Protecting your practice in a digital world

POPIA comes into effect on 1 July 2021

By Tasneem Gangat, Head: Compliance at Glacier by Sanlam

"The guiding purpose of the government regulator is to prevent rather than to create something" – Alan Greenspan

Unpacking the Protection of Personal Information Act (POPIA)

Over the recent past regulators have been creating a lot of red tape which then makes it harder to do business. It helps to understand the rationale behind the legislation and exactly what is required of us.

Let's look at some of the key concepts and the aim of POPIA.

Key concepts and definitions in POPIA

POPIA takes effect on 1 July this year and will compel companies to protect personal information and to prevent unauthorised exposure to such information. The express purpose of the Act is to protect people from harm to and to give effect to the right to privacy as contemplated in the constitution. The Act covers both natural persons and legal entities.

Key concepts

Data subject - The person to whom the personal information relates

Personal information – This can include demographic information, e.g. race, marital status, language, religion; biometric information, e.g. fingerprints, voice recognition; usernames and passwords, contact information, opinions and preferences, and background information.

Special personal information – Includes the protection of information of minors; religious or philosophical beliefs; race or ethnic information; sexual preference; trade union memberships, DNA, and political opinions.

Responsible party - The person who determines why and how to process the information, e.g. for-

profit companies, non-profit companies, governments, state agencies and people. They are referred to as controllers in other jurisdictions.

Operator - A person who processes personal information on behalf of the responsible party. This person can be held responsible for breaches, but the Responsible Party still remains accountable for the information.

Conditions for lawful processing

POPIA sets out eight conditions that businesses must comply with when processing the personal information of data subjects. These eight conditions are the foundational principles of POPIA that, when complied with, ensure that a data subject's personal information is being processed lawfully. This information is generally documented in a business's privacy policy and/or in their POPIA consent document. The eight conditions are listed below:

- Accountability - Responsible parties and operators must comply with these eight conditions.
- Processing limitation - Personal information should only be obtained for the intended purpose, and in a way that does not unnecessarily infringe the privacy of the data subject.
- Purpose specification – The purpose must be specific, defined and lawful.
- Further processing limitation – If the company needs to do something further with the information, it has to be compatible with the original reason the information was collected.
- Information quality – The information must be accurate and updated when required.
- Openness – The company must notify the regulator, and the individual in question, that the information is being processed, in instances where prior authorisation is required.
- Security safeguards – The company has to ensure that the confidentiality and the integrity of the data is secured.
- Data subject participation – The data subject has certain rights in terms of POPIA. They may request disclosure of the information held and can also request that incorrect information be corrected. They may also request deletion of the information.

There are certain circumstances where consent is not needed, provided there's a legitimate interest the company is protecting – this can be either the company's or the client's interest.

All Responsible Parties need to have a data governance framework in place. This should detail the security around the information, as well as list the processes involved. A data governance policy is also required.

What needs to be done in order to comply?

- Appoint an Information Officer. By default, this is the CEO, but they may delegate someone to fulfil this role.
- Draft a privacy policy.

- Create awareness within the company around measures that have been put in place.
- Amend contracts with operators
- Report data breaches to the regulator and data subjects. The Information Officer has to advise the regulator how the data breach happened, and measures that have been put in to place to ensure future safety of information and confirm that the affected data subjects have been informed.
- Check that you can lawfully transfer personal information to other countries. If information is transferred, you may be subject to laws and restrictions of the other country. Cloud storage could result in the privacy regime of another country being applicable to your data.
- Only share personal information when you are lawfully able to.

Penalties for non-compliance

There are two legal penalties for the responsible party:

- A fine or imprisonment of between R1m and R10m or one to ten years in jail.
- Paying compensation to the data subjects for the damage they have suffered.

It is unlikely that anyone will go to jail and the fines are small compared to other jurisdictions. However, the other penalties for the company include reputational damage, losing customers and employees, and failing to attract new customers.

The main motivation for complying with the POPIA Act should be to protect our clients from harm.

Visit the Tax & Legal Insights section on Glacier Insights for more information on POPIA.