tennant group

16 / 04 / 2021 | Edition 70.

the tennant times

A Legal Update

In this edition, we look at a number of issues relevant to retirement funds, including:

1. Compulsory annuitisation and withdrawals from retirement funds
2. Protection of Personal Information Act (POPIA) update:
   (a) Information officers, and
   (b) prior authorisation
3. FSCA Information Request 6 of 2020 (RF) – change to deadline

tennant life benefits

tennant administration services

Address: Hurlingham Office Park | 59 Woodlands Ave.
Block A | Suite 3
Cnr. Republic Rd. + William Nicol Dr.
Hurlingham Manor | 2196

Tel: (+27) 11 100 8110
Mail: info@tennant.co.za
Web: www.tennant.co.za
FSP: Licence No. 43648

1. Compulsory annuitisation and withdrawals from retirement funds

When a member withdraws from a fund (for example because the member has resigned from employment), the member may decide to take some of the withdrawal benefit in cash and transfer the rest to another approved fund. The member's benefit could be made up of a vested portion and a non-vested portion (see the previous publication about compulsory annuitisation). Thus, the question is: should the cash portion be taken from the vested portion or non-vested portion first?

The importance of the question is that the more cash that is taken from the non-vested portion (and not the vested portion), the more cash the member will be able to take when retiring from a fund to which the benefit was transferred.

Industry bodies wrote to the South African Revenue Service (SARS) requesting clarity on the answer to this question. SARS has confirmed that administrators must decide this for themselves and that SARS will not make this decision. There are a number of options that administrators can choose in this regard. Please contact you administrator with regards to their decision.

2. POPIA update (a) 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 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 in a position of management or 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.

POPIA duties that an information officer is required to comply with 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 prescribe the following duties to be performed by information officers, which include:

(a) a compliance framework to be developed, implemented, monitored and maintained;
(b) a personal information impact assessment to be 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 to be developed, maintained and made available as prescribed in terms of PAIA;
(d) internal measures to be developed together with adequate systems to process requests for information; and
(e) internal awareness sessions to be 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.

(b) POPIA and prior authorisation by the Information Regulator

A responsible party (e.g. a fund) must obtain *prior authorisation* from the Information Regulator prior to any processing if that responsible party plans to process certain categories of personal 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 (trans-border flows) where that country does not provide an adequate level of protection for the processing of personal information (i.e. the recipient of the information must be subject to a law, binding corporate rules or binding agreement which provides a level of protection that effectively upholds principles for reasonable processing of personal information that is substantially similar to the conditions for the lawful processing as mentioned under POPIA[1]).

Category (a)
The Guidance Note provides some clarification of what may be considered as a unique identifier under POPIA. In POPIA, the definition of a unique identifier is "any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party". This would include an account number issued by a financial institution which allows a data subject to access funds or credit facilities.

The Guidance Note has clarified that among other unique identifiers, the prior authorisation requirement for category (a) would include policy numbers (for insurance policies) as unique identifiers. It is arguable whether membership numbers for members of funds (allocated by administrators) are also unique identifiers.

Category (b)
Category (b) requires that a responsible party must obtain prior authorisation if it is processing: criminal behaviour or unlawful or objectionable conduct of data subjects on behalf of third parties. Where the fund, for example, is exercising a discretion under section 37D in order to make a deduction from, or withhold, a benefit it may be processing information about criminal behaviour or unlawful/ objectionable conduct about a member. However, our view is that the fund is processing this information for itself, not a third party (i.e. the employer or the member), so does not need to obtain prior authorisation.

Furthermore, the fact that the fund uses an operator (its administrator) to process the special personal information does not mean that it is processing the information for a third party. If a fund administrator or fund consultant is processing the same information, in our view, the administrator/ consultant would be processing the information as the fund's operator and would not have to obtain prior authorisation, as it is not a responsible party. Funds should test our views with their expert legal advisors if necessary.

Category (d)
Category (d) requires that a responsible party must obtain prior authorisation if they are processing special personal information ("SPI") or children's personal information that is leaving the country. The category is broad and funds should pay special attention to it.

If the fund processes personal information that requires authorisation, then it should immediately apply to the Information Regulator for prior authorisation *in the prescribed format*, so that the fund's application can be considered well before the end of June 2021. Questions in the prescribed format must be answered with sufficient detail and clarity as to

[1] There are some writers that are of the view that a responsible party would not currently have to stop processing the categories of personal information (which has been notified to the Information Regulator) until the Information Regulator has issued the required notice in the Government Gazette. This is not specified in the Guidance Note.

ensure a full understanding of the responsible party's processing activities. 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).

Prior authorisation is not required for the processing of the above-mentioned categories of personal information which took place prior to 1 July 2021, however any further or continued processing of the relevant categories of personal information (which was initially processed before 1 July 2021) will be subject to prior authorisation.

POPIA sets out timelines for the Information Regulator to make a decision on a prior authorisation application. The Information Regulator will approve or reject an application within four weeks of receipt, unless that office decides to conduct a detailed investigation, in which case it has a maximum of thirteen weeks to conclude its investigation and furnish a decision on the application. Please bear the time periods in mind if you are making application; if this time period goes over 1 July 2021, the fund may have to stop processing the information submitted for authorisation until it receives the authorisation[2].

A responsible party who processes personal information requiring prior authorisation before authorisation is granted by the Information Regulator will be guilty of an offence and liable for a fine of up to R10 million or imprisonment for a period not exceeding 12 months (or to both).

3. Financial Sector Conduct Authority ("FSCA") Information Request 6 of 2020 (RF) – change to deadline

The FSCA issued this Information Request on 14 December 2020. It is mandatory for funds and administrators to provide the requested information to the FSCA. The information requested is about pending section 14 transfers.

The deadline to provide this information to the FSCA has been moved to 31 May 2021. The FSCA has also provided a *recommended* format for a response.

[2] There is some debate about this among writers with some believing that the Information Regulator must issue the requisite Government Gazette before that office could require responsible parties to stop processing while the prior authorisation application is under consideration.