E|O|H|C|B
Employer's Organisation for Hairdressing • Cosmetology • Beauty
ADDING VALUE TO YOUR BUSINESS

THE JOURNAL

Protection of Personal Information (POPI) Act

Dear EOHCB Member,

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (‘*POPIA*’)

It’s been a long time coming, and the Protection of Personal Information Act 4 of 2013 (“POPIA”) finally come into full force on the 1st of July 2020.

The Protection of Personal Information Act (or POPI Act) is South Africa’s equivalent of the EU GDPR. It sets some conditions for responsible parties (called controllers in other jurisdictions) to lawfully process the personal information of data subjects (both natural and juristic persons).

The POPI Act does not stop you from processing and does not require you to get consent from data subjects to process their personal information. Whoever decides why and how to process personal information is responsible for complying with the conditions.

There are eight general conditions and three extra conditions. The responsible party is also responsible for a failure by their operators (those who process for them) to meet the conditions. The biggest impact is on organisations that process lots of personal information, especially *special personal information*, *children’s information,* and *account numbers*. The most affected industries are financial services, healthcare, and marketing.

This is a summary or short explanation of why it is important, who it affects, what the timeline is, and what action you should take.

Why do we need the Protection of Personal Information Act?

Essentially, the purpose of the Protection of Personal Information Act (POPIA) is to protect people from harm by protecting their personal information. To stop their money being stolen, to stop their identity being stolen, and generally to protect their privacy, which is a fundamental human right.

To achieve this, the Protection of Personal Information Act sets conditions for when it is lawful for someone to process someone else's personal information. Mariska du Plessis EOHCB NG Divisional Manager July 2020

The POPI Act is important because it protects data subjects from harm, like theft and discrimination. The risks of non-compliance include reputational damage, fines and imprisonment, and paying out damages claims to data subjects. The biggest risk, after reputational damage, is a fine for failing to protect account numbers.

Who are the Role Players?

The Protection of Personal Information Act (POPIA) involves three parties (who can be natural or juristic persons):

1. **The data subject**: the person to whom the information relates.
2. **The responsible party:** the person who determines why and how to process. For example, profit companies, non-profit companies, governments, state agencies and people. Called controllers in other jurisdictions.
3. **The operator:** a person who processes personal information on behalf of the responsible party. For example, an IT vendor. Called processors in other jurisdictions.

The Protection of Personal Information Act places various obligations on the responsible party, which is the body ultimately responsible for the lawful processing of personal information. Responsible parties should only use operators that can meet the requirements of lawful personal information processing prescribed by the Protection of Personal Information Act.

The Timeline of POPIA:

The POPIA commenced on the 1st of July 2020, which makes the deadline for organisations to comply 1 July 2021.

Protection of Personal Information (POPI) Act

On 12 May 2020, the Information Regulator made an urgent plea to government to bring POPIA in to full force, citing the adverse effects that the absence of fully functional and effective personal information regulatory authority is beginning to have on the country. Mariska du Plessis EOHCB NG Divisional Manager July 2020

When the President acts on the Information Regulator's request, which should be sooner rather than later, organisations will have a twelve-month grace period within which to become fully compliant.

Who is affected?

Any natural or juristic person who processes personal information, including large corporates and government.

What steps will you have to take to comply?

Responsible parties will have to take various steps to comply. For example:

1. Appoint an Information Officer.
2. Draft a Privacy Policy.
3. Raise awareness amongst all employees.
4. Amend contracts with operators.
5. Report data breaches to the regulator and data subjects.
6. Check that they can lawfully transfer personal information to other countries.
7. Only share personal information when they are lawfully able to.

What are the Penalties for Non-compliance?

There are essentially two legal penalties or consequences for the responsible party:

1. A fine or imprisonment of between R1 million and R10 million or one to ten years in jail.
2. Paying compensation to data subjects for the damage they have suffered.

It is very unlikely that anyone will go to jail and the fines are small compared to other jurisdictions. The other penalties include:

- Reputation damage
- Losing customers (and employees)
- Failing to attract new customers

But your main motivation for complying with the Protection of Personal Information Act (POPIA) should be to protect people from harm.

One step at a time:
The first port of call for any organisation is to consider the role of the information officer. For a private company, the information officer will be the CEO, or a person duly authorised by the CEO for that purpose. Published on 14 December 2018, the POPIA regulations extend the information officer's duties, and impose certain mandatory responsibilities. The role of information officer is therefore a critical role, and not something that can be dealt with lightly.

The next step is to get the requisite buy-in from the organisation, and assign responsibility for driving forward POPIA compliance. From that point, each business unit or department can start with personal information audits to map what personal information is processed by the business, how it is collected, processed, stored and destroyed, and whether the requisite consents have been sought. This level of visibility, early on, will put organisations in a much better position to perform proper gap analysis and prioritise those areas most at risk.

Existing policies can be updated and, where necessary, new policies created and implemented to address the actual compliance gaps identified during gap analysis. These may well include updates to employment or supplier contracts, supplier on-boarding processes, marketing policies, consent wording, record retention policies, subject access request policies, and data protection policies.

Organisations will also be required to develop, monitor and maintain a manual as prescribed.
In addition, organisations will be required to 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.
It is the role of the information officer to ensure that the compliance framework is implemented, monitored, and maintained throughout the organisation.

The final step to compliance would be to ensure the proper socialisation and implementation of systems, policies and procedures through training, internal awareness sessions, annual re-training, and compliance audits.

Contact your EOHCB representative to discuss the information contained in this journal and the implementation thereof.

Adding Value to YOUR business!