Retirement funds and the protection of personal information

Workshop 13, 14 May 2021

Leanne van Wyk
ICTS Legal Services (Pty) Ltd

PENSION LAWYERS ASSOCIATION

25 YEARS OF MAKING A DIFFERENCE · 25 YR

- What have funds been doing to ready themselves for POPIA?
- What are the issues they have run into?

PENSION LAWYERS ASSOCIATION

25 YEARS OF MAKING A DIFFERENCE

When must funds be ready?

Commencement date - 1 July 2020

One year grace period before the Information Regulator will start enforcing POPIA ends on **30 June 2021**

1 July 2021

Whose who in the retirement fund POPIA zoo?

Distinguishing responsible parties from operators

PENSION LAWYERS ASSOCIATION

25 YEARS OF MAKING A DIFFERENCE · 25 YR

The fund and its operators

Why does it matter who is a responsible party and who is an operator?

Fund – is a responsible party (for most of its activities). Think about all these activities….

Ensuring its own compliance

AND

The responsible party remains liable to data subjects for enforcement action by the Information Regulator in relation to actions of its operators

Know who your operators are, what risk they pose to you and put the relevant measures in place

Co responsible parties – the processing wouldn't be possible without both parties

PENSION LAWYERS ASSOCIATION

The fund and its operators

Who are the fund's operators and who are co responsible parties?

Responsible party

- Determines the purpose and means of processing of PI (alone or together with other responsible parties) –why and how
- Decides to collect the PI in the first place, what to collect and what will be done with it, how long to keep it…
- Penalties
- Has ultimate control over the PI and what happens with it
- Written contract with operator - confidentiality and security measures. The security measures and liabilities - must be *contractually* imposed (not imposed under POPIA)
- Compliance with eight conditions plus other requirements

Operator

- Processes PI for/on behalf of a responsible party & on its own authority in terms of a contract/mandate
- What IT systems or other methods to use to collect PI
- Receives the PI to perform functions
- Usually doesn't own the PI
- Can exercise some control over manner of processing
- Comply with the contract plus limited requirements under POPIA
- Maintain confidentiality of PI
- Only act on the instruction/ authorisation of Responsible Party
- Report security compromises

- Determined by actual activities in a specific situation, rather than a formal designation
- Not always clear-cut
- Operator may have a little or a lot of discretion over how the
- processing takes place, using its own expertise
- The fact that you are providing a service to someone else doesn't necessarily mean you are an operator
- Liability clauses – difficult to negotiate but good to have
- Exceeding a mandate – then a responsible party?

PENSION LAWYERS ASSOCIATION

The fund and its operators

Examples:

- Administrator
- Valuator
- Actuary
- Auditor
- Attorney
- Asset manager
- Consultant
- Administrator
- Participating employer
- Asset managers

Indications that you might be a responsible party

- Statutory obligations – processing as a result of a statutory obligation
- Professional obligations /expert or professional skill – subject to oversight by a professional body (as opposed to statutory obligations under legislation like FAIS) - responsibility may (also) lie with the professional service provider itself because it determines what information to obtain and process in order to do the work and because it is answerable itself for the content e.g. attorneys, auditors, actuaries (ICO Guidance gives solicitors (attorneys) and accountants as examples of professionals who may be data controllers (responsible party) in the performance of specialist services)

PENSION LAWYERS ASSOCIATION

The fund and its operators

Examples:

- Administrator
- Valuator
- Actuary
- Auditor
- Attorney
- Asset manager
- Consultant
- Administrator
- Participating employer
- Asset managers

- Actuaries/ Valuators/ auditors/ accountants - use large degrees of professional skill and judgement in determining how they are to provide the service to funds in accordance with their professional obligations plus certain activities are underpinned by legislation, thus they may (for some activities) have enough control over the processing of PI to be a responsible party

- A generalist service provider: provide services as per client's instructions. Doesn't have to comply with any externally imposed requirements (other than compliance with the general law). Can have broad or narrow instructions from client. Generalist service provider has little or no flexibility or independence in how he or she provides the service. Consultant?

- Administrators –more specific the authorisation/ instructions from the fund re PI, more likely to be operator for that activity. Fewer decisions about PI -more likely to be operator e.g. what to collect, how long to keep it, who they can give it to. Agreements – should be more specific than less, if to be an operator for those activities

- Asset managers – depends what they are doing. Also check processing of personal information (member, fund service providers, their own employees, etc)

PENSION LAWYERS ASSOCIATION

The fund and its operators

Examples:

- Administrator
- Valuator
- Actuary
- Auditor
- Attorney
- Asset manager
- Consultant
- Administrator
- Participating employer
- Asset managers

And what about the employer?

Operator –

- Section 37C death benefit investigations
- Death benefits nomination of beneficiary forms
- Claim forms?

Agreement

PENSION LAWYERS ASSOCIATION

To be or not to be… that is the question…

Retirement fund information officers

PENSION LAWYERS ASSOCIATION

25 YEARS OF MAKING A DIFFERENCE · 25 YR

PENSION LAWYERS ASSOCIATION

Retirement fund information officers

- Every fund has a “default” information officer by law
- Probably the Principal Officer (closest position to CEO)
- Can authorise someone else (prescribed format)
- But remains accountable
- Who can they authorise? Natural person, “internal” to the entity
- Person - executive level or equivalent
- Employees – management level or above
- Probably not someone at the employer
- Not someone at service provider (especially if the entity is the fund’s operator)
- Better to ‘acknowledge’ in writing. Must ‘authorise’ someone else in writing
- Appoint deputy Principal Officer and delegate only information officer responsibilities? But note - must act as PO if PO leaves the country/ unable to discharge duties. May need to amend rules
- Must register. When and what’s up with the 1 May 2021 date?

S8(2)(c): The PO may … delegate any of the PO’s functions under this Act and the rules of the fund to the deputy PO …

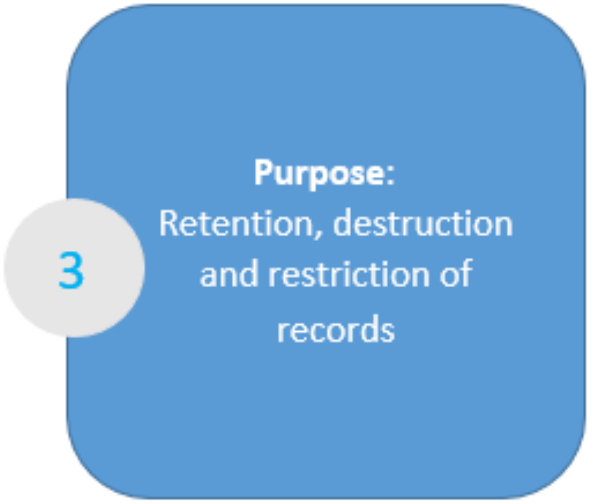
How long is a piece of string....

Retention decisions are proving problematic for funds

PENSION LAWYERS ASSOCIATION

25 YEARS OF MAKING A DIFFERENCE · 25 YR

Retention



- 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.

- Up to fund to determine – not administrator
- Under the GDPR, funds have been struggling to decide how long they should keep records of PI and have asked the regulator for guidance – not much guidance forthcoming yet
- Same in SA – guidance from Information Regulator/FSCA would be very welcome
- Some funds – ask for administrator retention schedule (if they have one) to use as basis
- Most service provider agreements – only deal with what they will do with information when agreement with fund terminates – not during subsistence of agreement (policy)
- Board/fund officials – Code of Conduct/agreement

PENSION LAWYERS ASSOCIATION

Records examples

Records examples	Records examples
Fund rules and amendments	Returns to the FSCA
Valuations	Complaints and requests
Financial statements	Member records
Minutes (including sub-committees) and resolutions	Beneficiary records
Agenda packs and annexures	Deduction records and evidence
FAIS advice documents	Unclaimed benefits and tracing
Policies	Dependants and nominees forms
Claim forms, option forms, switch forms	Retirement benefit counselling evidence
Claim reports	Benefit statements, projection statements
Disability/ill-health health information	Benefit quotes
Contributions records	Benefit payments and documentation
Contribution schedules	Trustee elections
Member booklets, presentations and other communication	Section 14 transfers

UK fund examples of retention wording from fund data protection policies

The Fund, in providing statutory duties under the regulations has determined that it cannot permanently delete a member's record. Should a member transfer out of the scheme, the Fund will retain a basic record confirming the member's name, contact, date of birth and national insurance number details but will endeavour to delete any other information including any documents relating to the member. The basic member details are required to be retained to enable the Fund to comply with statutory and legal obligations such as fraud prevention and GMP reconciliation.

How long will we hold your data?

We will only keep your personal data for as long as we need it to administer the Fund and to deal with any questions or complaints that we may receive about this, unless the law requires us to keep it for a longer period. In practice, this means that your personal data may be retained for as long as you (or any beneficiary who receives benefits after your death) are entitled to benefits from the Fund and for a period of 15 years after those benefits stop being paid. For the same reason, your personal data may also need to be retained where you have received a transfer, or refund, from the Fund in respect of your benefit entitlement.

- Personal data will be retained for **the greater of**:[2]
- such period as the Member (or any Beneficiary who receives benefits after the Member's death) are entitled to benefits from the Fund and for a period of 15 years[3] after those benefits stop being paid;
- 100 years from the Member's date of birth;[4]
- 100 years from the date of birth of any Beneficiary who received benefits from the Fund after the Member's death.

During any period when we retain personal data, we will keep that personal data up to date and take all reasonable steps to ensure that inaccurate data is either erased or rectified without delay. We will periodically review the personal data that we retain and consider whether it is still required; any personal data that we no longer require will be destroyed.[5]

Pre-authorisation by the Information Regulator

PENSION LAWYERS ASSOCIATION

25 YEARS OF MAKING A DIFFERENCE · 25 YR

PENSION LAWYERS ASSOCIATION

Compulsory prior authorisation

- There are instances where a responsible party must get **prior authorisation** from the Information Regulator **before** it may process personal information
- These must be identified and applied for (prescribed format for application)

Prior authorisation

- 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
- This is **compulsory**
- 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)

Prior authorisation - category (b)

- Includes information about disciplinary action, criminal record
- Where the fund, e.g. 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, my 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 this 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 my 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 my views with their legal advisors if necessary

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.**

PENSION LAWYERS ASSOCIATION

Category (d)

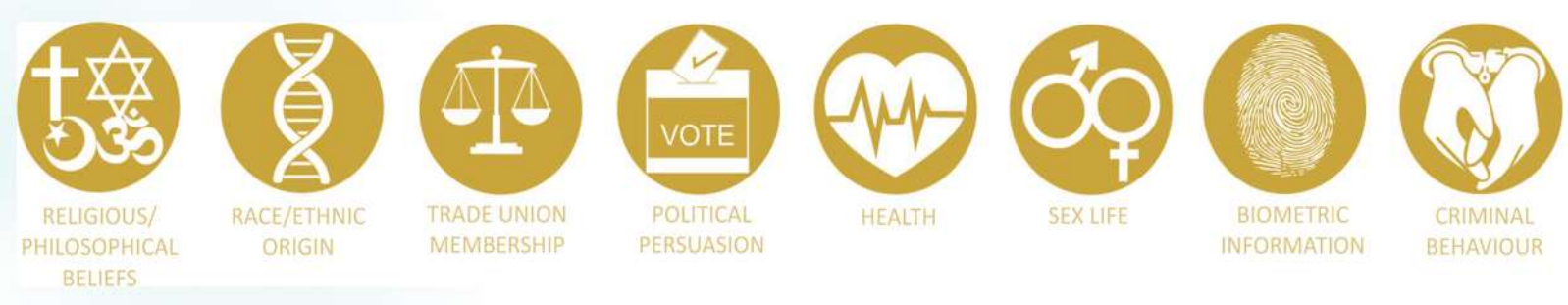
- This category is broad and funds should pay special attention to it
- Children – under 18 (or not legally competent)
- Special Personal Information – see below
- Watch out for cloud storage

2.6.2. the criminal behaviour of a data subject to the extent that such information relates to-

a) the alleged commission by a data subject of any offence; or

b) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

Responsible party must obtain prior authorisation if they are processing special personal information or children's personal information that is **leaving the country and the third party does not have the relevant protections required under S72 (law/ rules/ agreement)**



PENSION LAWYERS ASSOCIATION

Prior authorisation

- TIMING: apply soon in the prescribed format
- Provide sufficient detail to ensure a full understanding
- Apply 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
- **Timelines** decision within 4 weeks of receipt (may not process during this time), unless decides on a detailed investigation - 13 weeks
- **Offence**: a responsible party (e.g. fund) 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)

PENSION LAWYERS ASSOCIATION

Privacy impact assessment

(Yes, you must do one)

PENSION LAWYERS ASSOCIATION

25 YEARS OF MAKING A DIFFERENCE · 25 YR

Privacy impact assessment

Responsibilities of Information Officers

4. (1) An information officer must, in addition to the responsibilities referred to in section 55(1) of the Act, ensure that-

(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;

- Under GDPR, an impact assessment only required for high-risk processing
- Under POPIA – every Responsible Party must do an impact assessment
- Regulation 4 – Information Officer responsibility
- Adequate measures and standards exist to comply with the conditions
- Sounds more closely aligned to a gap analysis than a risk analysis
- Would suggest you also include prior authorisation, special personal information, children's information and account numbers

PENSION LAWYERS ASSOCIATION

Consent and justifications

PENSION LAWYERS ASSOCIATION

25 YEARS OF MAKING A DIFFERENCE · 25 YR

PENSION LAWYERS ASSOCIATION

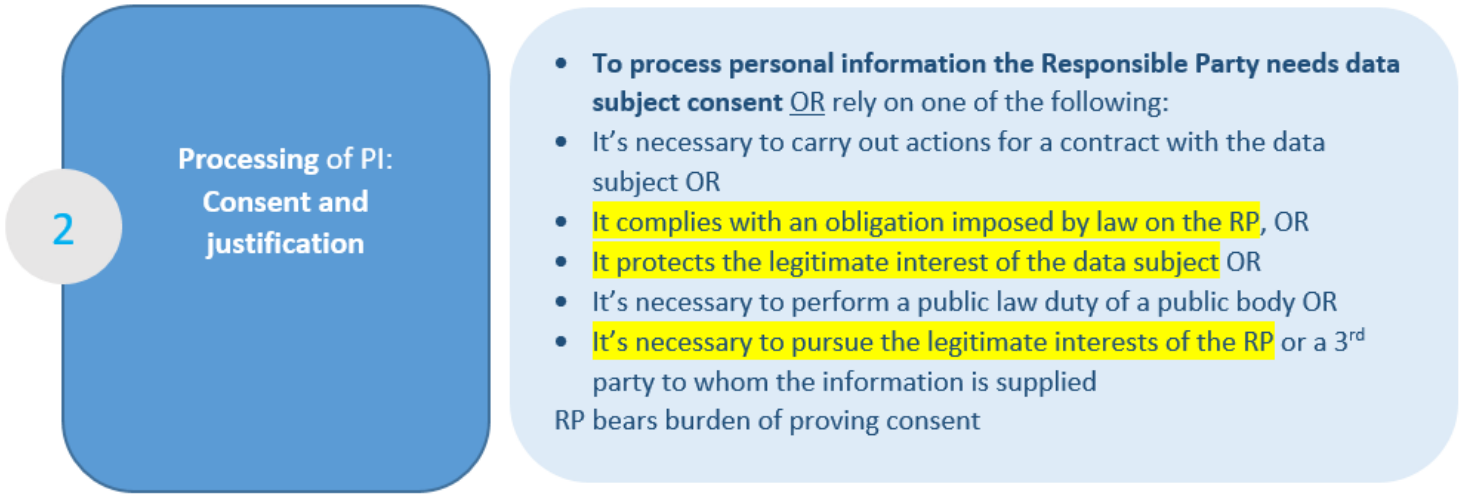
Grounds for processing: consent OR? Consider which ground you are going to rely for processing for your different activities

Examples

Plus

Justifications for non-compliance with other conditions for example – condition 2 – you must collect PI from the data subjects themselves

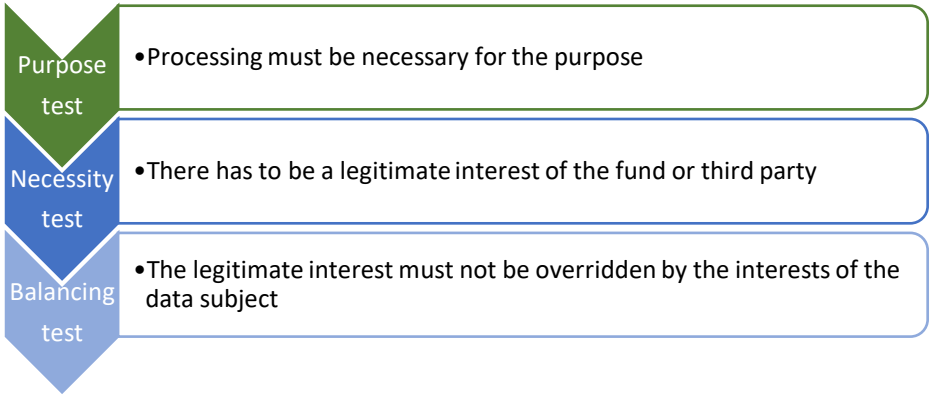
Identify justifications, test them, document them and communicate them



Consent and justifications

The legitimate interest test

- Where the fund relies on “legitimate interests of the fund” to process personal information it will balance its own interests with that of the data subject and will apply a **test** which looks at purpose, necessity and balance :
  - (a) Is there a legitimate reason (business objective) or purpose for the processing? Is it our legitimate interest? What is the legitimate interest?
  - (b) Is processing the information necessary for that purpose (e.g. a lawful business objective) and why is it important to the fund (is it elective or business critical)?
  - (c) “Is the legitimate interest overridden by the interests of the data subject?
- The fact that the data subject has a reasonable expectation that the fund will process their personal information helps to pass the test. Less likely to apply where the processing is unwanted
- A relevant and appropriate relationship between the parties will also assist – fund and member would be a relevant and appropriate relationship
- Balancing the data subject’s interest includes taking measures to protect their privacy rights



Are we going to see a Code of Conduct for retirement funds?

PENSION LAWYERS ASSOCIATION

25 YEARS OF MAKING A DIFFERENCE · 25 YR

THANK YOU

Let’s meet in the Q&A room for questions

Leanne van Wyk
ICTS Legal Services (Pty) Ltd
vanwykl@icts.co.za
083 257 8468

PENSION LAWYERS ASSOCIATION