MASERUMULE
Corporate Employment Law

Where results matter

HERE COMES POPI

The Protection of Personal Information Act 4 of 2013 ('POPI') was assented to (signed) on 19 November 2013 and Gazetted on 26 November 2013, which means it is now law. Responsible parties (entities wanting to process personal information) are afforded a one year grace period from the date of commencement to get their house in order. The grace period could be extended once for a further period of three years, until 26 November 2017. The President has signed a proclamation declaring some parts of the POPI effective from 11 April 2014.

On 11 April 2014, the following sections of POPI took effect, namely the definitions section (section 1), Part A of Chapter V that empowers the Minister to establish an Information Regulator, the section empowering the Minister to make regulations pertaining to the establishment of the Regulator and fees that may become payable by data subjects (section 112), and the section empowering the Minister to, among others, publish draft regulations for public comment (section 113). There is still no new information on when the balance of POPI is going to commence and the Minister has not given us an indication of the timeline. The practical implication of this is that entities can commence with its POPI roll out as the definitions serve as the point of departure for evaluating all internal processes, policies and agreements. POPI's enforcement mechanisms still need to be established. According to unconfirmed reports, the Deputy Minister of Justice announced on 21 May 2015 that the process of appointing the Information Regulator has begun, which will pave the way for the commencement of POPI.

While it is very hard to plan your roadmap if you don't know what the end date is, it will be time well spent to commence with the process of readying your entity for POPI's commencement.

Common law protection is limited as it does not provide active control over data by the individual, it merely protects against abuse. POPI has proactive protection as its purpose. POPI aims to regulate the processing of personal information entered in a record by or on behalf of both private and public bodies, including the State.

'Processing' is given a wide interpretation and includes **any operation or set of operations concerning personal information**. This covers the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination, transmission, distribution, merging, linking, blocking, erasure or destruction of personal information.

'Personal information' includes:

- name, address and ID number;
- blood type and fingerprints;
- educational, medical, criminal or employment history; and
- information pertaining to financial transactions.

Personal information is further categorized into 'special' personal information, which information enjoys a higher degree of protection. Special personal information includes information about religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, DNA, sexual life or criminal behaviour of a data subject.

POPI does not want to stop the free flow of information; it only wants to impose conditions on it. Therefore, employers wanting to continue processing personal information and special personal information must obtain the employee's consent. The consent given by the employee must be voluntary, specific, and informed.

In addition to the consent requirement, POPI attaches 8 conditions for processing of personal information. These are processing limitation, specific purpose, further processing limitation, information quality, openness, security safeguards, individual participation and accountability. Employers are tasked with ensuring each condition is adhered to when processing an employee's personal information. We recommend that you map the different HR/IR activities where you process personal information. This will enable you to ensure the conditions are adhered to at each instance of processing.

Furthermore, an Information Protection Officer needs to be appointed. If you do not appoint a specific employee as your Information Protection Officer, the same person responsible for PAIA, will be automatically deemed to be your Information Protection Officer. Generally, the Information Protection Officer is tasked with ensuring compliance, including the safe-keeping of, control of access to, correction and destruction of information.

As part of your POPI due diligence exercise, we recommend employers take the following steps towards compliance:

1. **Determine the types of personal information** held [sources: contract of employment, medical aid, pension fund membership (statutory requirements)].
2. **Categorise the personal information** into personal information and special personal information.
3. **Ascertain the essential personal information** and special personal information necessary for IR and HR purposes (keep it lean).
4. You must have **a clear purpose** for collecting and holding the information.
5. **Draft a 'privacy policy'** referring to internal and external parties who have a legitimate interest in the information [i.e. pension fund, medical aid and service providers].

6. **Map** the different activities where processing of personal information and special personal information becomes necessary (recruitment, selection, appointment, promotion, training, etc.).

7. **Confirm responsible parties** for personal information and special personal information.

In closing, the following actionable points will ensure that your due diligence exercise is more than just a mere box-ticking exercise:

1. **Identify** what personal information and special personal information are processed.

2. Put adequate **security safeguards** in place to prevent unauthorised access to personal information and special personal information.

3. Draft a **Privacy Policy.**

4. Schedule **information sessions** to create awareness among employees.

5. Put an **Incident Response Policy or Plan** in place before an incident of leakage of personal information and special personal information occurs.

The possible consequences, should your organisation choose not to initiate the process of becoming compliant with POPI, are the risk of suffering reputational damage, losing customers and failure to attract new ones due to their possible awareness of the risk of a privacy breach, having to pay out millions in damages to a civil class action upon being successfully sued by an employee or a client who suffered a loss as a result of your organisation's failure to adhere to the conditions attached to lawful processing of personal information and being fined up to R10 million or face 10 years in jail. These risks of not complying with POPI are far-reaching and it is in your best interest to ensure compliance through an environment that is conducive to constructive protection to personal information, with the employee's interests at heart.

The threat to information security is as real as ever. At the same time, the legal obligations on entities to secure the integrity and confidentiality of the information they process are growing. You have been securing your information for years for business reasons. Now, POPI also requires you to do so. Information Security is a legal obligation. You cannot claim you were not aware of your obligations. A failure to comply has serious risks associated with it.

You are welcome to contact us should you require assistance for purposes of becoming compliant with the POPI. We will give you invaluable insight into how POPI impacts on HR as well as what you can do to mitigate your risk.

Author: Andrea de Jongh
Senior Associate
Maserumule Corporate Employment Law

May 2015

www.masconsulting.co.za

