DASHBOARD
LEGAL UPDATES

EDITION 06 | APRIL | 2021

The Protection of Personal Information Act (POPIA) - part two

This publication is part two of a two-part POPIA publication series for retirement funds.

- Part one is a general explanation of certain provisions of POPIA.
- Part two deals with matters of practical implementation of POPIA.

Sometimes funds simply do not know where to start when it comes to POPIA.

POPIA is by no means uncomplicated. Thus, this publication article about what retirement funds can do to ensure they are initially POPIA compliant before 30 June 2021. This doesn't include every aspect of POPIA compliance. There are many ways to reach compliance and the suggestions in this publication are one of many approaches.

We do not think retirement funds should approach POPIA the same way companies do. Funds can leverage off their employer's projects, but they are different, and need to produce their own deliverables. Lawful POPIA processing should be propelled by the fund.

Step One – Training and agendas

Training on POPIA creates awareness of what needs to be done, an understanding that it is going to take time and resources as well as buy-in at a board level and from those that are going to be asked to do some work. This training should be generally about POPIA as well as be specific to retirement funds.

Consider adding POPIA as a standing item on the fund's agenda. Reporting and supervision concerning the fund's move to POPIA compliance before 1 July 2021 and then POPIA items thereafter such as the handling of data subject requests, supervision of operators and other matters of ongoing compliance would need to be part of board meeting discussions.

Step Two – create a POPIA data-base

Consider adding everything you do on POPIA for the Fund into the fund's electronic data-base. This will provide evidence of standards and measures you have put in place down the line. If you set it up at the beginning, you will be able to produce it easily if you are asked for it later (for example if you have a breach).

Step Three – appoint/authorise and register the Fund's Information Officer

Please see part one of this publication series for more information about information officers.

Step Four– map the fund's activities

Mapping means to document the activities where we process personal information and information relevant to the activities. Mapping the fund's activities means documenting all the activities the fund does on a day-to-day basis, e.g. receiving contributions or having board meetings.

The process of mapping activities identifies how the fund acquires, uses, keeps information, who else uses that information and for what purposes we use it. For each activity we also identify the personal information we are processing for that activity and the purpose of the processing. In addition, among other things, the fund should identify red flags, for example whether the activity includes the processing of special categories of personal information protected by POPIA, like special personal information, children's information, bank account details, information leaving the country and the like.

Mapping is the precursor to many other deliverables, such as the fund's privacy impact assessment (which is a statutory requirement). It may be difficult to do a privacy impact assessment (see below) if you have not first mapped out the activities that a fund performs.

Step Five – managing the Fund's operators

The fund is responsible for its operator's (service providers) compliance with the Eight Conditions of POPIA. As most of a fund's operations are delivered through operators, managing POPIA risks related to operators is very important for the fund. Start early. This means the fund needs to know what they are doing about POPIA, how they are going to ensure ongoing POPIA compliance as well as monitor them. This requires ongoing reporting from operators to the fund.

The fund's operators cannot be treated the same as some are more risky, from a protection of personal information point of view, than others. For example, the fund will be more concerned about its administrator than its legal advisor.

Identify and document all your operators. Then understand what fund personal information they will process, including any red flags as mentioned in mapping above. After this, you can risk-rate them which gives you an indication of which operators you need to focus on more and first.

Decide and agree what reporting you need from operators (including about their POPIA projects, security measures, privacy related complaints, etc.) and how you are going to monitor them.

Ensure there are no nasty surprises for anyone - communicate what you are going to need from operators by way of any assurances. Communicate the fund's policies to them, for example its data protection policy.

Ensure their agreements have been updated for POPIA (including the requirement to report breaches to the fund).

Step Six – complete the fund's privacy impact assessment and convert into a plan

All funds must, by law, do a privacy impact assessment. A privacy impact assessment means a document where the fund assesses the impact that POPIA has on it, their data subjects (e.g. members), its current privacy practices, its current state of compliance with POPIA, where the biggest impact will be, and what the fund should focus on. You can use your mapping information to assist the fund in completing its impact assessment.

Step Six – complete the fund's privacy impact assessment and convert into a plan

All funds must, by law, do a privacy impact assessment. A privacy impact assessment means a document where the fund assesses the impact that POPIA has on it, their data subjects (e.g. members), its current privacy practices, its current state of compliance with POPIA, where the biggest impact will be, and what the fund should focus on. You can use your mapping information to assist the fund in completing its impact assessment.

The notion that our Information Regulator has in relation to a privacy impact assessment seems to include the concept of a gap-analysis, where you test your fund activities against compliance with at least the Eight Conditions in POPIA. This is different to a traditional impact assessment, in our view, and requires a fairly detailed analysis. While you are doing this assessment, remember to document any authorisations, justification or grounds you are going to be relying on to process personal information outside of the Eight Conditions or other POPIA requirements, as the fund is going to need this information.

Once you have identified, in your impact assessment, what measures, standards and other actions you are going to take, remember to plan to ensure implementation on time. Who is going to do what and by when?

Step Seven – sort out what the fund is going to do about a POPIA compliance framework and what it will entail

Every fund, by law, must have a compliance framework to ensure POPIA compliance. Not every fund currently has an existing compliance framework. If you do have one, you will need to work your POPIA compliance framework into the overall fund compliance framework. If the fund does not currently have am existing compliance framework it will need to ensure that it at least implements a POPIA compliance framework.

Step Eight – consider what fund documentation you need to draft or change

You will need to ensure that fund documentation contains the required disclosures (and where relevant consents). Communication to data subjects, like members and beneficiaries, is key to lawful processing. You will need to set up processes and reporting for this (some of which may be prescribed).

You will need to check you have updated your Code of Conduct (or consents from and disclosures to board officials) and that you put in place a data protection policy. A data protection policy is not a requirement of law but it will create an additional layer of protection for the fund. This policy should include a data breach process/response as well as the fund's retention and destruction practices.

Forms, booklets, other policies, guides, member statements and other communication to members should be updated for the relevant disclosures (and other requirements) necessary under POPIA, where required.

Funds are currently exempted (until 31 December 2020) from having to do a section 51 PAIA manual. PAIA has been amended by POPIA and there are now additional requirements to include in a manual. I suggest a fund does have such a manual but that is extends it now to include the POPIA requirements and that it also includes the activities where it is relying on justification or grounds to process personal information, as these should be communicated. The manual can also set out data subject participation processes.

Step Nine – Other

You will also need to (among other things):

- Look at IT, physical and process security measures and processes;
- Roll out an awareness programme (required by law);
- Include identification and management of privacy complaints in your complaints management; and
- Check your insurance coverage related to POPIA.

Start now

There is quite a bit to do, so please take action soon.

We hope this article goes some way to putting you on the path towards lawful processing under POPIA.