MASERUMULE
Corporate Employment Law

Where results matter

IS YOUR ORGANISATION READY FOR POPI?

INTRODUCTION

The Protection of Personal Information Act 4 of 2013 ("POPI") was signed on 19 November 2013 and Gazetted on 26 November 2013, which means it is now law. POPI has significant consequences for all organisations that process the personal information of individuals or juristic persons.

A number of companies, despite the introduction of POPI, have disregarded the essential provisions which have been introduced by the aforementioned Act. It has transpired that there is a lot of uncertainty as to what is expected from companies in so far as POPI's compliance is concerned. As a result of this, not a lot has been done in practice in attempting to comply with the provisions of the Act and/or to minimize the risks that may arise as a result of failing to comply with the Act.

Consequently, in order to provide further clarity, we have decided to provide answers to the most frequently asked questions pertaining to POPI:

1) Which sections of POPI have already commenced?

- the definitions in section 1 – This section does not create any laws itself, but is necessary for other sections;

- the Information Regulator (Part A of Chapter 5) – Part A deals with the establishment, staffing, powers and meetings of the Information Regulator;

- Regulations (Section 112) – the Minister and the Information Regulator have the power to make regulations; and

- the procedure for making regulations (Section 113) – the procedure for making regulations is in place. However, there are no regulations in place yet. The regulations will assist the Responsible Parties with interpreting what is expected from them in terms of POPI.

2) Why should the taking of office of the Chair of the Information Regulator on 1 December 2016, and the draft Regulations released for comment on 8 September 2017 be of significance to companies?

The Information Regulator is a new regulator that has been created by POPI. POPI gives the Information Regulator extensive powers to investigate and fine Responsible Parties for non-compliance with POPI. Data subjects will be able to complain to the Information Regulator, and it will be able to take action on behalf of data subjects. More importantly at this stage the Information Regulator (five members in total) drafted the Regulations and published same. Whereas we were hoping that the regulations will provide guidance on the interpretation and application of POPI, we were disappointed. They are only five pages long (plus 26 pages of example forms). These regulations are largely administrative in nature and do not help organisations to interpret POPI or make it easier for them to comply. The Regulator is now in the process of reviewing the comments submitted to it and we are waiting for the next version of the regulations to be published. It is also anticipated that the Regulations will be promulgated, and approved before POPI's grace period lapses.

3) What is the POPI commencement date or POPI effective date for the balance of POPI?

There is no indication when the balance of POPI will commence or what the effective date will be. We are waiting for President Ramaphosa to proclaim the date. It might be towards the end of 2018 but may only be in 2019. Bear in mind that there is a one-year grace period that runs from the commencement date and companies only have to comply with POPI at the end of the grace period. Therefore, the POPI deadline might only be the end of 2019 or in 2020.

Consequently it is advisable that, despite the balance of POPI not having commenced yet, companies ensures that their HR departments comply with the balance of POPI's sections at this stage already. Specifically the eight conditions of processing. It will be

time well spent to commence with the process of readying your entity for POPI's commencement through a due diligence exercise, as companies will ultimately be required to adhere to POPI's requirements. The grace period is intended to allow Responsible Parties to get their house in order.

It is therefore important that management develops an understanding of the 8 conditions for the lawful processing of personal information and are able to apply those principles to the processing of employees' personal information in their organisations. As the eight conditions for the lawful processing of personal information will affect nearly every area of business that processes personal information, the consequences are that this will require behavioural changes, changes to legal documents, internal structural changes (i.e. information technology upgrades, assurances that a data base cannot be accessed and physical firewalls and safety measures), and an analyses of subcontracting practices.

As part of your POPI due diligence exercise, we recommend that companies 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. Companies 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.); and

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

In closing, the following actionable points will ensure that companies' due diligence 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; and

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

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.

Ali Ncume

May 2018

MASERUMULE

www.masconsulting.co.za