DYKES VAN HEERDEN
ATTORNEYS AND CONVEYANCERS

30 JUNE 2020

POPI: PROTECTION OF PERSONAL INFORMATION ACT

Introduction and history

POPI promotes the protection of personal information by public and private bodies.

POPI was signed into law by the President on 19 November 2013 and published in the Government Gazette on 26 November 2013.

The President signed a proclamation declaring certain provisions of POPI into effect from 11 April 2014. They included part A of Chapter 5 of the Act which provides for establishment of the Information Regulator. The other sections allow for making of regulations where they are required in the Act. These sections created the framework within which the Act will operate once fully in force.

The National Assembly approved the appointment of the members to the Information Regulator on 7 September 2016 and on 1 December 2016 the Information Regulator was appointed.

Now more than 6 years since the proclamation of the Act and 3 and half years after appointment of the Information Regulator, the remaining provisions (save for two) are operational as from 1 July 2020.

Application of the Act

POPI will apply to any institution, entity or body that processes and stores personal information, such as legal practices in general, insurance companies, schools, hospitals, debt counsellors, HOA, banks and estate agents.

Purpose of the Act

The purpose of the POPI is to give effect to the constitutional right to privacy. The Act intends to achieve a balance between the right of privacy and the right to information.

The Act intends to achieves its purpose by safeguarding personal information processed by public and private bodies.

Responsible person and the Data subject

- **Processing**

Processing is defined in the Act to include the collection, receipt, storage, recording, organisation, collation, updating or modification, usage, retrieval, retention and destruction of personal information.

- **Personal information**

Personal information is defined very broadly as an identifiable, living, natural person's information and, where applicable, an identifiable, existing juristic person's information, including:

- Any indentifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- The name of the person as it appears with other personal information relating to that person or if disclosure of the name itself would reveal information about the person;
- Information relating to the race, gender, sex, pregnancy, marital status, national, 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;
- Biometric information of the person;
- The personal opinions, views or preferences of the person;
- The views or opinion of another individual about the person;
- Information relating to the education or the medical, financial, criminal or employment history of the person.

Rights of data subjects (section 5)

In terms of the Act certain rights are given to "data subjects" (being the person to whom personal information relates). These rights include:

- Notification of the information being collected and for what purpose;
- Establishing what information the responsible party holds and request access to such information;
- Objection to give information;

- Request correction, destruction or deletion;
- Refuse processing for direct marketing by unsolicited electronic communications;
- Complain to the Regulator and institute civil proceedings;

Exclusions (section 6 and 7)

There are some exclusions to the application of the Act including:

- Processing in the course of purely personal or household activity;
- By a public body regarding national security;
- Investigation or proof of offenses;
- Research and statistical purposes;
- Prosecution of offenders;
- Exclusively for Journalistic purposes
- Relating to judicial functions of the court.

Requirements to be compliant - Conditions of lawful processing (section 4)

The Act provides for the establishment of minimum requirements for processing of personal information. The conditions for lawful processing include:

1. Accountability;
2. Processing limitations (consent);
3. Specific purpose;
4. Further processing;
5. Information quality;
6. Openness;
7. Security safeguards;
8. Consent for direct marketing;
9. Data subject participation.

Processing limitations - Consent and within purpose (section 12)

• Information is required to be collected by the data subject with the data subject's consent. Burden of proof on responsible persons.

• Data subject may withdraw consent and may object on reasonable grounds.

•Obtain directly from data subject unless: -

- The information is contained in or derived from a public record or has deliberately been made public by the data subject;
- Processing is necessary to carry out the actions to conclude or perform a contract to which the data subject is a party to;
- Processing compliance with an obligation imposed by law;
- To protect the legitimate interest of the responsible party.

Purpose specification (section 13 and 14)

The Act prescribes that personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. Steps must be taken in order to ensure that the data subject is aware of the purpose of the collection of the information.

Personal information may not be retained any longer than necessary for achieving the purpose it was collected for or subsequently processed unless it is allowed in terms of law, contract, historical, statistical or research purposes.

Destroy or delete in a manner thar prevents its reconstruction in an intelligible form.

Further processing (section 15)

The further processing of personal information must be in accordance with the purpose for which it was collected. Various factors are considered in order to determine whether the further processing of information is compatible with the original purpose of collection.

Information quality (section 16)

The responsible party must take reasonable practical steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

Openness (section 18)

The responsible party must take reasonable practical steps to ensure that the data subject is aware of: -

1. the information being collected and the source of the collection;

2. details of the responsible party;

3. the purpose that the information is being collected;

4. whether mandatory or voluntary; and

5. consequences of not providing.

When collecting the information directly from the data subject, the above steps must be done before the information is collected.

Security safeguards (section 19)

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent –

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

In order to give effect to this, the responsible party must take reasonable measures to –

(*a*) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(*d*) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

If personal information accessed or acquired by any unauthorised person the responsible party must notify the Regulator and data subject as soon as reasonably possible.

Data subject participation (sections 23-25)

The data subject may request a responsible party to correct or delete information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

On request from the data subject the responsible party as soon as reasonably possible correct, destroy or delete the personal information.

Direct marketing

Consent is required from the data subject for the processing of personal information for the purpose of direct marketing by means of electronic communication.

Becoming compliant

The process of becoming fully compliant will be a time-consuming and costly exercise that will have a significant impact on, *inter alia*, the following:

- Legal and compliance management;
- Human resources management;
- Information governance;
- Information security;
- Records management;
- Business continuation planning;
- Third party service provider management.

A basic overview of the compliance and implementation process will include, but is not limited to, the following:

- Conducting a privacy gap analysis (also referred to as a privacy impact assessment);
- Designing or obtaining all the required data privacy and information security policy and related documentation if not already in place;
- Updating and/or aligning the policy with other related legislation, personnel policy, business continuation plans, e-mail and acceptable use policies, breach of information security events reports, protection of personal information agreements, etcetera;
- Implementation of the abovementioned policies, agreements and procedures, inclusive of relevant training and awareness interventions;

- Assignment and registration of the prescribed information officer and deputy information officers (where applicable) with the information regulator after implementation of the legislation, etcetera;

It is thus recommended that companies affected by the Act initiate the process to become compliant as soon as possible to avoid a pressurised rush for compliance against deadlines once the requirements of the new Act become effective. It is not the responsibility of any outside agency to instruct or notify any party to comply with the new legislation.

When must you comply by?

1 July 2021. There is an initial 12-month grace period ending 30 June 2021.

Penalties for non-compliance

It must be kept in mind that compliance will been enforced by an Information Regulator, which will have far-reaching powers. The legislation provides for the following penalties for non-compliance after the initial grace period:

- 12 months' to ten years' imprisonment.
- Up to R 10 million fine.
- Civil remedies.

The consequences of non-compliance with the legislation are thus severe and must be viewed from a regulatory as well as from a reputational perspective.

The above should be seen as a brief comment and should not be seen as an extensive guideline or interpretation of the Act. Please obtain a full legal opinion if you wish to act on any aspect hereof as the guideline is not fully comprehensive.

dvh Going Beyond

The DVH group is a national group of attorney practices with offices situated in the Western Cape, Gauteng, and Kwa Zulu Natal.

www.dvh.law.za or scan the QR to contact us.

This newsflash has been prepared for information purposes only and does not constitute legal advice, or a legal opinion, the practical application of the provisions of this newsflash will vary depending on the facts of each case.