HOW TO AVOID SANCTIONS UNDER POPIA

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Melody Musoni | January 27, 2022

With the coming into full operation of the Protection of Personal Information Act, 4 of 2013 (POPIA), we have been receiving questions from clients regarding the implementation of the POPIA sanctions. We noticed that a lot of people are confused on when POPIA sanctions can be imposed on a business, organisation or individual acting as responsible parties. For example, if a responsible party fails to comply with a POPIA condition, does that automatically mean that there will be penalties? In this article, we discuss some of the sanctions under POPIA, when such sanctions can be imposed and we provide a few good practices to mitigate the risk of sanctions.

What are the sanctions?

Before we share tips on how to avoid the sanctions under POPIA, we think it is important if you know what these sanctions are. The type of sanctions imposed on a responsible party usually depends on the type of offence committed under POPIA or type of non-compliance with POPIA. The offences can be grouped into two – serious offences and minor offences. Serious offences are those which can result in higher administrative fines or longer jail terms (up to 10 years). Minor offences attract penalties of fines and jail terms of up to one year.

Serious offences under POPIA relate to failure to comply with an Enforcement Notice issued by the Information Regulator or failure to comply with a Statement from the Information Regulator regarding application for prior authorization; please take note that the commencement date for section 58 (2) of POPIA (relating to application for prior authorisation) is 1 February 2022. Serious offences are also constituted by the giving of false information to the Information Regulator while under oath, the unlawful processing of an account number such as disclosure of an account number, selling of an account number or offering to sell an account number, and obstructing the Information Regulator from carrying out its functions.

The other offences under POPIA which carry lesser penalties relate to submitting an Information Notice with false information, obstruction of the execution of a warrant, breach of confidentiality, several offences by witnesses involved in an investigation or non-compliance with certain requirements for prior authorization.

When an organisation or responsible party has been found guilty of an offence and there is a criminal sanction of serving jail term, normally the Information Officer of the organization will be the one to go to prison.

An Information Officer can also be found guilty in their personal capacity. This usually happens when they fail to carry out their duties as the Information Officer or fail to comply with an Enforcement Notice issued by the Information Regulator.

What is the process before the sanctions can be imposed?

POPIA has put in place minimum requirements which must be complied with when processing personal information. Simply because a business has not complied with a POPIA condition, does not automatically mean that the Information Regulator will come knocking on its doors and imposing the 10 million rand fine. There are certain procedural steps that the Information Regulator follows before it issues an Enforcement Notice. If a responsible party continues to ignore the Enforcement Notice or fail to comply with the list of action items, they will be committing an offence and further immediate action can be taken by the Information Regulator.

The first step of the process is the lodging of a complaint with the Information Regulator. The complaint process usually starts when a responsible party is alleged to be interfering with the protection of personal information of a data subject by not complying with the POPIA conditions, the relevant codes of conduct, not notifying the regulator of security compromises, not complying with direct marketing requirements or transborder data flow requirements. Any person can lodge a complaint with the Information Regulator. Upon receiving the complaint, the Information Regulator can take any action depending on the cases and such actions may include conducting a pre-investigation, conducting a full investigation of the matter, referring the matter to the Enforcement Committee or doing nothing. During pre-investigations, the Information Regulator gives the responsible party an opportunity to respond to the complaint. If the response is satisfactory, the Information Regulator may use its best endeavors to secure a settlement.

The Information Regulator can also launch a full investigation into the complaint. It can summon any person to come and give evidence. It can also apply to court for a search warrant, enter premises and conduct searches. After an investigation, the Information Regulator may refer the complaint to the Enforcement Committee. The committee must consider the matters and make a finding. The committee may make recommendations to the Information Regulator necessary or incidental to any action that should be taken against the responsible party or the Information Officer or head of a private body.

If the Information Regulator, after considering the recommendations of the Enforcement Committee, is satisfied that the responsible party has interfered with the protection of personal information of a data subject, the Information Regulator may serve the responsible party with an Enforcement Notice. The notice can prescribe certain steps that need to be taken by the responsible party within a specific period or certain steps that the responsible party should not be taking. The notice can require the responsible party to stop processing personal information specified in the notice or processing the personal information in a certain manner. A responsible party can exercise its right to appeal an Enforcement Notice to the High Court. Failure to comply with an Enforcement Notice is a serious offence. The criminal sanctions are up to 10 years jail time, a fine or both fine and imprisonment.

An Enforcement Committee may also make recommendations to the Information Regulator against an

Information Officer in terms of the Promotion of Access to Information Act (PAIA). There are certain duties imposed on an Information Officer in terms of both POPIA and PAIA. If the Information Officer destroys, damages, conceals, falsifies a record, they may be held criminally liable and sentenced to up to two years in jail or pay a fine. If the Information Officer acts grossly negligent in failing to make sure that the responsible party has a PAIA Manual in place, they may be held criminally liable and sentenced to up to 2 years in jail or pay a fine. A failure to comply with an Enforcement Notice can result in an Information Officer being imprisoned for a period not exceeding 3 years or payment of a fine or both fine and imprisonment.

How to mitigate POPIA sanctions

When a responsible party has been found guilty of committing an offence under POPIA, the next step will be for the Information Regulator to determine the appropriate fine.

One of the factors the Information Regulator takes into account to mitigate the sanctions is looking at whether the organisation failed to carry out a risk assessment or failed to operate good policies, procedures and practices to protect personal information. This is why we encourage organisations to:

- have clear POPIA compliance plans;
- understand data flows and have inventories and ROPAs (Records of Processing Activities) in place;
- embed privacy considerations into its vendor management process;
- regularly conduct POPIA due diligence exercises;
- have right systems to manage data throughout its lifecycle, from collection until deletion; and
- regularly train their employees and have good governance documents in place.

Other factors that are considered by the Information Regulator include the following:

- the nature of the personal information involved – one may argue that special personal information may warrant a higher level of protection and lack of such protection may attract higher penalties;
- the duration and extent of the contravention – if a POPIA non-compliance has been ongoing, there are good chances that the fine will be higher compared to a once-off non-compliance;
- the number of data subjects affected or potentially affected by the contravention – the higher the number of data subjects affected, the likelihood that there will be a higher fine;
- whether or not the contravention raises an issue of public importance – a good example will be the case with the publication of Matric results and concerns around POPIA compliance. You can read our comment relating to this;
- the likelihood of substantial damage or distress, including injury to feelings or anxiety suffered by data subjects;
- whether the responsible party or a third party could have prevented the contravention from occurring;
- whether the responsible party has previously committed an offence in terms of POPIA.

While sanctions under POPIA may be the last resort, it is very important for responsible parties to cultivate a culture of POPIA compliance in all their lines of business. We have written extensively on what businesses should be doing to comply with POPIA. You can read some of our articles on our website or you can contact us to discuss.

Contact us for more good, precise, advice.