

# POPI – WHAT DOES IT MEAN?

**What are the pitfalls and potential risks to employers?**

**What are the rights of employees?**

Written by:

Johan van der Walt

By way of the Protection of Personal Information Act (POPI), Act 4 of 2013, South Africa has been aligned with international standards as far as protection of personal information is concerned. The Act has been signed into law by the President on 19 November 2013 and published in the *Government Gazette* Notice 37067 on 26 November 2013. Certain sections of the Act, mainly relating to the office of the Regulator, came into effect on 11 April 2014. It is not yet clear at what date the remaining sections of the Act will become effective but, once it does come into effect, companies will have one year to comply with the Act's provisions, unless this period is amended by legislation.

This article is written from the perspective of an employer (referred to as a 'Responsible Party' in the Act) and an employee (referred to as a 'Data Subject' in the Act). The terms 'Responsible Party' and 'Data Subject' is however not restricted to only employers and employees.

## **What is the purpose of this Act?**

POPI will have major impact on the way in which employers and the government treat personal information collected from individuals.

The purpose of the Act is mainly to:

- Give effect to the constitutional right to privacy while protecting the free-flow of information and advancing the right of access to information;
- Regulate the manner in which personal information is processed in alignment with International Standards;
- Provide rights and remedies to individuals for non-compliance; and to
- Create measures, including the establishment of an Information Regulator, to promote and enforce the protection of personal information.

This Act affirms the right of individuals to have their personal information protected and not to have such information misused for purposes it was not originally intended for and it also provides the individual the right to take action if personal information is misused in such a way.

## **What is 'personal information'?**

Personal Information unique to a natural person or juristic person (a company for example) whereby such individual or company can be identified and includes, amongst others, the individual's name, ID number, race,



**Mondial®**

Dynamic Pragmatic Innovative

gender, biometric information (including blood type and fingerprints), age, contact details, personal history (including medical history), religion and private correspondence/ conversations. The Act describes in detail how such information should be treated as far as the collection, storage, retention, deletion or destruction thereof is concerned. Failure to comply with provisions of the Act could result in legal action and large fines.

Processing of personal information in terms of the Act refers to all actions (manual or electronic) carried out in relation to such information for example the collection, usage, storage, dissemination, modification or destruction thereof.

### **What are the pitfalls (potential areas of risk) from an employer perspective?**

#### **1. Accountability**

- An employer remains responsible for compliance with its obligations in terms of the Act as far as processing of an individual's personal information is concerned;
- This obligation is incumbent on employer even if the employer has entrusted the data collection process to an employee or a third.

#### **2. Processing**

- Personal information (broadly defined above) may only be processed if inter alia the data subject (hereinafter referred to as the 'employee' for purposes of this overview) consents to such processing and if such processing is carried out in a manner that does not infringe the rights of the employee;
- 'Data subject' in terms of the Act includes an employee, applicant for employment and former employee;
- The employee should be clear about the scope and purpose of the consent, in other words what the information will be used for. This includes for example reference checks, qualifications checks and credit checks and the intent could be for evaluation for promotion purposes;
- Collection of information must be for a specific purpose which relates to an activity of the responsible party (or employer for purposes of this overview). The employee must be aware of the purpose for which the information is being collected and the information must be retained for no longer than required for the specific purpose;
- Information may not be kept longer or processed further in a way that is not aligned with the purpose for which it was collected. If such information is required for another purpose, the employee, for example, must be consulted and his/her consent must be obtained, unless the information is in the public domain. Employers should therefore develop internal safeguards to prevent information being processed in a way contrary to the purpose for which it was originally collected.

#### **3. Quality of information**

- The onus is on the employer to ensure that the information is complete, accurate, not misleading and up to date. The employer should therefore conduct audits to assess what information is retained and the correctness thereof;
- The employee should be requested to confirm that information that is being held is complete, accurate and up to date;

- The employer should take the necessary security measures to ensure that integrity of information is maintained and that access to the information is restricted and that personal information is safeguarded against loss, destruction or unlawful access;
- The employer should finally also secure employees' consent to retention of records and ensure that employees who have access to employee records and work with these on a day to day basis are reliable.

#### **4. Openness - 'no hidden agendas'**

- The employee must be made aware of amongst others, the following:
  - that personal information is being collected;
  - the name and address of the employer; and
  - the purpose for which the information is being collected.
- The employer, when recruiting, must therefore ensure that applicants are aware of what information is required and the purpose for which it is being used and also ensure that the name and address of the employer appears on all application forms and advertisements.

#### **Rights of the employee**

- The employee can request confirmation as to whether the employer holds information about him/her and a description of the personal information held. The employer must also advise the employee that information that is being held can be corrected by the employee on request.
- The employer should therefore provide each employee with a copy of the information held relating to them, where reasonably practicable, and afford the employee the opportunity to submit requests for correction. It is advisable that employers develop procedures on reporting and handling requests for corrections.

#### **What steps should employers take to address these potential risks?**

- Conduct exit interviews and obtain consent from employees as far as providing references is concerned;
- Review application forms, adverts, interview process and amend where necessary in order to comply with the Act;
- Train employees on how to comply with the provisions of the Act. Training for relevant employees should address record keeping, collecting information, dissemination of information for example providing references to third parties;
- Conduct audits of records and retention periods in order to determine for example safeguards, access and destruction of personal information;
- Secure consent of applicants and new and existing employees to processing in terms of advertisements, application forms and contracts of employment.

***With acknowledgement to Mr Faan Coetzee, Executive Consultant, Employment at DLA Cliffe Dekker Hofmeyr, Johannesburg***

#### ***Johan van der Walt***

Johan, a director of Mondial Consultants, is a University graduate and admitted attorney with over 35 years' experience in law, corporate governance and risk management, corporate communications and project management. Before the formation of Mondial Consultants in 2008, he was employed by BHP Billiton for a period of 20 years as Risk Champion and Company Secretary in one of the company's divisions. Johan was jointly responsible for the formation of Mondial in 2008 and is a member of the company's management team responsible for the strategic direction and day to day management of the business. Apart from being responsible for a number of current Mondial clients in the risk management space he also represents Mondial as the Company Secretary for a listed JSE entity.



**Mondial®**

Dynamic Pragmatic Innovative

**Tel:** +27 861 007 662

**Fax** +27 86 564 0005

**Email** [info@mondialcons.com](mailto:info@mondialcons.com)

**Website:** [www.mondialcons.com](http://www.mondialcons.com)

**Office Address**

17 Central Office Park

257 Jean Avenue

Centurion

Gauteng

**Postal Address**

PO Box 7752

Centurion

Gauteng

0049