by persons authorised to carry on any profession or other activity.

Offences, penalties and administrative fees

- Any person who hinders obstructs or unlawfully influences the Regulator;
- A responsible party which fails to comply with an enforcement notice;
- Offences by witnesses, for example, lying under oath or failing to attend hearings;
- Unlawful Acts by the responsible party in connection with account numbers;
- Unlawful Acts by third parties in connection with the account number.

For the abovementioned offences, the maximum penalties are a fine or imprisonment for a period not exceeding 10 years or both a fine and such imprisonment. For the less serious offences, for example, hindering an official in the execution of a search and seizure warrant the maximum penalty would be a fine or imprisonment for a period not exceeding 12 months, or both a fine and such imprisonment.

- FIN-