The implications of the Protection of Personal Information Act, 2013 on the fulfillment of trustees' duties

Pamela Stein
Webber Wentzel
pamela.stein@webberwentzel.com

PENSION LAWYERS ASSOCIATION

Today's presentation

- **POPI: overview and key terms**
- **Application of POPI**
- **Eight conditions for lawful processing of personal information**
- **Compliance and Sanctions**
- **Trustee Obligations under POPI: operators, members and dependants**

PENSION LAWYERS ASSOCIATION

Why need for POPI?

- Is a constitutional imperative –informational privacy-balanced with other rights
- Enhances the individual's ability to protect personal information-rights and remedies created
- Allows SA to be internationally competitive in the information age-regulation in accordance with international standards
- Industry codes encouraged

POPI legislative history

- The 10th draft of the Bill was adopted by the National Assembly in August 2013 and assented to on 19 November 2013
- Impact of EU Review in final draft of POPI
- Now imminent proclamation of commencement date
- Once enacted, period of 1 year (or 3 if Minister extends) to get house in order with information that is being processed at the time of the Act

What POPI regulates

- POPI regulates of processing of personal information of a data subject by the responsible party or an operator
- “Customers”
- Suppliers/Contractors
- Employees

Key Definitions

- **Personal Information** means information relating to an identifiable, living natural person, and where applicable juristic person, including:
  - 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
  - education or the medical, criminal, employment or financial history of a person
  - identifying number, email address, telephone and physical address,location info, online identifier
  - biometric information
  - personal opinions, views or preferences of the data subject
  - explicitly or implicitly private or confidential correspondence
  - views of others about that person
  - name if name would reveal information about the person

Key definitions

- "**processing**" means collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as restriction, erasure or destruction of information

- "**Responsible party**" – public or private body which alone or in conjunction with others determines the purpose of and means for processing personal information

- "**Operator**" - person who processes PI for responsible party in terms of contract or mandate, without coming under the direct authority of the responsible party

Key definitions

- "**Special Personal Information**" means a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sexual life, biometric information, criminal behaviour – alleged commission by data subject of an offence or any proceedings in respect of this offence

- **'Information Officer'** – is the CEO or equivalent officer or any person duly authorised by that officer. Every responsible party must appoint an information officer to ensure compliance by the responsible party with provisions of the Act, and the officer must be registered with the Regulator

Lawful processing

- The heart of POPI is to ensure lawful processing by requiring compliance with with eight the data protection conditions
- Desire to making POPI accessible to all
- Proactive approach adopted :Section 4 and 5 of POPI sets out rights and obligations

Application of POPI

- **Applies to processing of PI**
  - of data subject
  - entered into a record by or for responsible party
  - who is domiciled in the Republic or, where not domiciled in the Republic, makes use of automated or non-automated means to process PI in the Republic (unless used solely to forward PI through the Republic)
  - irrelevant where data subject is domiciled – domicile of responsible party is key
- If **other legislation** contains more extensive provisions regarding the lawful processing of PI, that legislation will prevail otherwise POPI applies

Application of POPI (continued)

General – processing excluded from POPI

- anonimised or de-identified information from which the identity of a data subject cannot be determined
- purely personal use or household activity;
- activity by or for public body involving national security or prevention of unlawful activities;
- processing by Cabinet and its committees or Executive Council of a province;
- processing relating to the judicial functions of a court referred to in section 166 of the Constitution

Application of POPI (continued)

Journalistic Exclusion

- Processing solely for journalistic, literary or artistic expression if exclusion necessary in the public interest, to reconcile right to privacy with right to freedom of expression
- Excluded if responsible party subject to code of ethics with adequate safeguards to protect personal information (the code will apply)

Regulator's power to exempt processing

- Regulator may grant section 37 exemption published by notice in Gazette authorising responsible party to process PI even if breach of condition
- If exemption in public interest which outweighs, to a substantial degree, interference with privacy of the data subject

Data Protection Conditions

- **Condition 1: Accountability**
- **Condition 2: Processing limitation**
- **Condition 3: Purpose Specification**
- **Condition 4: Further Processing Limitation**
- **Condition 5: Information quality**
- **Condition 6: Openness**
- **Condition 7 : Security Safeguards**
- **Condition 8: Data participation**

Conditions for lawful processing of personal information in 3 parts

- Part A: PROCESSING OF PERSONAL INFORMATION IN GENERAL
- Part B: PROCESSING OF SPECIAL PERSONAL INFORMATION
- Part C: PROCESSING OF PERSONAL INFORMATION OF CHILDREN

Conditions for Lawful Processing

CONDITION 1: ACCOUNTABILITY

- Responsible party to ensure conditions for lawful processing

CONDITION 2: PROCESSING LIMITATION

- Lawfulness of processing-there must be a justification
- Minimality and relevance
- Consent or other justification
- Withdrawl of consent
- Collection directly from data subject

CONDITION 3: PURPOSE SPECIFICATION

- Collection for specific purpose
- Retention and restriction of records

Conditions for Lawful Processing

CONDITION 4: FURTHER PROCESSING LIMITATION

- Further processing only permitted if compatible with purpose of collection

CONDITION 5: INFORMATION QUALITY

- Quality of information must be maintained

CONDITION 6: OPENNESS

- Documentation to be kept
- Extensive notification requirements to data subject when collecting personal information

Conditions for Lawful Processing

CONDITION 7: SECURITY SAFEGUARDS

- Responsible party must take measures to secure the integrity and confidentiality of personal information:
- Operator :information processed by or person acting under authority
- Security measures regarding information processed by operator
- Notification of security compromises

CONDITION 8: DATA SUBJECT PARTICIPATION

- Access to personal information
- Correction of personal information
- Manner of access

PROCESSING OF SPECIAL PERSONAL INFORMATION

- **Special Personal Information**" means data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sexual life, biometric information, criminal behaviour – alleged commission by data subject of an offence or any proceedings in respect of this offence
- Prohibition on processing special personal information unless there is :
- Consent
- Processing is required by law
- Historical or research purposes
- Regulator Under exemption
- Authorisation concerning sensitive personal information found in sections 28 to 33
- Prohibition on processing personal information of a child unless there is consent, processing required by law, historical/research purposes, regulator authorizes

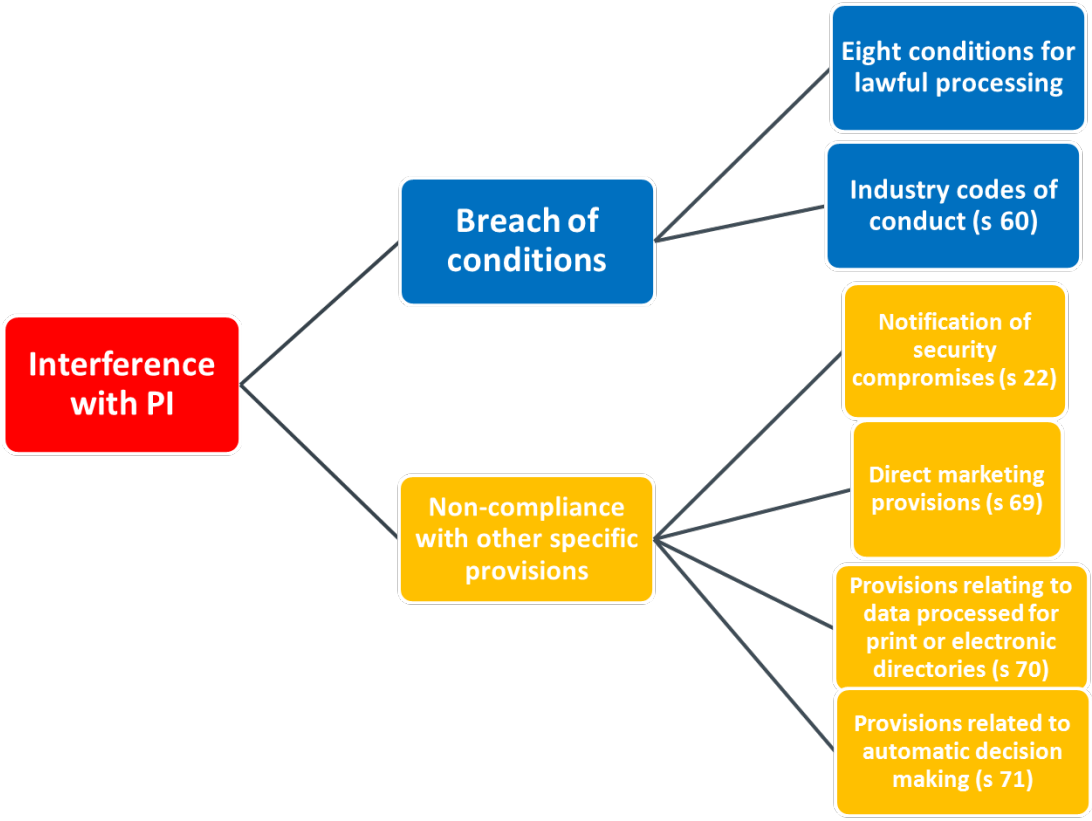
Restrictions on transborder information flows

- A key area of concern in todays global Village :the data protection principle restricting the free flow of personal information across borders;
- limitation is in place because cross-border transfers carry special enforcement risks – particularly where the destination jurisdiction has no data protection law;
- Section 72:Cross-border information transfers are only permitted if justification present: consent, contractual necessity, binding corporate rules or binding agreement or that the recipient of the data is regulated by an adequate of level of data protection, the transfer is beneficial to the data subject and the data subject would be likely to grant consent;
- restrictions on cross-border information flows requires an independent assessment of whether the necessary conditions for a lawful transfer exist.

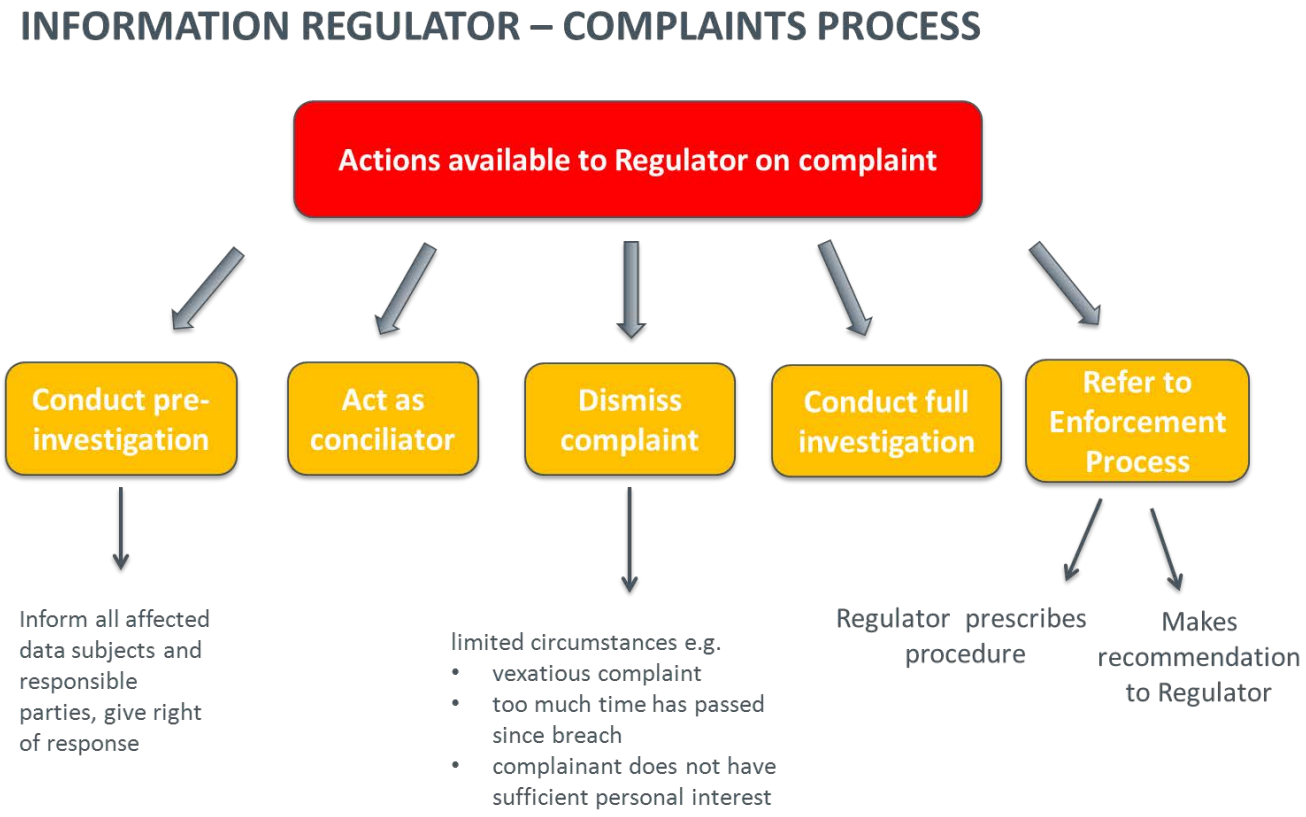
Information Regulator

- New state agency is created by POPI
- Regulator = Chairperson + four others
- Regulator appoints staff & committees
- Must establish Enforcement Committee chaired by judge or senior lawyer

Information Regulator – Complaints Process



Information Regulator – Complaints Process



PENSION LAWYERS ASSOCIATION

WHEN I'M 64

Civil Damages

- Regulator or data subject may sue for damages
- Strict liability for "Interference with PI" – "whether or not intent or negligence"
- Patrimonial and non-patrimonial damages
- Aggravated damages
- Order published in the Government Gazette and media announcement

PENSION LAWYERS ASSOCIATION

Consequences for non-compliance: fines/imprisonment

- Imprisonment not exceeding 10 years and/or a fine
  - Any person who hinders, obstructs or unlawfully influences the Regulator or any person acting under the direction of the Regulator
  - A responsible party who fails to comply with an Enforcement Notice
  - A responsible party who violates conditions of processing of an account number

Consequences of non compliance: fines

- Administrative fines
  - Regulator may issue infringement notice in event of alleged offence
  - Must specify the amount of the administrative fine – may not exceed R10 million
  - Within 30 days of receipt
    - Pay fine;
    - Make installment arrangements to pay fine; or
    - Elect to be tried in court

PENSION LAWYERS ASSOCIATION

Regulatory fines in EU jurisdictions – examples

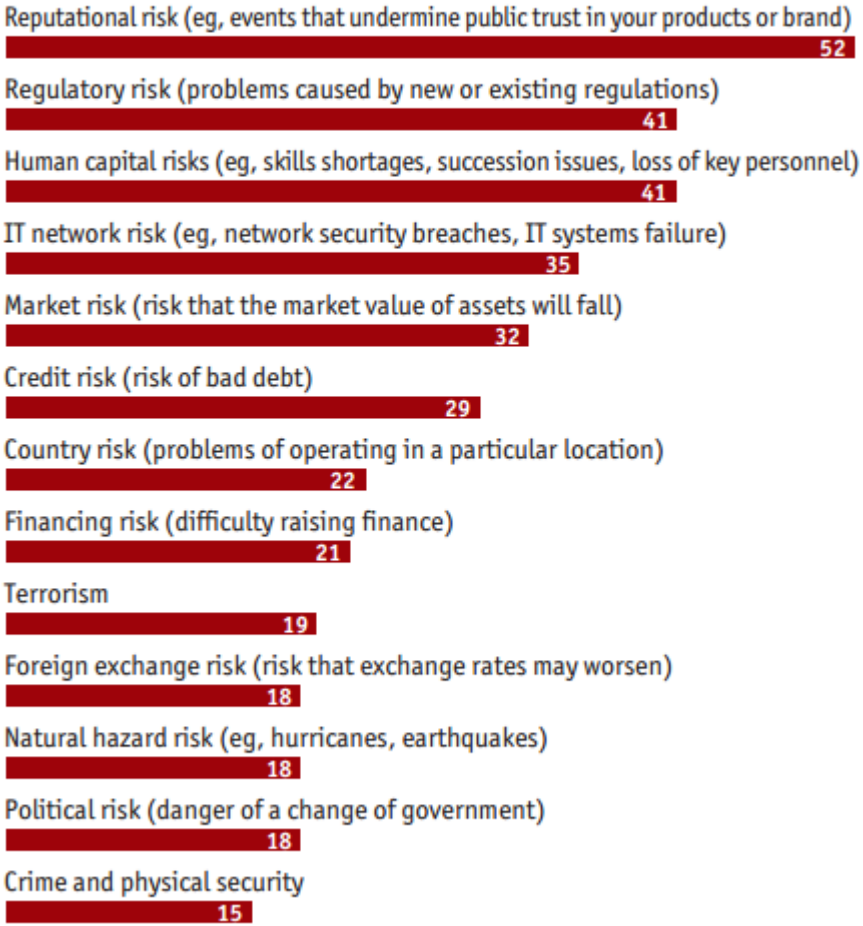
Country	Date	Company	Fine imposed	Reason
UK	Jan 2013	Sony	250 000 GBP	Failure to prevent personal information of Playstation users from being hacked
UK	Oct 2013	The Prudential	50 000 GBP	Mixing up accounts of two customers
UK	May 2012	NHS Trust	325 000 GBP	Failure to prevent special personal information being sold on internet auction site
UK	September 2013	Scottish Borders Council	250,000 GBP	Council's employee 's pension fund records Not properly deleted found in paper recycle bin in supermarket Park

Regulatory fines in EU jurisdictions – examples

Country	Date	Company	Fine imposed	Reason
Netherlands	Dec 2011	Dollar Revenue	1 mil Euros Executives fined in personal capacity	Installing adware/sypware software on 22 million computers
France	July 2011	Association Lexeek	10 000 Euros plus injunction	Published legal cases online which contained parties' names
France	Mar 2011	Google	100 000 Euros	Collection of WiFi and login/email data during Google Street View operations

PENSION LAWYERS ASSOCIATION

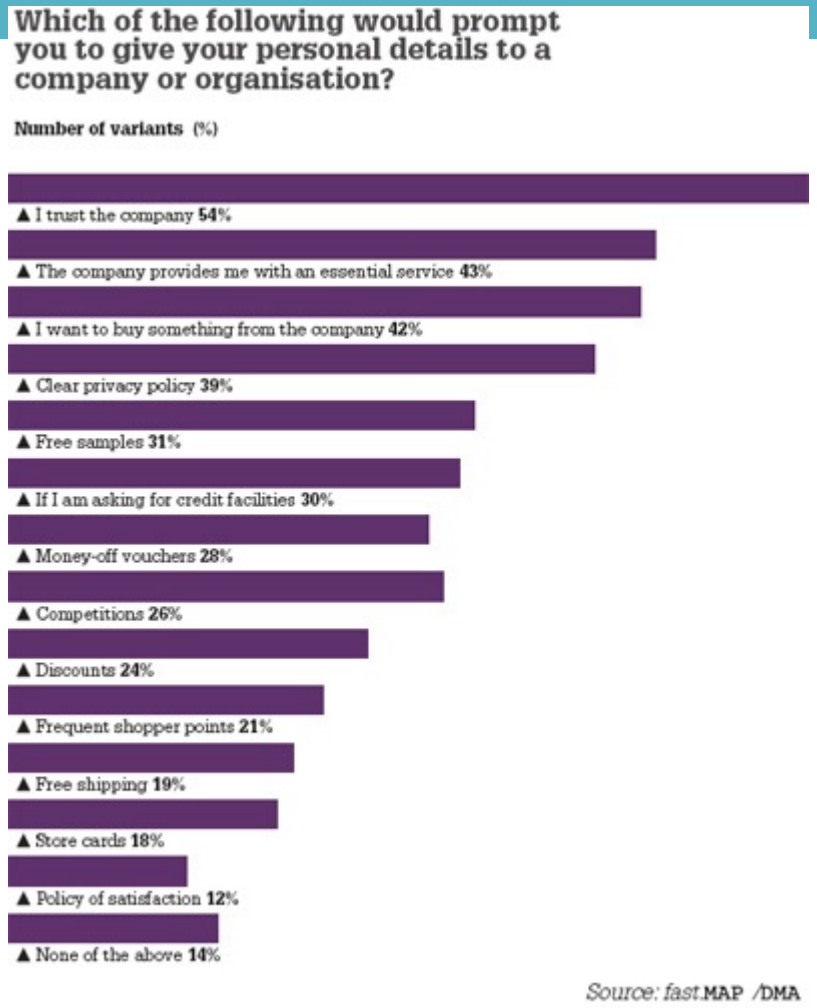
How significant a threat do the following risks pose to your company's global business operation today?
(index score, where 100 = highest)



Source: Economist Intelligence Unit, 2005

To what extent are the following actions a source of reputational risk for your organisation?
(% respondents)

Data protection policies secure consumer trust



Source: fast.MAP /DMA

PENSION LAWYERS ASSOCIATION

WHEN I'M 64

Trustee obligations: what are the risks under POPI

- Reputational risk;
- Members rights under POPI;
- Processing of sensitive personal information from members and dependants;
- Data security breaches;
- Transfers of PI to third parties within and outside South Africa;
- Operators : proper due diligence and adequate contracts;
- Direct marketing – strictly regulated

Operators

- **Operators** process personal information for responsible parties must act in terms of a contract or mandate and must:
  - process information only with knowledge or authorisation of responsible party;
  - treat personal information as confidential and not disclose unless required by law or in course of the proper performance of their duties;
  - implement security measures that meet the standard set in POPI;

Security Measures

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

- loss of, damage to or unauthorised destruction of personal information; and
- unlawful access to or processing of personal information.

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

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented and ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards;
- 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.

Trustee obligations : Outsourcing

- Ensure that adequate written contracts are in place and are reviewed from a data protection perspective. There are mandatory clauses that have to be included wherever processing of personal information, such as pension fund member information, is outsourced;
- Seek warranties on technical and organisational security measures protecting the records;
- Always work with a reputable organisation and ensure that it only acts on your instructions;
- Make sure the organisation has appropriate data security measures in place, including how it disposes of data and ensure you have recorded your checks in the event of any future dispute;
- Make sure the organisation has appropriate security checks on the reliability of staff
- Make sure that contract requires the contractor to report any security breaches or other problems to you, and have procedures in place on how you will act if problems are reported;
- Transfers outside of the SA are generally prohibited, therefore trustees should seek legal advice on the additional requirements imposed on them in this situation.

Trustee Obligations: Members

- **Must ensure lawful processing of members PI:**

  Accountability/ processing limitation/ purpose specification/ further processing limitation/ information quality/ openness/ security safeguards/ data subject participation

- **Conditions for processing special PI must be in place:**

  consent or other justification, also confidentiality imposed by POPI

Trustee Obligations: dependants

- Section 32 :The prohibition on processing personal information concerning a data subject's health or sex life does not apply to the processing by –
- administrative bodies, pension funds ,employers or institutions working for them if such processing is necessary for-
- the implementation of the provisions of the laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject;
- Confidentiality is however imposed
- Consent?

Trustee Obligations: dependants

- Same obligations as for members for lawful processing;
- Section 37C of the PFA imposes an obligation on trustees to make an equitable distribution- personal and sensitive PI from potential dependants is processed :
    - Birth, origin, marriage, age, pregnancy, employment, education, financial, culture, physical or mental well-being, disability, origin
    - Health, medical ,sex life and religion.
- Original purpose and further processing conditions apply to PI
- Special PI – section 32 authorisation, but confidentiality imposed.

Practical steps to ensure compliance

Introduction

- Key steps:
  - Appointing/ designating an information officer;
  - Processing and compliance audit;
  - Identify responsible persons within a group;
  - Identify operator;
  - Ensure that appropriate legal grounds exist for each processing activity;
  - Ensure data/information security;
  - Privacy notifications, terms and conditions, policies and procedures.

PENSION LAWYERS ASSOCIATION

Information Officer

- Sec 55 – every responsible party must appoint information officer
- Information officer has the same meaning as in PAIA, being the CEO or equivalent officer or any person duly authorised by that officer
- Ensuring compliance by the responsible party with provisions of the Act
- Has to be registered with the Regulator

PENSION LAWYERS ASSOCIATION

Processing and compliance audit

- Identify all the collection points of personal information, e.g. websites, application forms, call centres, employment application forms etc.
- Identify personal information being collected and whether it is being collected directly from the data subject or via a third party;
- Identify all purposes for processing, all internal and external access ,and possible disclosure;
- Ensure lawful processing is implemented at the point of collection

PENSION LAWYERS ASSOCIATION

Review Policies and Procedures

- Privacy policies and processing notices
  - Should be clear on purposes for which personal information will be used/processed,and include all the information that is required under the Openness Condition- Condition 6
  - Deal with Marketing;
  - Processing by third parties ;
  - Will there be cross-border transfers?;
  - I agree
  - Use of cookies
- Other corporate policies such as information security policy, information collection policy and procurement procedures should include data protection provisions
- Standard Clauses in Contracts where personal information iscollected

PENSION LAWYERS ASSOCIATION

Data Subject Access Requests and Investigations

- Information officer should be made responsible for this, same person as designated for PAIA requests;
- Standard procedures should be set out
- Data subjects should be informed of their rights

PENSION LAWYERS ASSOCIATION

Thank you

PENSION LAWYERS ASSOCIATION