Protection from Harassment Act

Jan du Toit

Not many South Africans are aware of the fact that on the 12th of April 2013 a proclamation was published in the Government Gazette, whereby Pres. Zuma set 27 April 2013 as the date on which the Protection from Harassment Act (Act no. 17 of 2011) came into operation. The purpose of this act is to provide for the issuing of protection orders against harassment and to afford victims of harassment with an effective remedy against such behaviour.

In terms of this Act harassment is defined as either directly or indirectly engaging in conduct that the harasser knows or ought to know –

(a) causes harm or inspires the reasonable belief that harm may be caused to the complainant or a related person by unreasonably-

(i) following, watching. pursuing or accosting of the complainant or a related person, or loitering outside of or near the building or place where the complainant or a related person resides, works, carries on business, studies or happens to be;

(ii) engaging in verbal, electronic or any other communication aimed at the complainant or a related person, by any means, whether or not conversation ensues; or

(iii) sending, delivering or causing the delivery of letters, telegrams, packages, facsimiles, electronic mail or other objects to the complainant or a related person or leaving them where they will be found by, given to or brought to the attention of, the complainant or a related person; or

(b) amounts to sexual harassment of the complainant or a related person.

The word *"harm"* I defined as any mental, psychological, physical or economic harm.

Sexual harassment is defined as any:

(a) unwelcome sexual attention from a person who knows or ought reasonably to know that such attention is unwelcome:

(b) unwelcome explicit or implicit behaviour, suggestions, messages or remarks of a sexual nature that have the effect of offending, intimidating or humiliating the complainant or a related person in circumstances, which a reasonable person having regard to all the circumstances would have anticipated that the complainant or related person would be offended, humiliated or intimidated;

(c) implied or expressed promise of reward for complying with a sexually oriented request; or

(d) implied or expressed threat of reprisal or actual reprisal for refusal to comply with a sexually oriented request;

In terms of the Employment Equity Act the harassment of an employee is a form of unfair discrimination and is prohibited on any one, or a combination of grounds of unfair discrimination. Section 10(6) of the EEA provides remedies for victims of *inter alia* sexual harassment in the workplace.

Employers and employees should therefore take note provisions of this act since it could have far-reaching implications in the workplace. As a result of the Protection from Harassment Act it will now be possible for an employee to obtain, in addition to the provisions of the EEA, a protection order against an abusive employer or colleague.

In terms of section 2 of the act a complainant may apply to a magistrates' court for a protection order be issued against a harasser. The court must as soon as is reasonably possible consider such an application submitted to it.

If the court is satisfied that there is *prima facie* evidence that –

(a) the respondent (harasser) is engaging or has engaged in harassment;

(b) harm is being or may be suffered by the complainant or a related person as a result of that conduct if a protection order is not issued immediately; and

(c) the protection to be accorded by the interim protection order is likely not to be achieved if prior notice of the application is given to the respondent the court must, notwithstanding the fact that the respondent has not been given notice of the proceedings, issue an interim protection order against the respondent.

After the issuing of the interim order, there will be an opportunity at a later stage for the respondent to defend him or her before a final order is made. Such an order is made on the balance of probabilities that the respondent has engaged or is engaging in harassment. Such an order, including an interim protection order, may prohibit the respondent from –

(a) engaging in or attempting to engage in harassment;

(b) enlisting the help of another person to engage in harassment; or

(c) committing any other act as specified in the protection order.

The court may also impose any additional conditions on the respondent which it deems reasonably necessary to protect and provide for the safety or well-being of the complainant. It is important to note that an "additional condition" may well be an order that the harasser may not be within a specific radius of the complainant.

Whenever a court issues a protection order, including an interim protection order, the court must make an order –

(a) authorising the issue of a warrant for the arrest of the respondent, in the prescribed form; and

(b) suspending the execution of that warrant subject to compliance with any prohibition, condition, obligation or order imposed.

This means that the harasser may be "automatically" arrested without further proceedings if he / she fails to adhere to the requirements of such an order and may face prison time for up to five years.

Complainants must however take note that making false statements to a Magistrates' Court may be on conviction fined or imprisoned for a period not exceeding five years.

Going forward employers may face some difficult situations in the workplace as a result of a protection order that was for instances issued in the favour of an employee against his / her supervisor, or another

employee. Employers are advised to introduce harassment policies and awareness campaigns in the workplace and to deal with complaints in a swift but fair manner.

Jan du Toit can assist employers with IR and HR related services and can be contacted for a consultation at .

The Protection of Personal Information

By Jan du Toit, Senior Consultant, SA Labour Guide

After more than seven years in the making, President Ramaphosa announced last year an effective date of 1 July 2020 for the Protection of Personal Information Act (POPI), Act 4 of 2013. "Responsible Parties" only have approximately 5 months left until 30 June 2021 to become compliant in full.

The duration of a typical POPI compliance project will differ from one business to another depending on the nature and size of the business, as well as the Personal Information processed by a Responsible Party. Business owners are therefore advised to, without delay, embark on a compliance project to meet the deadline.

Even though the Protection of Personal Information Act is welcomed by most, it has been long overdue and will require business owners ("Responsible Parties" in terms of the Act) to process Personal Information according to 8 processing conditions as set out in the Act.

The purpose of the Protection of Personal Information Act is in essence found in the title of the Act; to protect the Personal Information of "Data Subjects". It gives effect to ones right to privacy as enshrined in the Constitution but also provides balance in terms of the right to privacy weighed up against the right to access to information.

The Act regulates the manner in which Personal Information must be processed and provides protection and recourse to those whose rights are infringed. Further to this, the Act makes provision for the establishment of an Information Regulator. Advocate, Pansy Tlakula has already been appointed as the Information Regulator a couple of years ago and has done a great deal of work in establishing her office.

Before I get into more detail about the eight processing conditions, it is important to note that the Act is "definitions driven". It is therefore of utmost importance to first highlight some of the definitions found in the Act for readers to better understand the eight processing conditions.

The first definition is that of "Personal Information". Personal Information is widely defined in the Act and includes, but is not limited to, information relating to an identifiable living natural person or a juristic person ("Data Subjects"), such as:

- Race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, believe, culture, language, birth
- History - education, medical, financial, criminal, employment
- Identifiers – number, symbols, e-mail address, physical address, telephone numbers, location, online ID or other assignment to a person such as a unique identifier (in example a student or patient number)
- Biometric information – physical or psychological behavioural characterization, blood type, fingerprints, DNA analysis, retinal scanning, voice recognition
- Personal opinion views or preferences
- Correspondence implicitly or explicitly of a private and confidential nature
- Views or opinions of another individual\
- The name of the person with other information or the name alone

The second definition of importance is that of "processing". The processing of Personal Information includes but is not limited to any operation/activity or any set of operations, whether automated or not, concerning Personal Information. It includes:

- Collection / receipt / recording / organizing / collation / storage / updating / modification / retrieval / alteration of Personal Information
- Dissemination by means of transmission distribution or making available to others.
- Merging / linking / restricting / degradation / erasure / destruction of Personal Information.

A Responsible Party can either be a public body, private body or any other person or persons, domiciled in South Africa and that determines the purpose and means for processing of Personal Information.

Throughout the entire lifecycle of Personal Information in any business, eight processing conditions must be adhered to. The eight processing conditions are summarized below:

Condition 1 – Accountability. The Responsible Party must always ensure that the conditions set out in Chapter 3 of the Act and all the associated measures are complied with.

Condition 2 – Personal Information must be collected and processed lawfully in a reasonable manner that does not infringe the privacy of a Data Subject. The Personal Information may only be processed if it is adequate, relevant, and not excessive.
Personal Information may only be processed if the Data Subject consented thereto. Alternatively, where it is necessary to do so for the conclusion or performance of a contract, an obligation in terms of law, to protect the legitimate interest of the Data Subject, or to pursue a legitimate interest of the Responsible Party.

A further requirement is that the Personal Information must be collected directly from the Data Subject.

Condition 3 requires that Personal Information must be collected for a specific explicitly defined and lawful purpose related to a function or activity of the Responsible Party. Such Personal Information may not be retained any longer than necessary for achieving the purposes for which the information was collected and/or subsequently processed.

Condition 4 prohibits the further processing of Personal Information unless such processing is compatible with the initial purpose of collecting the information.

Condition 5 requires that Responsible Parties must take reasonable, practicable steps to ensure that Personal Information is complete, accurate, and not misleading. Such Personal Information must also be kept up to date, taking into consideration the purpose of the Personal Information.

The nature and purpose of the Personal Information will dictate as to how often such Personal Information must be updated.

Condition 6 addresses some of the rights of Data Subjects, such as the right to be informed by the Responsible Party before information is collected. The purpose of collecting and from where Personal Information will be collected must be disclosed to the Data Subject.

A Data Subject is entitled to the details of the Responsible Party and to be made aware of the consequences of not making Personal Information available to the Responsible Party.

Should it be required that Personal Information be collected and processed in terms of legislation, the Data Subject must be made aware accordingly.

As per Section 72 of the Act, the Data Subject must be advised if **Personal Information will be transferred across the borders of South Africa**. Under such circumstances the Data Subject is entitled

to first be made aware of legislation in other countries that provides adequate protection of the Personal Information. In the absence of legislation, whether there are any binding corporate rules in place, alternatively a written agreement that offers adequate protection for the Data Subject, concluded between the Responsible Party and he third party.

Condition 7 requires that Responsible Parties must secure the integrity and confidentiality of Personal Information by taking appropriate reasonable, technical and organisational measures, to prevent loss or unlawful access of Personal Information under the control of a Responsible Party.

In this regard the Responsible Party is required to identify all reasonable and foreseeable internal and external risks, and to establish and maintain appropriate safeguards. Compliance with such safeguards must be regularly audited and measures updated if so required.

Condition 8 deals with the rights of Data Subjects and participation. In terms of condition 8, Data Subjects have the right to establish whether Personal Information is held by a Responsible Party and to have it corrected or destroyed if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or have been obtained unlawfully.

Responsible Parties are also further required to introduce Data Subject rights and participation in their PAIA (Promotion of Access to Information Act) manuals.

Responsible Parties are also **not permitted to send direct marketing material to Data Subjects** without their written consent as per from 4 four of the regulations of the Act.

Other important considerations in terms of the Act are that a Responsible Party may be issued with an administrative fine of up to R10 million for its non-compliance with the Act. Additionally, Data Subjects have the right to sue Responsible Parties and under specific circumstances, the Information Officer of the Responsible Party may be imprisoned.

Each Responsible Party **must register an Information Officer** (the head of the organization or a person acting in such capacity) with the Information Regulator. The Information Officer may appoint deputies to assist with ensuring compliance within the business.

From the above, it is evident that a POPIA compliance project is not something that should be undertaken without a solid understanding of the Act.