DASHBOARD
LEGAL UPDATES

EDITION 05 | APRIL | 2021

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

This publication is part one 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.

Effective date

Most of the provisions of POPIA that are of interest to us became effective as of 1 July 2020. We all now have until 1 July 2021 to reach a state where we are compliant with this legislation.

There is allowance in law for an extension to the date of 1 July 2021, but that appears unlikely and we certainly cannot rely on an extension being forthcoming.

Does POPIA apply to retirement funds?

Yes, it does.

POPIA applies (with exceptions) to the processing of personal information in a record by, or on behalf of, a responsible party.

Thus, it become important to understand the following words:

Personal information is widely defined and includes almost all information you can think of about a living, identifiable person (and where applicable juristic persons), including race, gender, pregnancy, marital status, medical history, contact details, biometric information, their personal opinions amongst other information (note for POPIA purposes personal information about a deceased person is not personal information).

Processing is also widely defied and includes almost anything one does with personal information, including, receiving or collecting it, storing it (electronically or physically), filing it, or destroying it.

A **record** means any recorded information regardless of the form in which it is recorded. So a record includes electronic and paper information, x-rays, photos, labels, drawing, graph, map, etc which is in the possession of the responsible party (whether or not they created it).

A **data subject** is a person (natural or juristic) to whom personal information relates. In the fund context, this could include, for example, a member or former member, beneficiary, a board member, a service provider, or a divorce order or maintenance order payee.

A **responsible party** means the person who determines the purpose and means for processing information. In the retirement funds context, *depending on what activity is being performed*, retirement funds will mainly be responsible parties for the majority of their activities. The Responsible Party bears the bulk of accountability for compliance under POPIA, as compared to operators.

Operators process information for, or on behalf of, responsible parties. It is probable that many fund service providers, such as administrators and consultants will mainly be operators for most of the activities they are performing for the fund. Operator's responsibilities are set out below.

A retirement fund, for many fund activities, determines how its operators will process the personal information of the fund's members (and others). For example, the fund enters into an administration agreement with the administrator determining the purposes for which that administrator will process personal information on its behalf.

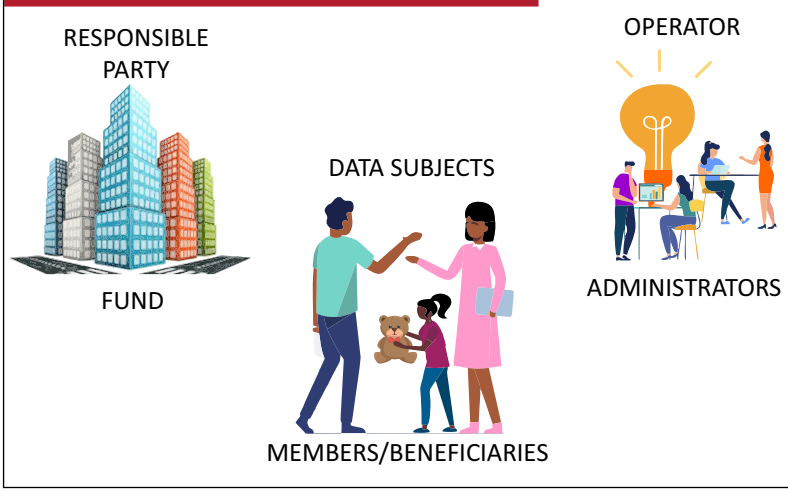
An operator's responsibilities

- Secure the personal information. Establish and comply with security measures provisions
- Only process information as agreed with the responsible party
- A written agreement with the responsible party
- Notify breaches to the responsible party
- Treat personal information confidentially and do not disclose it (unless required by law or in the course of properly doing our duties)
- Tell the responsible party if you are using third parties to process the personal information

The Eight Conditions

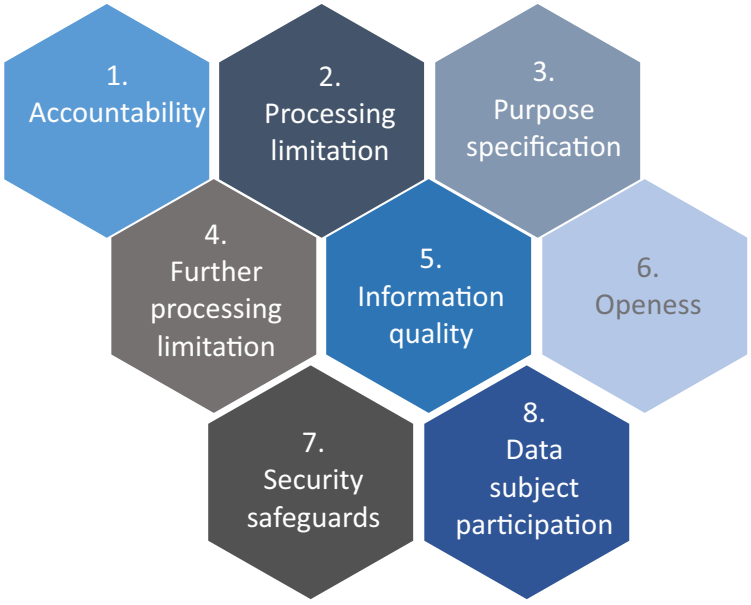
Responsible parties are required to comply with the *Eight Conditions* when they process personal information for the first time and every time. *Responsible parties* (such as funds – for many of their activities) **must ensure that their operators comply with the Eight Conditions when they are processing personal information for the fund.**

Simplified example - fund payment of a benefit



Think of all the activities that a fund performs, for example: payment of claims, receiving and investing contributions, board elections, financial statements, service provider management, valuations, etc. All of these activities include the processing of personal information. Thus, every time the fund performs such an activity in needs to comply with the eight conditions and other requirements of POPIA (or ensure that its operator complies).

What are the Eight Conditions? So very simply they are the following:



It is necessary to dig a little deeper to understand the Eight Conditions. The Eight Conditions are groups of principles. There is often more than one principle per Condition.

Another notable feature of POPIA is that it often provides us with a Condition or a "rule" and then provides a number of **justifications** whereby if you fall into one of these justifications the rule does not apply. This makes POPIA fairly complex to implement. These justifications need to be identified, documented and communicated.

More detail about the Eight Conditions, with which responsible parties must comply when processing personal information, appears below. The number corresponds to the Condition number.

1 **Accountability** of Responsible Party

To ensure Conditions for lawful processing are complied with:
- When determining purpose and means of processing, and
- During the process.

2 **Processing** of PI: **Lawfulness**

And in a responsible manner that does not infringe on the privacy of a data subject.

The Responsible Party is responsible for ensuring that personal information is processed, upfront and every time subsequently, in accordance with POPIA, lawfully and does not infringe on the privacy of a data subject.
The Responsible Party must ensure that it and its operators comply with the Eight Conditions for lawful processing of personal information as set out in POPIA.

2 **Processing** of PI: **Minimality**

Given the purpose for which it is processed, the processing is adequate, relevant and not excessive.

- Only process personal information in a way that connects correctly, or relates suitably to the fund's purposes
- Don't process personal information for more than the fund's purposes
- Don't process more personal information than the fund needs to for the purposes
- Don't collect more personal information that the fund needs – but ensure you collect what the fund needs
- Don't process more personal information than the fund communicated it would or for a purpose the fund did not communicate (see information about purpose below).

2 Processing of PI (Personal Information): Consent and justification

- Data subject consent is required, OR
- It's necessary to carry out actions for a contract with the data subject OR
- It complies with an obligation imposed by law on the RP**, OR
- It protects the legitimate interest of the data subject OR
- It's necessary to perform a public law duty of a public body OR
- It's necessary to pursue the legitimate interests of the RP or a 3rd party to whom the information is supplied

RP bears burden of proving consent
Data subject can withdraw consent at any time (subject to provisos).

2 Processing of PI: Objections

A data subject may object to processing of PI at any time subject to certain limitations and procedures.

The Fund may only process personal information if the data subjects consent or one of the above justifications exist for not obtaining consent. Generally speaking, for many activities, it is not practical for funds to rely on consent, thus they must identify the justification they will use to process personal information (for specific activities) without consent.

2 Processing of PI: Collection from data subject

Personal Information must be collected directly from the data subject.

This is a difficult Condition for funds to comply with as often funds receive personal information about the data subject from the employer, not the data subject (e.g. member) themselves. The justifications for not complying with this Condition are:

- Consent from the data subject
- *Collection from another source would not prejudice a legitimate interest of the data subject*
- *Collection from another source is required to comply with an obligation imposed by law*
- *To maintain the legitimate interests of the fund*.

Justifications would need to be identified, documented and communicated by the fund.

3 Purpose: Collection for a specific purpose

Personal Information is collected for a specific, explicitly defined purpose related to your function or activity.

Purpose is a central concept in POPIA. Personal Information may only be collected for a specific, explicitly defined, lawful purpose that is related to a function or activity that the fund is performing. The fund has to know and document its purposes for processing personal information. The Responsible Party (e.g. the fund) must ensure that the data subject (e.g. a members or beneficiary) knows about the purpose (unless there is a justification that applies). The purpose must be made known to the data subject before the personal information is collected, but not too long before. The best time is probably when the personal information is being collected. This creates the need for amendments to fund documentation or new fund documentation (forms, policies and manuals).

4 Further processing limitation

Further processing of personal information must be compatible with the purpose for which it was collected A test is set out for this.

The fund may only further process personal information (i.e. for purposes other than those the personal information was collected) if the further processing is compatible with the purpose for which we originally collected the personal information. A responsible party must assess whether further processing of personal information is compatible with the original purpose for which it was collected by considering:

- The relationship between the additional processing and the original purpose;
- The nature of the information involved;
- How the additional processing will affect the data subject;
- How the information was collected; and
- Any contractual rights and obligations between the parties.

5 Information quality

Reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary (having regard to the purpose).

6 Openess - documentation

Documentation must be maintained for all processing operations specified in its manual.

The fund has continuing obligations under Condition five with respect to the integrity of personal information.

Conditions 6 means that documentation must be kept by the fund for all processing operations (activities) that it has specified in its section 51 Promotion of Access to Information Act manual. Retirement funds are currently exempted from having to have a section 51 PAIA manual. This exemption currently applies until 30 June 2021. There is no talk currently of a further exemption after this date. Manuals are lodged with the SA Human Rights Council (currently) or other entity (as prescribed in future). The Information Regulator may at some stage prescribe more information about what she wants in manuals and as regards data subject requests.

6 **Openess -** notification when collecting

If information is collected the data subject must be aware of certain specified information at specified times/timeframes.

When information is being collected, data subjects must be made aware of the information below.

- the information that is being collected and if the information is not being collected from the data subject, the data subject must be made aware of the source from which the information is being collected;
- the name and address of the person/organisation collecting the information;
- the purpose of the collection of information;
- whether the supply of the information by the data subject is voluntary or mandatory;
- the consequences of failure to provide the information;
- whether the information is being collected in accordance with any law;
- if it is intended for the information to leave the country and what level of protection will be afforded to the information after it has left South Africa.
- who will be receiving the information;
- that the data subject has access to the information and the right to correct any details;
- that the data subject has the right to object to the information being processed; and
- that the data subject has the right to lodge a complaint with the Information Regulator. The contact details of the Information Regulator must also be supplied.

The information must be made know to data subjects before collection, if being collected directly from the data subject, or soon as reasonably practicable after if not collected directly from the data subject. If the data subject is already aware of the above points (e.g. you have told them before) then you don't need to tell them again. If you collect additional information from a data subject for a different purpose, you have to go through this process again.

Justifications not to comply with this Condition include:

- Consent;
- Would not prejudice legitimate interest of data subject;
- Not reasonably practicable for the particular case.

Again, this requires amendment or creation of fund documentation.

3 **Purpose**: Retention, destruction and restiriction of records

- Records must not be retained longer than necessary to achieve the purpose for which they were collected or subsequently processed (except for a few reasons).
- Personal information must be destroyed, deleted or de-identified once the RP is no longer authorised to keep it.
- Destruction must be done so that it can't be reconstructed intelligibly.
- Personal information must be restricted in certain circumstances and is then subject to procedural requirements for access.

Regarding retention of information:

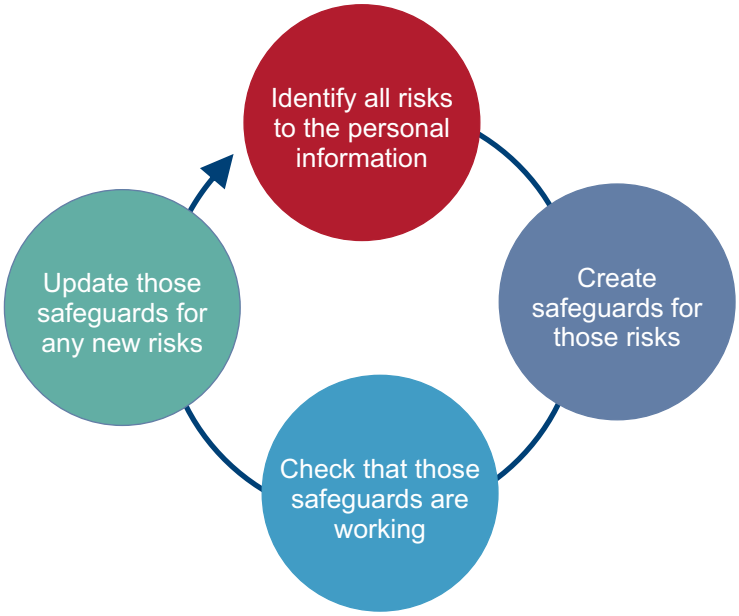
One of the 'exceptions'/ justifications is that if we are authorised by law to keep the personal information, we may do so.

Retention is a very difficult subject for retirement funds to manage as funds are often asked for personal information long after a member has left the fund.

7 **Security safeguards:** Integrity and confidentiality

- Secure integrity and confidentiality of PI under its control/ in its possession by taking appropriate, reasonable, technical and organisational measures to prevent loss, damages, unauthorised destruction and unlawful access or processing.
- A process is set out for this.
- Due regard to generally accepted information security practices and procedures that apply to it/ the industry and professional rules and regulations.

The fund is required to safeguard personal information through technical and organisational measures – this is both a business function and an IT function. The responsible party must do the following and ensure its operators do too:



7 **Security safeguards:** Operators or persons acting under authority

Operators and anyone processing for a RP or operator must mostly:

- Process only with the knowledge/ authorisation of the RP.
- Treat information as confidential and not disclose it.

7 **Security safeguards:** Operators

- In terms of a written agreement the operator must establish and maintain specific security measures.
- Operator must notify Responsible Party immediately if it believes that PI has been accessed/ acquired by unauthorised person.

7 Notifications of security compromises to the data subject and Regulator

- Where there are reasonable grounds to believe that personal information of a data subject has been accessed/acquired by unauthorised person this must be notified (generally) as soon as reasonably possible to: the Regulator and the data subject.
- Notification to data subject must be in writing, communicated in a specified way and include prescribed information.
- The Regulator may direct publicity of the compromise.

8 Data subject participation -Access, correction and manner of access

- A data subject may:
  - Request a RP to confirm that it holds personal information about them or request that information.
  - Ask for deletion, destruction or correction of certain information.
- There are some prescribed actions for the Responsible Party.
- Procedures and fees may be prescribed.
- The Promotion of Access to Information Act applies to the requests.

Data subjects can:

- Ask what personal information we hold about them and request access;
- Ask for corrections, deletions, or destruction;
- Object to the fund processing their personal information;
- Procedures, forms and fees (manual/notice);
- Complain to the responsible party; and
- Complain to the Information Regulator.

Other POPIA requirements

It is not enough to simply comply with the Eight Conditions. There are many other provisions of POPIA, which we need to understand and with which we need to comply, for example about:

- Children's information
- Special personal information
- Account numbers
- Direct marketing
- Prior authorisation of processing
- Automated processing;
- Information Officers, and
- Personal information leaving the country.

Some of these additional requirements are set out below.

Special personal information

Special personal information is specified classes of personal information that are sensitive. The principle for special personal information is that we may not process it unless there are grounds that justify it (as set out in POPIA) or if authorised by the Information Regulator. There are:

(a) general grounds authorising us to process all types of special personal information; and
(b) there are specific grounds for each type of special personal information that authorise us to process that specific type of special personal information.

One of the possible actions that a fund could take if it does not have a ground to process special personal information is to obtain prior authorisation from the Information Regulator to do this type of processing. This has to be obtained before the processing is commenced.

Funds (and their operators) often process special personal information, for example when performing section 37C death benefit investigations, for disability benefits, processing nomination of beneficiary forms or exercising a discretion to withhold benefits. The different types of special personal information are:

RELIGIOUS/ PHILOSOPHICAL BELIEFS | RACE/ETHNIC ORIGIN | TRADE UNION MEMBERSHIP | POLITICAL PERSUASION | HEALTH | SEX LIFE | BIOMETRIC INFORMATION | CRIMINAL BEHAVIOUR

Children's personal information

Children (persons under 18) are afforded special protection under the law (including POPIA) as they are vulnerable members of our society. We may not process children's information unless we fall within specific justifications in POPIA, for example we have consent, it is necessary to exercise an obligation in law, etc. These justifications need to be identified, documented and communicated.

Personal information leaving South Africa

We may not transfer personal information about a data subject outside the country (including cloud storage) unless we comply with specific requirements/exceptions. The fund should ensure that the exceptions to the general prohibition against such processing of information, as set out in POPIA, exists. These exceptions relate to consent, which country the personal information is passing through and what privacy legislation it has, what agreements or binding corporate rules are in place with the processing parties, etc.

Account numbers

These are criminal offences related to processing account numbers that attract a fine of up to R10 million or 10 years in jail. Subject to certain criteria existing, it is a criminal offence to knowingly or recklessly obtain or disclose an account number or not comply with the conditions and other requirements set out in POPIA with respect to account numbers.

Prior authorisation

A responsible party must obtain prior authorisation from the Information Regulator prior to any processing if that responsible party plans to process certain categories of information. These categories are:

(a) any unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection; and with the aim of linking the information with information processed by other responsible parties. (Unique identifiers include bank account numbers, identity numbers and telephone numbers);
(b) processing of information on criminal behaviour or unlawful or objectionable conduct on behalf of third parties. This would apply to any person contracted to conduct a criminal record enquiry or reference check about past conduct or disciplinary action;
(c) where there is processing of information for the purposes of credit reporting (for instance credit bureaus); and
(d) where a responsible party transfers special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for processing personal information.

The last category is broad and funds should pay special attention to it.

If the fund processes this kind of information, then it should immediately apply to the Information Regulator for prior authorisation, so that the fund's application can be considered before the end of June 2021. The fund would only be required to apply for prior authorisation once and not each time that personal information is received or processed (unless the processing departs from that which has been authorised).

Information Officers

Under POPIA every responsible party (e.g. a fund) must have an information officer and must register the information officer with the Information Regulator. Information officers are appointed automatically in terms of the Promotion of Access to Information Act (PAIA). Your PAIA information officer is also your POPIA information officer. For a fund, the information officer is the head of the private body as contemplated in PAIA. The head in the case of a juristic person (like a fund) is:

(a) the chief executive officer or equivalent officer; or
(b) any person duly authorised by that officer; or
(c) the person who is acting as such or any person duly authorised by the acting person.

So for funds, the chief executive officer or equivalent officer is automatically by default the information officer. Funds don't usually have chief executive officers, thus many funds have interpreted the "head" of a fund to be the principal officer of the fund. The head of the fund may authorise another person to exercise the powers, duties and responsibilities conferred or imposed on the information officer by POPIA and PAIA.

The Information Regulator on 1 April 2021, published the final version of the Guidance Note about Information Officers and Deputy Information Officers. The authorisation of another person to be the information officer must be in writing using a template that is substantially similar to the authorisation template annexed to the Guidance Note. Even if another person is authorised, the automatically appointed, default information officer retains the accountability and responsibility for any power or function authorised to another person.

There are varying interpretations of what the Guidance Note requires as to who may be an information officer in the fund context, thus, what follows is our own view. The Guidance Note states that if the information officer of the fund is authorising another person to be the information officer, it must be a natural person within the juristic body (i.e. the fund) that is authorised to act as an information officer of the juristic person (i.e. the fund). This would probably require the information officer (if not the principal officer) to be a fund official e.g. a board member, deputy principal officer or the chairman of the fund. If an employee of the fund is authorised to be the information officer, then the employee must be management and above.

Although the duties and responsibilities outlined in sections 55 and 56 of POPIA for information officers (see below) will be enforced on 1 July 2021, funds should be proactively implementing arrangements for the authorisation of their information officers, and where applicable the delegation of duties to any deputy information officers, to ensure that their responsibilities in Regulation 4 (see below) may be taken up by the information officer, and any appointed Deputy Information Officers as of 1 May 2021. However the Guidance Note also states that information officers and deputy information officers are required, in terms of Section 55(2) of POPIA, to take up their duties only after being registered with the Regulator.

Funds should register information officers promptly. Information Officers can be registered now through email and post and shortly (probably the end of April) using online registration from the Information Regulator's website. Email is probably the best method at the moment. Thereafter they can take up their duties officially.

There is a prescribed format for this application which is included in the Guidance Note (available on the Information Regulator's website at: https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf).
Please note that it is both the fund's and the information officer's duty to ensure the fund's information officer is registered.

Information officer duties

POPIA duties that an information officer is required to comply include, among other things, encouraging and ensuring that the responsible party (fund) complies with the provisions of POPIA, dealing with requests made under POPIA, and assisting the Information Regulator with any investigations conducted in respect of the fund.

The Regulations to POPIA Regulations prescribes the following duties to be performed by information officers, which include:

(a) a compliance framework is developed, implemented, monitored and maintained;
(b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
(c) a manual is developed, maintained and made available as prescribed in terms of PAIA;
(d) internal measures are developed together with adequate systems to process requests for information; and
(e) internal awareness sessions are conducted regarding the provisions of POPIA, the Regulations, codes of conduct or any other information obtained from the Information Regulator.

PAIA requires that in respect of private bodies (such as funds), the Information Regulator may annually request a private body to furnish it with information about requests received for access to records. The Information Regulator has not yet made such a request for information.

Part two

Please see part two in the POPIA series of publications.