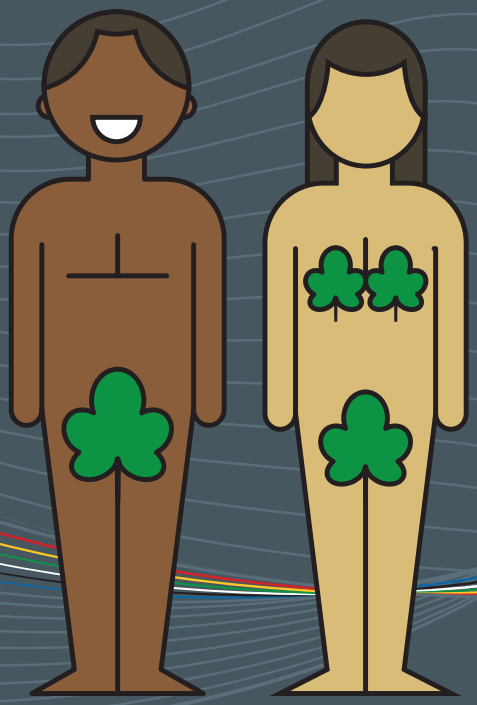

PROTECTION OF PERSONAL INFORMATION

Pamela Stein and Candice Meyer

2015 / 2016

WEBBER WENTZEL
in alliance with > Linklaters

PROTECTION OF PERSONAL INFORMATION

Pamela Stein and Candice Meyer

Introduction

After eight years of deliberations and numerous reviews, South Africa's first comprehensive data protection law, the Protection of Personal Information Act (POPI), was assented to on 19 November 2013 and its date of commencement is to be proclaimed. Organisations have a transitional period of one year from the commencement date to ensure compliance with POPI before its provisions take effect.

Application of POPI

POPI applies to every person ("person" includes natural and juristic persons), known as the "responsible party", who processes the personal information of another, known as the "data subject", where the responsible party is domiciled in South Africa. If the responsible party is not domiciled in South Africa, but makes use of automated or non-automated means for the processing of personal information in South Africa, then it must also comply with the provisions of POPI.

POPI applies to all processing of information in the private and public sectors, with limited exclusions including processing:

- in the course of household or personal activity;
- of personal information that has been de-identified and which cannot be re-identified;
- by public bodies involved in crime prevention, national security, cabinet meetings, and where judicial functions are exercised;
- of personal information which takes place solely for the purpose of journalistic, literary or artistic expression where the responsible party who processes such personal information is subject to a code of ethics that provides adequate safeguards for the protection of personal information; and
- of personal information in South Africa by non-resident responsible parties, only for the purposes of forwarding personal information through South Africa.

Key Definitions

Personal information

"Personal information" is widely defined. It includes information that relates to an identifiable person's (the data subject's):

- name, if the name would reveal information about the data subject;
- physical, mental, spiritual, economic, cultural or social identity;
- health, educational or financial history;
- identifying numbers and addresses including biometric information; and
- personal opinions and private or confidential correspondence.

The views of others about the data subject are also considered to be "personal information". To ensure that POPI is technologically relevant and following the European Union Draft Regulation on Data Protection (the EU Draft Regulation) proposal, the definition includes location information, online identifiers or any other particular assignments of the data subject.

Responsible party

"Responsible party" means the public or private body which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

Data subject

"Data subject" means the person to whom personal information relates.

Special personal information

"Special personal information" is a category of personal information. Its processing is regulated separately under POPI because of the nature of the information. The definition covers a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sexual life, biometric information, and criminal behaviour.

Processing

"Processing" covers every action concerning the personal information, from its collection to its destruction and irrespective of whether this takes place by automatic or non-automatic means.

Operator

"Operator" means the person who processes personal information for a responsible party in terms of a contract or mandate, and who does not come under the direct authority of that party. Under POPI, operators are held to the same security standards as the responsible party.

Information officer

"Information officer" means the chief executive officer or equivalent officer, or any person duly authorised by that officer. Every responsible party must appoint an information officer to ensure compliance by the responsible party with the provisions of POPI. The officer must be registered with the Information Regulator (the Regulator).

Making POPI accessible

It is the drafters' intention to make POPI as accessible as possible to those who will be affected by its provisions. In keeping with this approach, a comprehensive list of the requirements for lawful processing of personal information is located early in the legislation (Section 4), with convenient cross-references to the sections where these requirements are amplified. It also contains a list of the data subject's rights (Section 5), again with useful cross-references to the sections of POPI that give these rights substantive content.

Conditions for Lawful Processing

At the heart of POPI is the principle that all processing of personal information must comply with eight data protection principles. Failure to do so will render the processing unlawful.

Condition 1: Accountability

In an attempt to encourage data protection by design, and following the approach adopted by the EU Draft Regulation, this condition requires the responsible party to ensure compliance with all the conditions for lawful processing. This must be done when determining the purpose and the means of the processing, as well as during the processing of the data itself.

Condition 2: Processing limitation

Under this condition, processing may only take place if one of the following circumstances exists:

- the data subject consents to the processing;
- the processing is necessary to conclude or perform a contract to which the data subject is a party;
- the processing is necessary for compliance with an obligation imposed by law on the responsible party;
- the processing protects a legitimate interest of the data subject;
- the processing is necessary to pursue the legitimate interests of the responsible party or a third party to whom the information is supplied; or
- the processing is necessary for the proper performance of the public law duty by a public body.

Personal information must be collected from the data subject unless a justification to collect from elsewhere exists. Besides national security and crime prevention, other exceptions to this rule include circumstances where:

- consent of the data subject to collect from elsewhere has been obtained;
- the data is contained in a public record or has been deliberately made public by the data subject;
- the collection from another source would not prejudice the legitimate interest of the data subject;
- compliance with the condition would prejudice a lawful purpose of the collection; or
- compliance would not be reasonably practical in the circumstances.

Condition 3: Purpose specification

POPI gives effect to the purpose specification condition by requiring that the collection must be for an explicitly defined lawful purpose related to a function or activity of the responsible party.

Unless there are exceptional circumstances, personal information may only be retained for as long as it is necessary to achieve the purpose for which it was collected. The exceptions to this recognise the retention of data for historical, statistical and research, and contractual purposes and that other legislation may require the retention of the record for longer periods of time. Under this condition, personal information must be de-identified, destroyed or deleted after the responsible party is no longer authorised to retain the record.

POPI has adopted the approach of Article 17 of the EU Draft Regulation by giving the data subject the right to be "forgotten" in an online environment. This is achieved by granting the data subject the right to have his or her personal information erased by the responsible party.

This condition also includes an obligation on the responsible party to, in certain circumstances, restrict the processing of personal information for a period of time. For example where a data subject challenges the accuracy of the data, during the period of time that the responsible party attempts to verify the data, the responsible party may not process the personal information except for storage purposes or for the purposes of proof, unless the data subject consents.

Condition 4: Further processing limitation

Further processing of personal information may only take place where it is compatible with the purpose for which the data was collected, unless a data subject has consented.

In assessing compatibility, the following considerations are relevant:

- the relationship between the intended further processing purpose and the purpose for which the information was originally collected;
- the nature of the data;
- the consequences of further processing for the data subject;
- the manner in which the information was collected; and
- the contractual rights and obligations of the parties.

There are a number of exceptions to this condition, primarily relating to public bodies and their obligations, and the public interest.

Condition 5: Information quality

A responsible party is required to take practical steps to ensure that the personal information held is complete, accurate, not misleading and updated.

Condition 6: Openness

The responsible party is required to maintain documentation of all processing operations under its control. This condition follows the approach in Article 14 of the EU Draft Regulation. It requires that the responsible party, at the time of collection of the personal information, offers full disclosure of the following details:

- the full details of the responsible party;
- where information will be collected from, if not from the data subject;
- the purpose for which the information is being collected;
- whether the supply of information is voluntary or mandatory;
- the consequences of failure to provide information;
- whether any law authorising the collection of information exists;
- whether the responsible party intends to transfer the information to another country, and what level of data protection the destination country or organisation has in place;
- who the recipients of the information will be;
- the existence of the data subject's right to access, object and correct the information held; and
- whether the data subject has the right to complain to the Regulator if necessary.

Non-compliance is only condoned where:

- the data subject consents;
- if there is no prejudice to the data subject's legitimate interests;
- a criminal investigation and prosecution or maintenance of the law by a public body would be prejudiced;
- it is necessary for conduct of proceedings in court or a tribunal;
- data is collected in compliance with an obligation imposed by law or for enforcement of legislation regarding the collection of revenue;
- it is in the interests of national security;
- compliance would prejudice a lawful purpose of collection;
- where compliance is not reasonably practicable; or
- the data subject will be de-identified or used for historical, statistical or research purposes.

Condition 7: Security safeguards

This condition requires a responsible party to secure the integrity and confidentiality of personal information in its possession by taking appropriate, reasonable, technical and organisational measures to prevent the loss, damage, unauthorised destruction or unlawful access to the personal information it holds.

An operator or anyone processing personal information on behalf of the responsible party is bound by confidentiality, and may not disclose the personal information it is processing.

An operator may only process personal information on behalf of a responsible party with the knowledge or authorisation of the responsible party. The processing of personal information by an operator must be governed by a written contract, which must ensure that the operator maintains the same level of security safeguards that the responsible party is held to under POPI.

POPI has adopted Article 31 of the EU Draft Regulation, which requires a responsible party to notify the Regulator and the data subject of any security breach, unless this is prejudicial from a law enforcement perspective. Section 22 of POPI sets out the way in which notification must take place and includes the type of information that must be contained in the notification. The aim of this notification is primarily to allow the data subject to take protective measures against the potential consequences of the security compromise.

Condition 8: Data subject participation

In terms of this condition, a responsible party is required to provide the data subject with access to the personal information held on his or her behalf. The data subject is entitled to correct the personal information, request its destruction, or require the responsible party to provide credible evidence in support of the information.

A responsible party may or must refuse to disclose any information to the data subject, where such disclosure would be prohibited under Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act, No. 2 of 2000. These grounds of refusal include the protection of the privacy of a third party, the protection of confidential information or the protection of the safety of individuals.

Special Personal Information

POPI prohibits the processing of special personal information, unless the processing is permitted in one of the exceptions set out in Sections 27 to 33.

These exceptions cover circumstances where the data subject consents to the processing or the responsible party is required to comply with an obligation in law. Processing is also authorised where the data subject is a member of a trade union, religious organisation or political party.

Processing of personal information concerning the data subject's health or sex life for the purposes of medical or healthcare is permitted. Processing of information on a data subject's criminal behaviour or biometric information is permitted by bodies which are responsible for applying criminal law, or where responsible parties have obtained this information in accordance with the law. The Regulator may also, on application, grant specific authorisation for the processing of special personal information.

Children's Personal Information

POPI prohibits the processing of any personal information of a child, unless the processing falls into one of the specified exceptions. A "child" is defined as a person under the age of 18 years.

Processing of children's information can only take place if:

- a competent person gives prior consent to such processing;
- it is necessary for the establishment, exercise or defense of a right or obligation in law;
- it is necessary to comply with an obligation of international public law;
- it is necessary for historical, statistical or research purposes which are in the public interest and to obtain consent would be too onerous, provided that sufficient guarantees are in place to ensure that the child's privacy is not disproportionately adversely affected;
- the personal information of the child has deliberately been made public by the child with the consent of a competent person; or
- the Regulator grants permission for such processing where it is the public interest and sufficient safeguards are in place to protect the personal information of the child.

Cross-Border Information Flow

The transfer of personal information to a third party in a foreign country is lawful, only in the following circumstances:

- where the data subject has consented to such transfer;
- where the recipient of the information is subject to a law, binding corporate rules or binding agreement that provides an adequate level of data protection;
- if the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- if the transfer is necessary for the conclusion or performance of a contract concluded between the data subject and the responsible party in the interest of the data subject; or
- if the transfer is for the benefit of the data subject who cannot reasonably be reached to give consent, and, if the data subject were to be reached, consent would be given.

Information Officer

Every public and private body is required to appoint an information officer, or deputy information officers. These officers may only take up their duties after the responsible party has registered them with the Regulator.

In private bodies, the chief executive officer or equivalent officer is automatically designated as the information officer of that organisation. In public bodies, the information officer is the same officer who is the incumbent in the post as set out in Schedule 1 or 3 of the Public Service Act, No. 103 of 1994. Both public and private bodies may appoint deputy information officers, and delegate powers to them.

Information officers are responsible for:

- encouraging and ensuring compliance with the conditions for lawful processing in their organisations;
- dealing with subject access requests under POPI;
- working with the Regulator on investigations in relation to that body; and
- ensuring compliance with POPI.

Direct Marketing

A direct marketer has one opportunity to obtain consent from a data subject for processing the data subject's personal information for direct marketing.

Where the data subject is an existing customer of the responsible party, the responsible party may process the personal information of that data subject to market similar products or services to him or her. The data subject must, however, be given a reasonable opportunity to object to the direct marketing, both at the time the data subject's personal information is collected and on each subsequent occasion the responsible party sends marketing material to the data subject.

The Regulator

The Regulator is an independent statutory authority established under POPI and is accountable to and funded primarily by Parliament. It consists of a full-time chairperson and four other members, two of whom must be appointed on a full-time basis.

The Regulator must appoint suitably qualified staff including a chief executive officer to assist in the performance of its duties.

The Regulator's tasks include:

- educating the public on POPI;
- monitoring the implementation of POPI in public and private bodies;
- enforcing compliance with the provisions of POPI;
- undertaking regular consultation on the protection of personal information with interested parties, both nationally and internationally;
- processing complaints about violations of POPI;
- attempting to resolve such complaints, including through mediation;
- conducting research and reporting to Parliament on local and international developments in the protection of personal information;
- issuing codes of conduct and guidelines to assist in the implementation of POPI;
- facilitating cross-border cooperation in the enforcement of privacy laws; and
- carrying out any other functions and duties imposed on it under POPI.

The Regulator is given wide powers to carry out its functions, including search and seizure powers and the power to compel evidence under oath.

Compliance and Sanctions

The Regulator must investigate complaints lodged concerning:

- any breaches of the conditions for lawful processing;
- non-compliance with the requirements of notification of security compromises;
- breaches of the direct marketing, directories and automated decision-making provisions of POPI; and
- breaches of the provisions governing the transfers of personal information outside the Republic.

The Regulator must attempt to settle the complaints between the parties concerned, if this is possible. Once a complaint has been investigated, the Regulator may refer it to an enforcement committee who will hear both parties, consider the complaint and make recommendations.

The Regulator can then, after considering the recommendation of the enforcement committee, issue an enforcement notice compelling the responsible party to take certain steps or to stop processing the personal information.

An appeal against an enforcement notice can be made to the High Court. A responsible party may pay an administrative fine of up to ZAR 10 million for failure to comply with an enforcement notice or elect to be prosecuted in a criminal court and subjected to a fine and/or imprisonment of up to a maximum of 10 years.

Civil Remedies

A data subject or the Regulator may bring a civil action for damages against a responsible party for a breach of the various provisions of POPI. In such a claim, POPI imposes strict liability (or no fault-based liability) on the responsible party. There is also potential to claim against a responsible party for aggravated damages in the event of a breach.

A court determining a claim for civil damages under POPI must also issue an order that the courts findings be published in the media.

Transitional Arrangements

All processing of personal information must conform to the provisions of POPI, within one year after the commencement of the legislation. This period may be extended by ministerial intervention.

Conclusion

When POPI comes into effect, South Africa's data protection law will be in line with that of its major trading partners. The provisions of POPI allow for protection of all data subjects and regulation of all data processors with minimal exceptions and exclusions. Non-compliance with the provisions in POPI may be punishable by a fine, criminal prosecution and/or imprisonment.