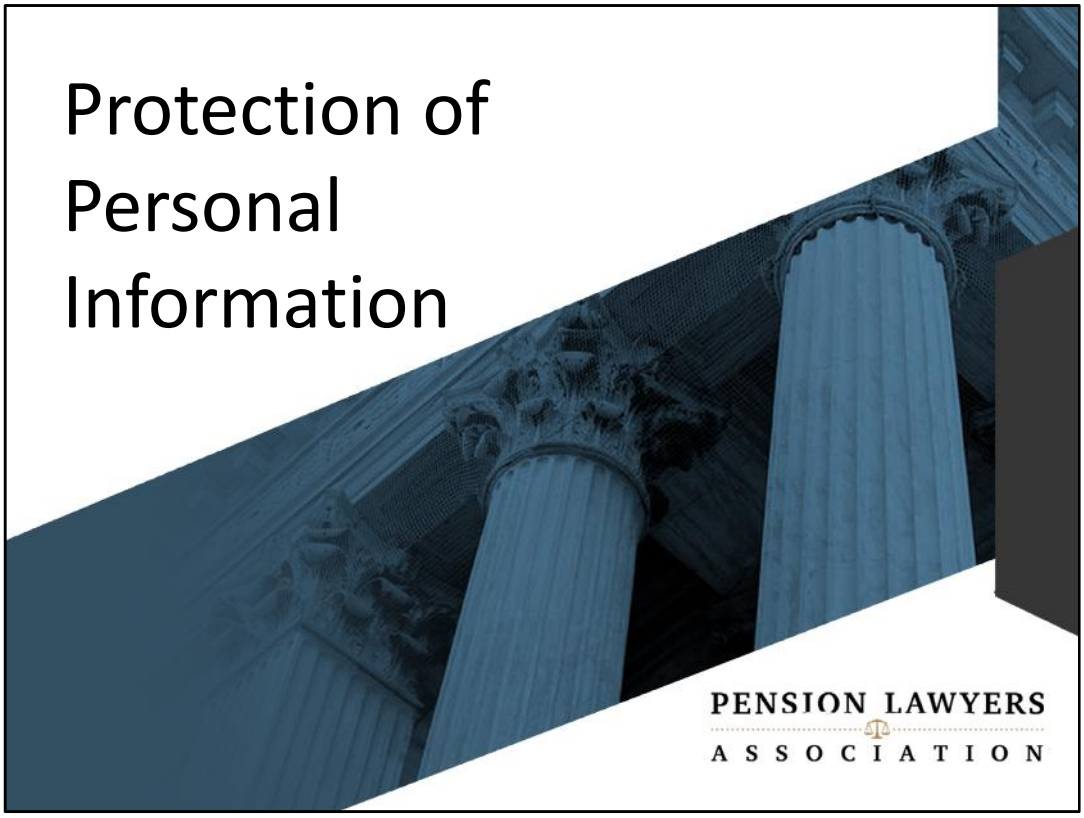
Protection of Personal Information



Protection of Personal Information Act – What is in store for retirement funds?

by Samantha Davidson

PENSION LAWYERS ASSOCIATION

Agenda

1. History and purpose of legislation
2. Key concepts
3. Features for retirement funds
4. IRFA submissions

1. HISTORY AND PURPOSE OF LEGISLATION

Legal protection of privacy in SA

- Common law – delict (sue for damages)
- Bill of rights – section 14
- Protection of Personal Information Act, 2013 (Information Regulator and Enforcement Committee)

Common law:

To succeed in an invasion of privacy action, a plaintiff must show that the defendant acted wrongfully, with animus injuriandi, and impaired the plaintiff's personality rights.

Invasions of privacy may broadly be classified as encompassing either intrusions into the plaintiff's physical solitude and seclusion, or giving publicity to private facts.

To prove that the invasion was not wrongful, the same defences are available to a defendant as exist in defamation law. Hence, in general, truth for the public benefit, fair comment and privilege may be raised as defences.

Lexis Nexis "Law of South Africa" at 428

As in common law, the constitutional right to privacy is not an absolute right - it may be limited in terms of law of general application and has to be balanced with other rights entrenched in the Constitution.

Constitution of the Republic of South Africa, 1996

S 14 – right to privacy

S 32 – right of access to information

S 36 – limitation of rights

The Constitution of the Republic of South Africa, 1996

Section 14:

"Everyone has the right to privacy, which includes the right not to have:

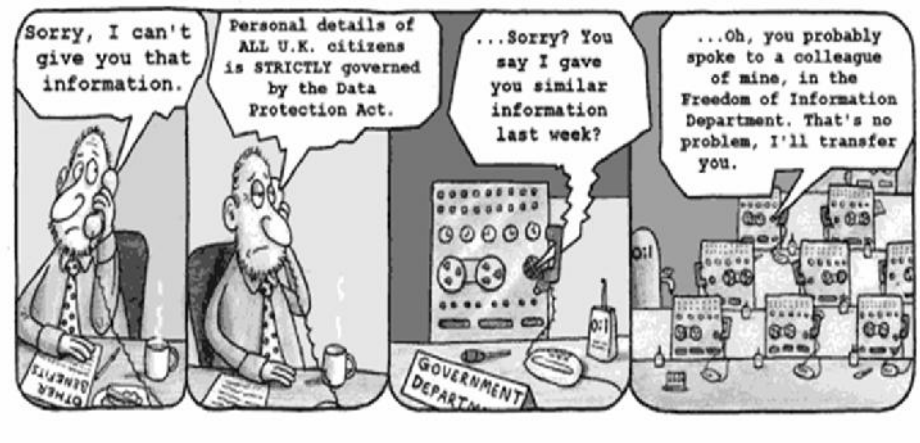
(a) their person or home searched;
(b) Their property searched;
(c) Their possessions seized;
(d) The privacy of their communications infringed."

Section 32 (1) "Everyone has the right of access to-

(a) Any information held by the state; and
(b) Any information that is held by another person and that is required for the exercise or protection of any rights."

Section 36(1) "The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including:

(a) The nature of the right;
(b) The importance of the purpose of the limitation;
(c) The nature and extent of the limitation;
(d) The relation between the limitation and its purpose; and
(e) Less restrictive means to achieve the purpose.


Sorry, I can't give you that information.
Personal details of ALL U.K. citizens is STRICTLY governed by the Data Protection Act.
...Sorry? You say I gave you similar information last week?
...Oh, you probably spoke to a colleague of mine, in the Freedom of Information Department. That's no problem, I'll transfer you.
GOVERNMENT

South African Law Reform Commission

Project 124 (October 2005): Privacy and Data Protection

- included 1st draft of POPI Act
- noted over 30 countries had already enacted info protection legislation

http://www.justice.gov.za/salrc/dpapers/dp109.pdf

1980 - OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Data

Organisation for Economic Co-operation and Development
= forum where governments work together to address the economic, social and environmental challenges of globalisation.

34 member countries

SA is a key partner

Guidelines were a response to 2 trends

- Recognition of the importance of information
- Impact of automated processing (computer technology) of personal information on rights of individuals

"Thirty Years after the OECD Privacy Guidelines"
www.oecd.org/sti/ieconomy/49710223.pdf

1995 – EU Data Protection Directive

Personal info can only flow to countries with “adequate protection”
= possible barrier to international trade

POPI Act 4 of 2013

- 19/11/2013 signed by President
- From 11/04/2014:
  - S 1 (definitions)
  - Part A of ch 5 (Information Regulator)
  - S 112 and 113 (regulations by Minister of Justice)
- Awaiting effective date of balance

7 September 2016, Parliament voted for the following appointments to the office of the Information Regulator (for POPI and PAIA), which were later approved by the Minister of Justice and Correctional Supervision:

Chair:	Adv Pansy Tlakula (former chief electoral officer of IEC)
Full time members:	Adv Cordelia Stroom
	Johannes Wepond
Part-time members:	Prof Tana Pistorius
	Sizwe Snail

Draft Regulations under POPI Act

Published on 8 September 2017 (two months for comments) re:

- forms and processes incl.:
  - complaints
  - code of conduct for sector
- duties of information officer

Purpose of POPI Act

- Protect personal information when processed by a responsible person
- Provide rights and remedies when breach
- Establish office of Information Regulator to promote and enforce rights in Act

Purpose of Act
2. The purpose of this Act is to—
(a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—
(i) balancing the right to privacy against other rights, particularly the right of access to information; and
(ii) protecting important interests, including the free flow of information within the Republic and across international borders;
(b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;
(c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and
(d) establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

2. KEY CONCEPTS

"personal information"

Of "data subject":

- living, natural person (e.g. member, beneficiary, trustee)
- existing juristic person (e.g. fund, corporate employer)

Not "personal" if already in public domain

Data subject can be anywhere in the world, but if their personal info is processed in SA, the POPI Act applies

"personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

"processing"

- collecting, receiving, recording, organizing, storing, updating, using, distributing, deleting
- by automatic means or not
- written, drawn, tape recorded
- using any device

in SA (excludes in the course of purely household or personal activity)

Conditions for lawful processing

include:

- collect directly from data subject
- limited to what is required for purpose
- purpose specification
- complete, accurate, up to date info
- disclosure to data subject on request

Section 4 of POPI Act

Lawful processing of personal information
(1) The conditions for the lawful processing of personal information by or for a responsible party are the following:
(a) ''Accountability'', as referred to in section 8;
(b) ''Processing limitation'', as referred to in sections 9 to 12;
(c) ''Purpose specification'', as referred to in sections 13 and 14;
(d) ''Further processing limitation'', as referred to in section 15;
(e) ''Information quality'', as referred to in section 16;
(f) ''Openness'', as referred to in sections 17 and 18;
(g) ''Security safeguards'', as referred to in sections 19 to 22; and
(h) ''Data subject participation'', as referred to in sections 23 to 25.

….exclusions (s6 and 7) and exemptions (s37 and 38)…

Can be varied by Code of Conduct for particular industry/sector

Special protection for information of a child

Transborder flow of personal info

A responsible person in SA may not transfer personal info to a third party who is in a foreign country unless certain conditions are met

N.B. Host of “cloud” server is often foreign

"responsible person"

means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information

If you take part in determining the purpose of and the means for processing personal information, you are a responsible party
"A Guide to the Protection of Personal Information Act" by de Stadler and Esselaar (Juta) at page 43

3. FEATURES FOR RETIREMENT FUNDS

Who is the responsible person?

Eg: member's ID/age

Employer – resident/work permit required, check over 15 yrs, assess normal retirement age
Fund (BOT) – check over 55 yrs for retirement benefit + apply correct tax, life stage investment transitioning, insured benefits (if age-related)
Long-term insurer – premiums for and availability of insured benefits

S13B Administrator also processes this personal info, but are they merely an **"operator''?**

means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party

For example to verify the bank account into which a benefit payment is to be made on exit from the fund, or to trace if the benefit is unclaimed.

Doesn't the administrator determine *"the purpose of and means for processing personal information".* The BOT seldom instructs the administrator on the means/processes to be followed.

Conditions for lawful processing are imposed on processing "*by or for*" a responsible party
(so both responsible party and operator are bound) BUT…

Section 4 of POPI Act

Distinction is N.B

"responsible person" must ensure all conditions for the lawful processing of personal info are met – otherwise, liable

"operator" must only process with knowledge and authorization of responsible person and must not disclose the personal info (exceptions)

Section 8 of POPI Act:

Responsible party to ensure conditions for lawful processing
The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

Section 20 of POPI Act
Information processed by operator or person acting under authority
An operator or anyone processing personal information on behalf of a responsible party or an operator, must—
(a) process such information only with the knowledge or authorisation of the responsible party; and
(b) treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

Joint liability?

New EU Data Protection Regulation seeks to impose direct responsibility and liability on data processors (operators under POPI Act), subjecting them to the same enforcement mechanisms as apply to data controllers (responsible party under POPI Act)

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

Admin fines of up to 4% of their worldwide turnover

Possible test: "for whose purpose is the processing taking place?"

e.g. internet service provider (ISP) for emailing - ISP processes traffic and billing data (ISP is responsible party) but re: content of email, sender is responsible party (ISP is operator)

The extent to which a person has control over the purpose of and means for processing will determine whether a person is an operator (processor) or a responsible party (controller)

Example from the EU Data Protection Working Party "Opinion on the concept of 'controller' and 'processor'" WP 169 (2010) cited in "Information and Communications Technology Law"2nd edition, van der Merwe and others (Lexis Nexis) at page 439

Fund is definitely a responsible person
Administrator is probably an operator part of the time and a responsible person part of the time

Must be a written contract between responsible party and operator

to, among other things, ensure operator establishes and maintains security measures (s19)

Section 19 of POPI Act

Security measures on integrity and confidentiality of personal information

(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to—

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

FEATURES FOR RETIREMENT FUNDS cont.

Conditions for lawful processing

S5(a)(i) **right to be notified that personal info is being collected**

S18 (notice includes):

- Source
- Name, address of responsible party
- Purpose
- Any law authorizing collection
- If to be transferred internationally
- Rights to access, object, complain

unless consent to non-compliance or no prejudice to legit interests

18. (1) If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of—
(a) the information being collected and where the information is not collected from the data subject, the source from which it is collected;
(b) the name and address of the responsible party;
(c) the purpose for which the information is being collected;
(d) whether or not the supply of the information by that data subject is voluntary or mandatory;
(e) the consequences of failure to provide the information;
(f) any particular law authorising or requiring the collection of the information;
(g) the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;
(h) any further information such as the—
(i) recipient or category of recipients of the information;
(ii) nature or category of the information;
(iii) existence of the right of access to and the right to rectify the information collected;
(iv) existence of the right to object to the processing of personal information as referred to in section 11(3); and
(v) right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator,
which is necessary, having regard to the specific circumstances in which the information is

or is not to be processed, to enable processing in respect of the data subject to be reasonable.

Data often from employer payroll –
Funds must decide how they will give notice, generally:

? Fund rules (do members read them)
? member benefit statement
? annual report to members

- on Nomination of beneficiary form
- Transfer on exit
- S37C investigation process

S11(1) can only process personal info if:

- Consent
- Necessary for performance/ conclusion of contract and data subject is party to that contract
- Obliged by law
- To protect legit interest of data subject
- Public law duty
- Necessary for legit interests of responsible party or recipient

IRFA have made submission for Code of Conduct to recognise what usual processing does not require consent

S12 must collect directly unless:

- Consent
- Obliged by law
- No prejudice to legit interest of data subject
- For litigation
- Necessary for legit interests of responsible party or recipient
- National security
- Not reasonably practicable

IRFA have made submission for Code of Conduct on usual processing that can take place without collecting data directly from member/data subject

S13 collection must be for specific, lawful purpose
(reminder – as stipulated in S5 notice)

S15 further processing must be compatible with purpose

E.g.

- can fund use next of kin from nomination of beneficiary form to try and trace member with unclaimed benefits?
- Can fund use ID no. of pensioner to check whether their death has been recorded with Home Affairs?

S14 must destroy record as soon as purpose achieved unless:

- law requires/permits retention
- Reasonably required for lawful purposes related to usual functions
- Consent
- Retention required by contract

Destroy/delete = "*prevent reconstruction in an intelligible form"*

E.g.: Income Tax Act requires:

- Tax assessments kept for 5 yrs
- Staff personnel records kept for 3 yrs after employment ceased
- Salary and wage registers kept for 5 yrs
- Invoices, bank statements, year-end working papers, vouchers and general correspondence kept for 5 yrs

S16 responsible party must take reasonably practicable steps ensure personal info is complete, accurate, updated

S23 access to personal information

Safer to invite verification than publish

23. (1) A data subject, having provided adequate proof of identity, has the right to—
(a) request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and
(b) request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information—
(i) within a reasonable time;
(ii) at a prescribed fee, if any;
(iii) in a reasonable manner and format; and
(iv) in a form that is generally understandable.
(2) If, in response to a request in terms of subsection (1), personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 24 to request the correction of information.

S19 security measures - responsible person must:

- Secure integrity and confidentiality;
- Take appropriate, reasonable, technical and organizational measures
  - assess risks
  - implement safeguards
  - test and update

19. (1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—
(a) loss of, damage to or unauthorised destruction of personal information; and
(b) unlawful access to or processing of personal information.
(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to—
(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
(b) establish and maintain appropriate safeguards against the risks identified;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

4. IRFA Submissions

Legal and Technical Committee of the Institute of Retirement Funds Africa (IRFA) made 3 submissions to the Information Regulator:

- Code of conduct
- "tribunal" to include PF Adjudicator and FSB Appeal Board
- PO to be default Info Officer

Retirement funds exempted from many provisions of Promotion of Access to Information Act. E.g. no need to appoint "Information Officer"(defined as the head of the private body)

Code of Conduct

Fund = responsible party
Administrator = operator

Basis upon which funds can process personal info without consent and not collected directly from data subject

List can also be used by funds to give notice of personal info being processed

Listed:

- Provider of personal information
- Receiver of personal information
- Type of information
- Law that imposes obligation to process/ legit interest advanced
- Comments (e.g. fund insured benefits and Long-term Insurance Act = ASISA industry code expected)

Sample Extract from IRFA Submission on Code of Conduct

Provider of personal information	Receiver of personal information	Type of information	Law that imposes obligation/ legitimate interest	Comments
Fund/ administrator	Fund's auditor Fund's valuator/actuary Administrator's auditor	Proper registers, books and records of the operations of the fund Including: membership records with details and dates of joining and leaving the fund, contributions received, premiums paid in respect of insured benefits (e.g. death and ill health), payments of pensions and benefits, movement of assets, receipt or payment of money or assets in respect of transfers in and out, payments made to a member leaving the fund other than on transfer.	Section 7D(1)(a) Pension Funds Act, 1956 Circular PF No. 98	

IRFA on Tribunals

S12(2) direct collection, S15 further processing, S18 notice of processing

unless for the conduct of proceedings (commenced or reasonably contemplated) in court or tribunal

- IRFA submission is PF Adjudicator and FSB Appeals Board = tribunal

PLA represented on IRFA Legal and Technical Committee – will give feedback re: response of Info Regulator to submissions.

(FSB not opposed to submissions)


THANK YOU
PENSION LAWYERS
ASSOCIATION
WWW.PENSIONLAWYERS.CO.ZA