

Actuaries and the Protection of Personal Information Act

Unraveling the strings...



ASSA SESSIONAL – NOVEMBER 2020

CHAIRING:

STEPHEN WALKER: RETIREMENT FUND VALUATOR
OLD MUTUAL CORPORATE CONSULTANTS

SPEAKER:

LEANNE VAN WYK: DIRECTOR
ICTS LEGAL SERVICES (PTY) LTD

Why should I care about POPIA?

Because I have a reputation to protect (breaches of this Act will be high profile)

Because if I get it wrong it's going to cost time and money

Because I could be instructed to stop processing personal information

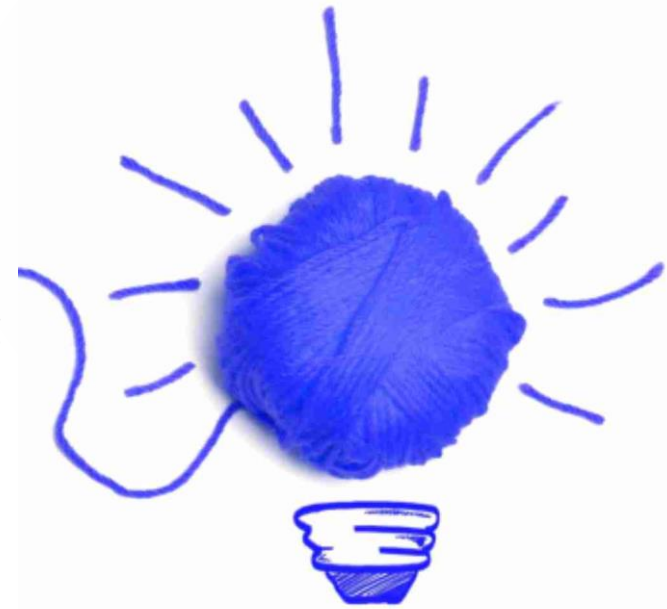
Fines, penalties (up to R10 million), imprisonment, etc

Streamline processes and do things I know I should be doing anyway (house-keeping)

Because I want to protect the personal information of members

Because it's law

COFI Governance Principles – include principles relating to personal information, especially safety and security (and sometimes even refer to POPIA)





POPIA dates – how long have I got?

Commencement date is

1 July 2020

One year grace period before
the Information Regulator will
start enforcing POPIA i.e. until

30 June 2021

What is being protected by POPIA and when does it apply?

- ▶ POPIA is aimed at protecting people's personal information and will regulate all processing of personal information
- ▶ Principle-based legislation

POPIA applies when there is:

Processing of personal information, in a record by (or for) a Responsible Party

A quick run down on terminology



POPIA applies when there is **processing** of **personal information**, in a record by (or for) a **Responsible Party**

Personal information: is a very wide concept and basically includes anything about a natural, living person (and others like a company or a fund) - includes information about a person's race, gender, marital status, ethnic or social origin, age, physical or mental health, language, religion, education, medical, financial, criminal or employment history, contact details, biometric information, personal opinions, views or preferences and confidential correspondence

Living human beings or existing organisations that are capable of being identified, which means that Personal Information excludes de-identified information

Processing: is very widely defined and includes the collection, collation, storage, use, erasure, destruction alteration or distribution of a record which has personal information in it. Basically, anything that is done with personal information from the time it is incepted to the time it is destroyed is processing

▶ A **record:** is any form of recorded information, whether electronic, written, graphical or diagrammatic. For example your electronic records, paper records, an x-ray or even a photo

What does it mean to de-identify information?

Often data that actuaries use will not be identifiable back to a specific person and you don't need it to be able to do the work

This goes some way to reducing the amount of personal information you are dealing with

Personal information must be properly de-identified as required under POPIA

Cases overseas dealing with this, as well as regulatory guides on how to de-identify information and when it is de-identified.

If the bits of data can be put together in such a way that an individual can be identified from it, the data will constitute personal information and POPIA will apply to it

“de-identify”, in relation to personal information of a data subject, means to delete any information that—

- (a) identifies the data subject;
- (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and **“de-identified”** has a corresponding meaning;

What does it mean to de-identify information?

Big Data threatens de-identification, because of the huge amounts of data involved. The cumulative effect of large amounts of data is that it is much more likely that de-identified data sets can be matched with personal information, so data can be re-identified

ACTUARIES
DIGITAL

2014, Australia

De-identification of data has long been proclaimed as an effective means of safeguarding privacy, and side-stepping the obligations imposed by privacy laws – de-identified data is not ‘personal information’ to which the laws apply. Today, however, with unprecedented volumes of data being available, it is uncertain as to how effective de-identification is, and will continue to be in keeping data anonymous. With more and more data in the hands of data processors, it is more and more likely that de-identified data will be capable of being ‘re-identified.’⁶

How reasonably foreseeable is it that the information can be re-identified? It may be technically possible for data to be re-identified, but so complicated and time consuming that it is not a practical possibility

In assessing the likelihood of de-identified data identifying an individual, factors such as cost, difficulty, practicality and likelihood of re-identification could be taken into account

“**de-identify**”, in relation to personal information of a data subject, means to delete any information that—

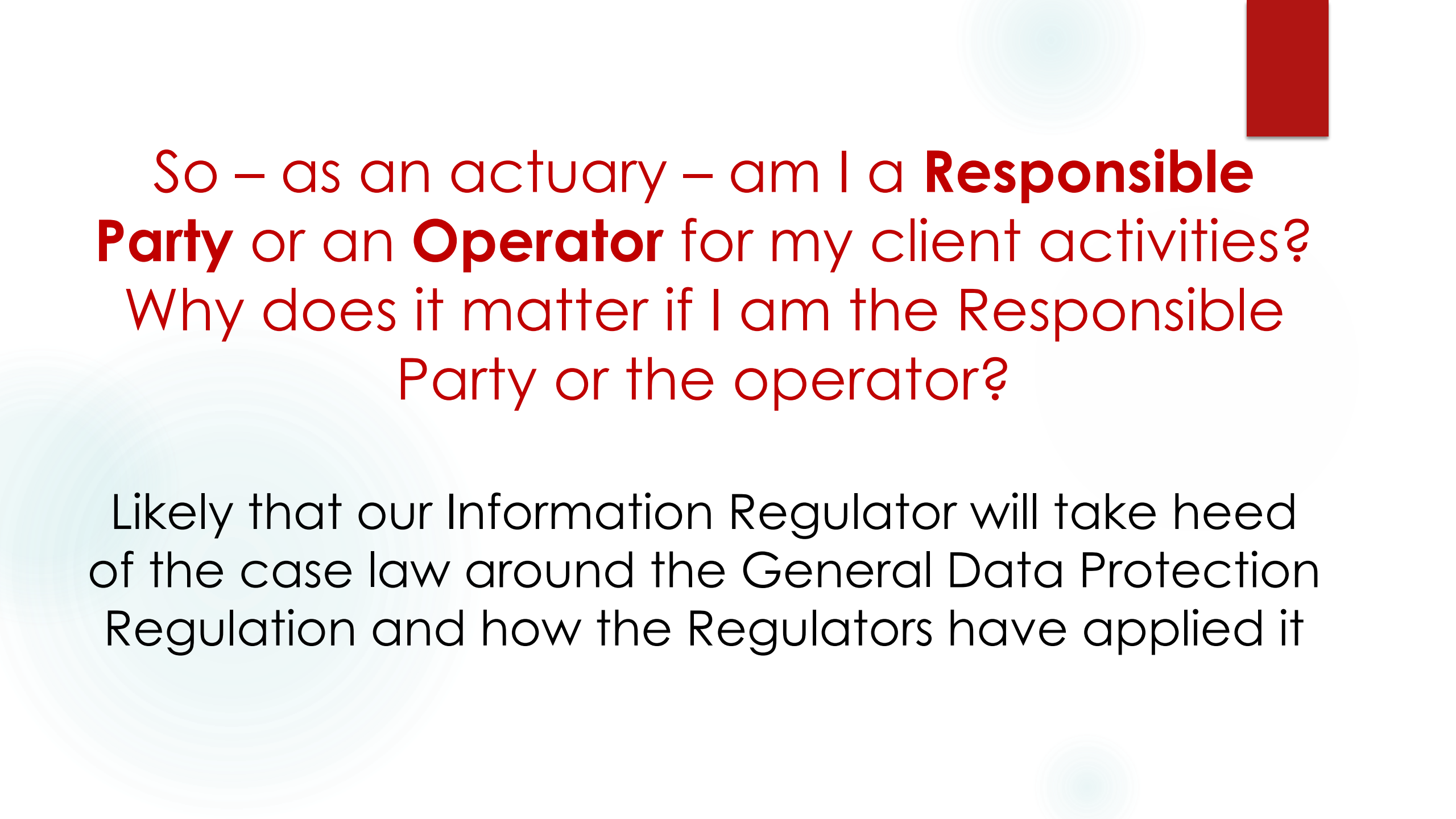
- (a) identifies the data subject;
- (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and “**de-identified**” has a corresponding meaning;

What types of processors of personal information are there?

The processor is the person who is processing the personal information. They are either:

- The **responsible party** – if they are the only person or organisation involved in the activity or they are determining **why** (purpose for) the personal information is being processed, how, means of and when e.g. fund and employer
- The **operator** – if they are processing on behalf of the responsible party in terms of contract, agreement, or mandate without coming under their direct authority (even if they are determining how to process the person information, under certain circumstances).
- An operator may process personal information only with the *knowledge and authorisation* of the responsible party, unless otherwise required by law or in the course of the proper performance of its duties



So – as an actuary – am I a **Responsible Party** or an **Operator** for my client activities?
Why does it matter if I am the Responsible Party or the operator?

Likely that our Information Regulator will take heed of the case law around the General Data Protection Regulation and how the Regulators have applied it

The Responsible Party

- If we are the **responsible party (RP)** then we *bear the lion's share of having to comply with POPIA*
- RP must **satisfy the eight conditions (plus other requirements)** to lawfully process personal information upfront and every time it processes personal information
- Must also **ensure that its operators comply** with the eight conditions (and other requirements) when it processes personal information
- Enter into a **written agreement** with our operators
- **Operators** have much fewer legislative requirements

- So responsible parties are only going to want to deal with operators who are POPIA compliant, because they are responsible for operator's actions
- May require contractual undertakings
- May require ongoing assurances

The **responsible party always remains responsible** for the processing of information

An operator's responsibilities

Secure the personal information. Establish and comply with security measures provisions

Only process information as agreed with the responsible party

Have 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

Simplified example – fund payment of a benefit

Responsible Party



FUND

Operator



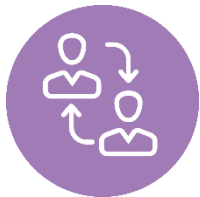
ADMINISTRATORS

Data subjects



MEMBERS/BENEFICIARIES

Example 1 – 37C death benefit process



Employer does investigation and report

FUND'S OPERATOR



Fund makes allocation decision

RESPONSIBLE PARTY



Administrator pays benefit

FUND'S OPERATOR



Beneficiaries

DATA SUBJECTS

Example 2 –contributions and schedules



Employer pays contributions and provide schedules

RESPONSIBLE PARTY



Fund receives contributions and invests them

RESPONSIBLE PARTY



Administrator administers contributions

FUND'S OPERATOR



Investment manager invests fund assets obo fund

OPERATOR PROBABLY



members

DATA SUBJECTS

Fund is a Responsible Party for most of its activities

Employer – both Responsible Party (e.g. payment of contributions) and Operator (e.g. death benefit investigations)

Administrator – for fund activities – is an operator

Investment manager – for fund activities – probably an operator

But what about the actuary to, or valuator of, a fund?

“responsible party” 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;

RESPONSIBLE PARTY



VALUATOR

Statutory
relationship

RESPONSIBLE PARTY



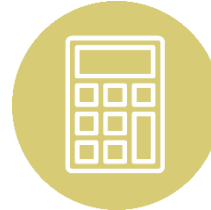
FUND

Contractor
relationship

Contractual
relationship

OR

RESPONSIBLE PARTY



ACTUARY

RESPONSIBLE PARTY



ACTUARIAL/ INSURANCE/
ETC COMPANY

Employment
relationship



ACTUARY

Employee, not
responsible party

Types of actuarial relationship with a fund:

Employee of company
appointed by the fund

Valuator of fund (personal
capacity)

Contractor (actuarial services)
to the fund (personal
capacity)

What types of action can be taken against a Responsible Party?

- ▶ **Civil action** – in a court, instituted by a data subject or the regulator at the request of a data subject (damages, aggravated damages, interest and costs of suit could be ordered by the court)
- ▶ **Criminal prosecution** for an offence by the state – on conviction by a court - imprisonment and/or a fine
- ▶ **Infringement notice** by the regulator (up to R10 million) for an alleged offence under POPIA
- ▶ **Assessment** by the regulator of whether a specific instance of processing of personal information complies with POPIA
- ▶ **Information notice** by the regulator to a responsible party requiring reports and information. Information can be made public by the regulator
- ▶ **Enforcement notice** issued by the regulator which includes the right of the regulator to instruct the responsible party to stop processing personal information specified in the notice, for a purpose, or in a manner specified in the notice.

In the GDPR world, actuaries are (mostly) Responsible Parties

- The {Responsible Party} determines the purposes for and the manner in which personal data is processed. This means that the {Responsible Party} exercises overall control over the 'why' and the 'how' of a data processing activity
- Funds use specialist service providers such as lawyers to provide them with legal advice, and actuaries to provide advice on scheme funding, consultants on investment matters etc.
- The Information Commissioner's Office (ICO), - the UK's data protection authority - suggests that the fund may not have sole {Responsible Party} responsibility, even though it initiated the work by asking for advice or commissioning a report
- Responsibility also lies with the specialist service provider, which is subject to professional, ethical and legal obligations and consequently itself often determines what information to obtain and process in order to do the work
- So actuaries and lawyers have been seen as {Responsible Parties} and not {Operators} in the fund context

MERCER PRIVACY NOTICE RELATING TO ACTUARIAL SERVICES

This Privacy Notice covers the following areas:

- (1) Our status
- (2) Information we collect about you
- (3) How we use your personal information
- (4) Who we share your personal information with
- (5) How we protect your personal information
- (6) Your rights
- (7) Contacting us
- (8) Changes to our Privacy Notice



Data Controller = Responsible Party



Data Processor = Operator

(1) Our status

When we process your personal information in connection with the actuarial services we provide, we act as independent data controllers alongside relevant trustees or participating employer of your pension scheme (as applicable) to whom we are providing our services who also act as data controllers. We work with our trustee or employer clients to meet our respective obligations under data protection law.

Where a Mercer scheme actuary has been appointed in respect of your pension scheme, the relevant scheme actuary will also act as a data controller in relation to your personal information that he or she processes. To the extent applicable, the information in this Privacy Notice also applies to the processing of your personal information by the scheme actuary. To find out the identity of the relevant scheme actuary, please contact the Trustees of your pension scheme.

This Privacy Notice only applies in relation to the processing of personal information that we undertake as a controller in relation to our actuarial services. It does not apply to activities that we perform as a processor on behalf of our clients (such as pension scheme administration services). Details of such processing will be set out in the privacy notice of your relevant pension scheme trustee and/or employer.

How Willis Towers Watson uses personal data when it provides actuarial services to UK pension scheme trustees

Willis Towers Watson 

When we process your Personal Information, we act as controllers together with the Trustees and we cooperate with the Trustees in meeting our compliance obligations under the law. For example, it is the Trustees' responsibility to notify data subjects about the use of their Personal Information (as described in this privacy notice); to ensure the accuracy of the Personal Information they provide to us for processing; and to handle requests received from data subjects.

This privacy notice does not apply to any services where we act as a processor on behalf of the Trustees, for example when we provide pensions administration services.

Choices and Access

Willis Towers Watson, the Scheme Actuary, and the Trustees are each controllers responsible for the Personal Information that we process.

5. Will any advisers to the trustees be data controllers and, if so, do we need to send them a data processing questionnaire?

The ICO's guidance confirms that it regards legal advisers as data controllers as they determine how data received in relation to an individual will be processed to allow them to enforce their legal rights. The scheme actuary will also be a data controller for the same reason. Others (for example life assurance providers, DC platform providers) may accept that they are data controllers in relation to at least some of the services provided.



Data Controller = Responsible Party



Data Processor = Operator

If I am a Responsible Party – what do I
have to comply with?



The Eight Conditions and other requirements

POPIA contains eight general protection conditions (see your pre-reading)

Plus other requirements

It is important to know that while POPIA sets out the principles, it also sets out many circumstances when a responsible party does not have to comply with the principles (i.e. “justifications”)

You must do this ... unless ...



The Eight POPIA Conditions for Responsible Parties



The Eight POPIA Conditions for Responsible Parties

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.

2 Processing of PI: Minimality

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

2 Processing of PI: Consent and justification

- Data subject consent 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.

2 Processing of PI: Collection from data subject

Personal Information must be collected directly from the data subject.

3 Purpose: Collection for a specific purpose

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

3 Purpose: Retention, destruction and restriction 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.

4 Further processing Limitation

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

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 Openness - documentation

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

6 Openness - notification when collecting

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

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.

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 Notification 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.



It is important
to understand
the concept
of “purpose”

The Eight POPIA Conditions for Responsible Parties

Condition Three - Purpose

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
- Personal Information can only be collected for a specific, explicitly defined, lawful purpose that is related to a function or activity that we perform
- We have to know our purposes for processing personal information
- The Responsible Party must ensure that the data subject know about the purposes (unless there is a justification)
- When? Logically it must be *before* the personal information is collected, but not too long before. The best time is probably when the personal information is being collected
- Creates need for manual/policy/notice (external doc)

What personal information may I process?



The Eight POPIA Conditions for Responsible Parties

Condition Two – Processing

2

Processing of PI: Minimality

Given the purpose for which personal information is processed, the processing is **adequate, relevant and not excessive**

Given the purpose for which we are processing personal information, we can only process personal information if it is **adequate, relevant and not excessive**

- Only process personal information in a way that connects correctly, or relates suitably to your purposes
- Don't process personal information for more than your purposes
- Don't process more personal information than you need to for the purposes
- Don't collect more personal information that you need – but ensure you collect what you need
- Don't process more personal information than you communicated you would or for a purpose you did not communicate

Special Personal Information and Children's personal information have extra requirements

I have heard that I always need to get the consent of data subjects before I process personal information, is this correct?



The Eight POPIA Conditions for Responsible Parties

Condition Two – Processing

2

Processing of PI:
Consent and
justification

- To process personal information the Responsible Party needs data subject consent OR rely on one of the following:
 - 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

- The Fund may only process personal information if the data subjects consent or one of the above exist
- Not practical for funds to rely on consent
- Risky to rely on consent – can be withdrawn at any time and may need renewing
- Data subject can object
- In my view, the actuary is going to process because it is pursuing its or the fund's legitimate interests (performing the activities we are expected to perform) and we therefore don't need consent (but need to look at specific purposes/activities)

Identify
Document
Communicate

Establishing legal basis for processing personal information example



Legal basis

All processing (i.e. use) of your personal information is justified by a "lawful basis" for processing. In the majority of cases, processing will be justified on the basis that:

- the processing is necessary for the performance of a contract to which you are a party, or to take steps (at your request) to enter into a contract (e.g. where we help an employer to fulfil an obligation to you under an employment contract in relation to the delivery of employee benefits);
- the processing is necessary for us to comply with a relevant legal obligation (e.g. where we are required to collect certain information about our clients for tax or accounting purposes, or where we are required to make disclosures to courts or regulators); or
- the processing is in our legitimate commercial interests, subject to your interests and fundamental rights (e.g. where we use personal information provided to us by our clients to deliver our services, and that processing is not necessary in relation to a contract to which you are a party).

In limited circumstances, we will use your consent as the basis for processing your personal information, for example, where we are required to obtain your prior consent in order to send you marketing communications.

Before collecting and/or using any special categories of data, or criminal record data, we will establish a lawful exemption which will allow us to use that information. This exemption will typically be:

- your explicit consent;
- the establishment, exercise or defense by us or third parties of legal claims; or
- a context specific exemption provided for under local laws of EU Member States and other countries implementing the GDPR, such as in relation to the processing of special category data for insurance purposes, or for determining benefits under an occupational pension scheme.

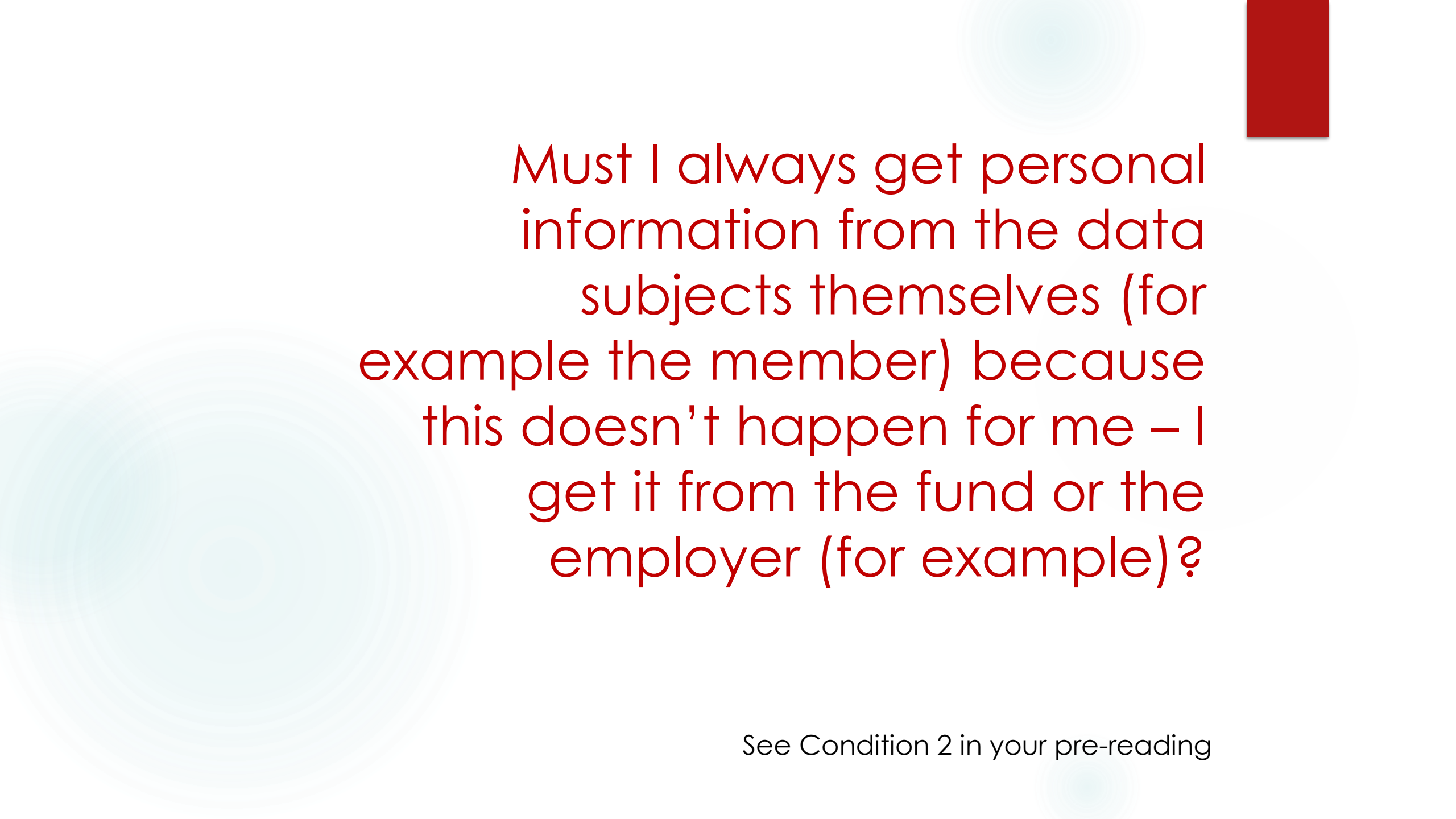
Establishing legal basis for processing personal information example

WillisTowersWatson 

Legal Bases for Processing Personal Information

We must have a legal basis to process your Personal Information. In most cases the legal basis will be one of the following:

- for our legitimate interests, for example to provide Services to the Trustees, to ensure that the Services we provide are appropriate to the Trustees' requirements, to improve our Services, manage our risks, maintain accurate transaction records, and manage our business in an efficient way;
- for the legitimate interests of the Trustees and other third parties (for example, to investigate and assess claims made against policies held or underwritten by them and to prevent and detect suspicions of fraud); or
- to comply with our legal and professional obligations, such as due diligence and reporting obligations.



Must I always get personal information from the data subjects themselves (for example the member) because this doesn't happen for me – I get it from the fund or the employer (for example)?

See Condition 2 in your pre-reading

The Eight POPIA Conditions for Responsible Parties

Condition Two – Processing

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 actuaries receive personal information from the fund or that the fund has received from the employer, not the data subject (e.g. member) themselves

Justification for not complying with this Condition:

- (a) Consent (X)
- (b) collection from another source would not prejudice a legitimate interest of the data subject
- (c) Collection from another source is required to comply with an obligation imposed by law
- (d) To maintain the legitimate interest of the fund

Identify
Document
Communicate



What must I do if I see that for some of
my activities I am not complying with
the eight conditions or other
requirements?

I could get authorisation from the Information Regulator

I could check if there are any Codes of Conduct that apply

I could check if the Information Regulator has set any specific rules

But before all of the above – I must check POPIA for justifications

Justifications

The Conditions and other requirements are often set out in the form of the condition/ rule/ principle and then a list of justifications after that particular rule - which give you a list of circumstances when you don't have to follow the rule

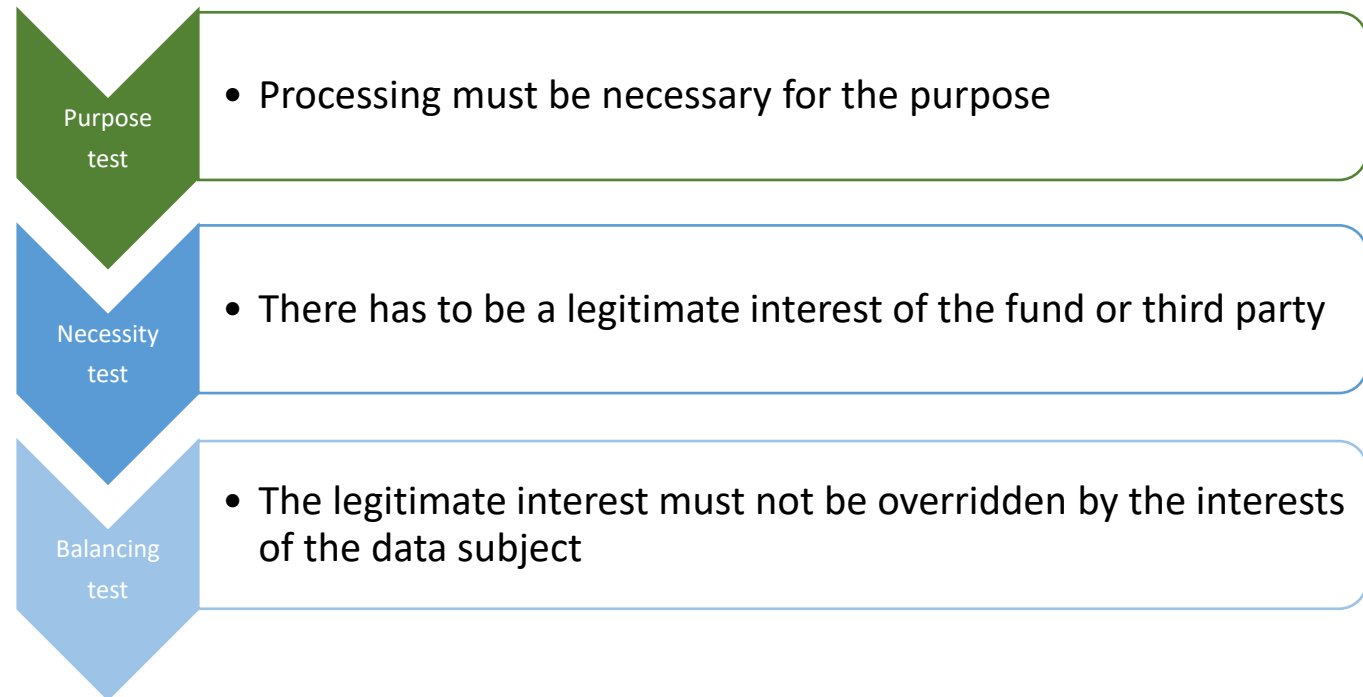
Examples of justifications for not complying with conditions:

- In the legitimate interest of the data subject
- If complying with an obligation in law
- In the legitimate interest of the Responsible Party or a third party
- Consent of the data subject

There are a number of instances in POPIA where we can use the justification of legitimate interest to process personal information that we would not otherwise have been able to process without, for example, getting the consent of the data subject or the Information Regulator

Examples of where we can use the 'legitimate interest of the responsible party or a third party' justification (both of which are relevant to retirement funds)

- Requiring the consent of the data subject to process their personal information (Condition 2)
- Processing personal information that we have not got from the data subject themselves (Condition 2)

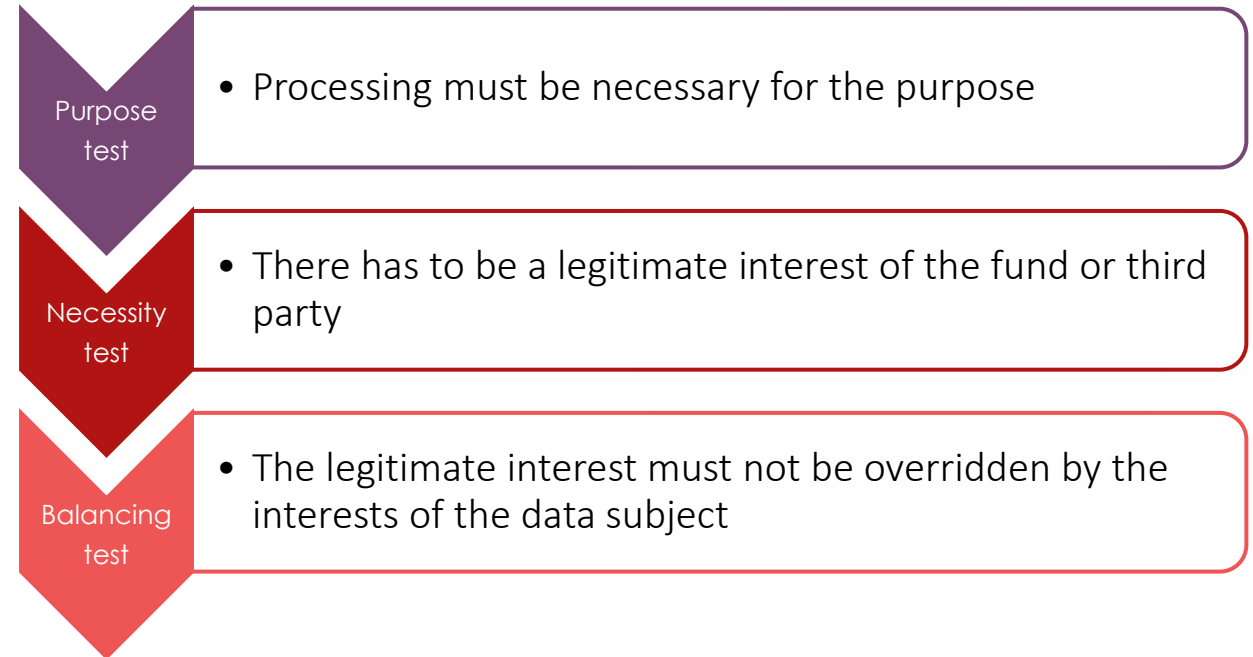


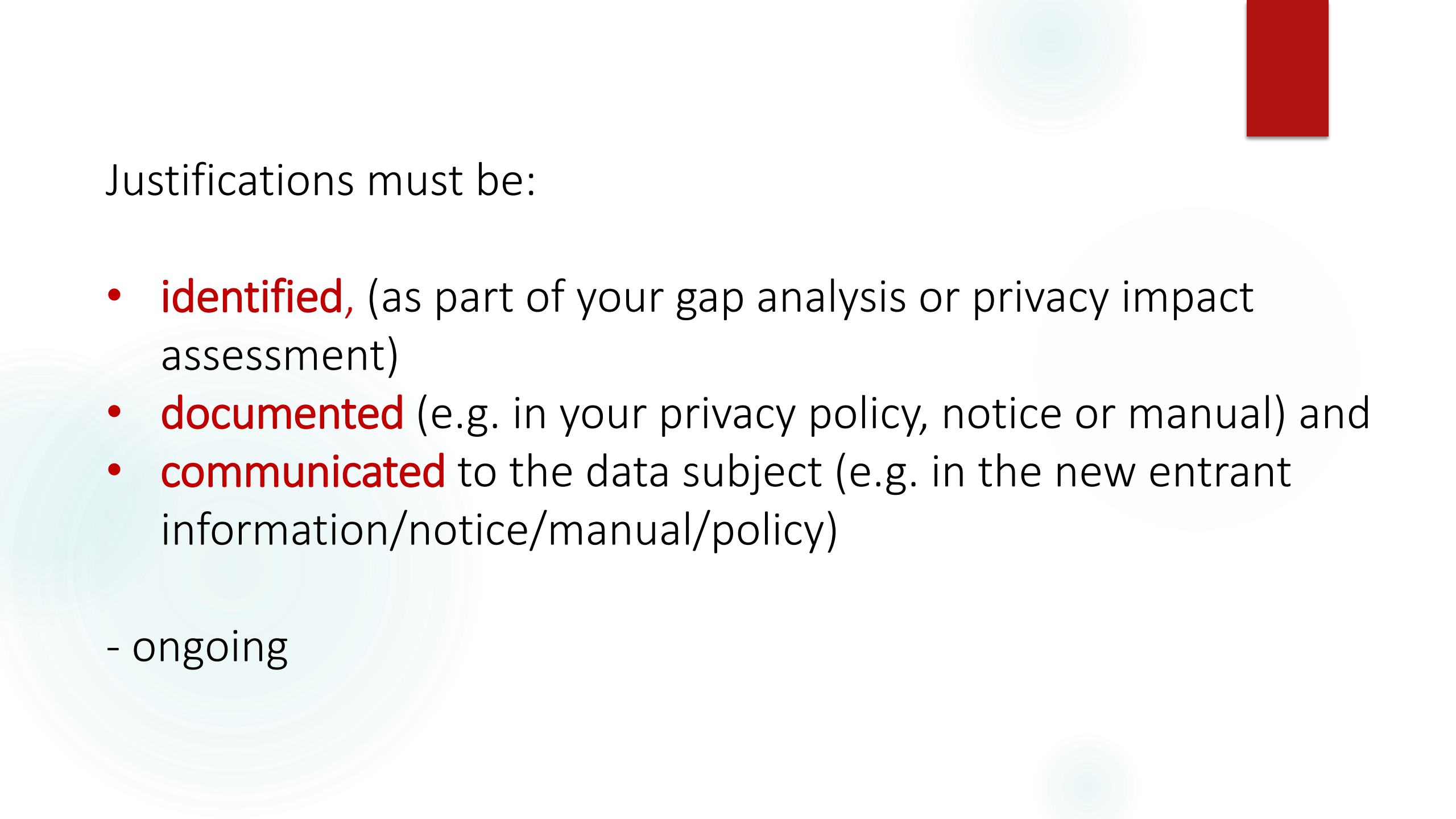
The legitimate interest test

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 the following test which looks at purpose, necessity and balance (until such time as the Information Regulator or our courts determine a different test):

- ▶ (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 pass the test where the processing is unwanted by the data subject
- A relevant and appropriate relationship between the parties will also assist – fund actuary and member would be a relevant and appropriate relationship
- Balancing the data subject’s interest includes taking measures to protect their privacy rights





Justifications must be:

- **identified**, (as part of your gap analysis or privacy impact assessment)
- **documented** (e.g. in your privacy policy, notice or manual) and
- **communicated** to the data subject (e.g. in the new entrant information/notice/manual/policy)

- ongoing

MERCER PRIVACY NOTICE RELATING TO ACTUARIAL SERVICES

(3) How we use your personal information

This section sets out the purposes for which we use personal information that we collect and, in compliance with our obligations under European data protection law, identifies the “legal grounds” (or “use justifications”) which we rely on to process the information (the full description of each of these grounds can be found [here](#)).

We may use your personal information for the following purposes:

(a) **Benefit strategy and design and to assist in running the scheme:** To advise in relation to the running of our clients’ pension arrangements, including assessing the relevant pension requirements. We also advise on the financial implications of pension arrangements and proposed changes to them and advise on the design and financing of disability income schemes and risk benefit schemes. This activity also includes providing advice to certain executives / high earners and others with benefits above the Lifetime Allowance;

Use justification: legitimate interests (to enable us to perform our contractual obligations), legal obligation. In the limited circumstances where we are required to process Special Category Personal Data, we may rely on substantial public interests (namely that it is necessary for making determinations in connection with the occupational pension scheme) or will rely on your explicit consent.

(b) **Accounting:** To prepare calculations in respect of our clients’ pension scheme and post-retirement medical benefit accounting numbers.

Use justification: legitimate interests (to enable us to perform our contractual obligations), legal obligation.

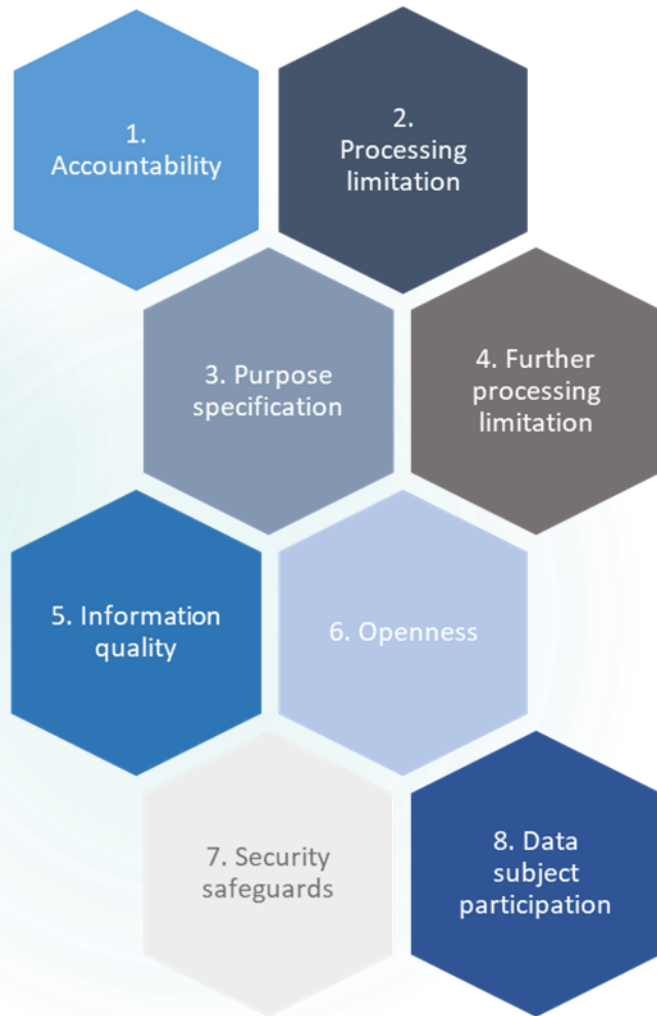
(g) **(To communicate effectively with our clients:** To conduct our business, including to respond to our clients’ queries and to otherwise communicate with our clients, including to inform them of changes to our services and products and to handle claims.

Use justification: legitimate interests (to enable us to perform our obligations and provide our services to you), legal obligations, legal claims.

(h) **To reorganise or make changes to our business:** To share data as part of any due diligence process, or following a sale or reorganisation, in the event that we: (i) are subject to negotiations for the sale of all or part of our business to a third party; (ii) are sold to a third party; or (iii) undergo a reorganisation.

Use justification: Legitimate interests (in order to allow us to change or business).

What are the other requirements besides from the 'Eight' Conditions?



The Eight Conditions plus other requirements



What is Special
Personal Information
and may I continue
to process it?



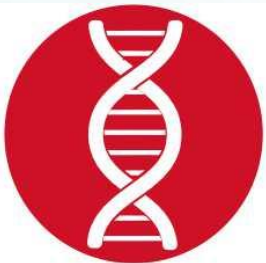
Special Personal Information

We may not process Special Personal Information unless specifically permitted by POPIA or if authorised by the Information Regulator

The classes of Special Personal Information are:



RELIGIOUS/
PHILOSOPHICAL
BELIEFS



RACE/ETHNIC
ORIGIN



TRADE UNION
MEMBERSHIP



POLITICAL
PERSUASION



HEALTH



SEX LIFE



BIOMETRIC
INFORMATION



CRIMINAL
BEHAVIOUR

Special Personal Information

Grounds for processing SPI

- ▶ A responsible party generally may not process special personal information. But, it may process special personal information if it has grounds that justify it doing so:
- ▶ There are general grounds authorising us processing special personal information and there are more specific grounds for each type of special personal information that may authorise us processing that type of special personal information

Special Personal Information –general grounds

The general grounds are:

Nothing particularly useful to us,
except legal reasons

- ▶ **Data subject's consent** – the data subject has consented to the processing
- ▶ **Legal reasons** – processing is necessary to establish, exercise, or defend a legal right or obligation
- ▶ **International legal reasons** – processing is necessary to comply with an international public law obligation
- ▶ **Public interest informational reasons** – processing is necessary for historical, statistical, or research purposes and serves a public interest
- ▶ **Informational reasons where consent is difficult or impossible** – processing is for historical, statistical, or research purposes and consent is difficult or impossible (provided that there are sufficient guarantees to make sure that the processing does not affect the data subject's privacy more than it needs to)
- ▶ **Public information** – the data subject has deliberately made the information public
- ▶ **Special personal information authorisation** – the responsible party is authorised to process the special personal information in terms of a specific ground

Special Personal Information: specific grounds example:

Authorisation concerning data subject's health or sex life

32. (1) The prohibition on processing personal information concerning a data subject's health or sex life, as referred to in section 26, does not apply to the processing by—

- (a) medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;
- (b) insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for—
 - (i) assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing;
 - (ii) the performance of an insurance or medical scheme agreement; or
 - (iii) the enforcement of any contractual rights and obligations;
- (c) schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;
- (d) any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;
- (e) any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or
- (f) administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for—
 - (i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or
 - (ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

(2) In the cases referred to under subsection (1), the information may only be processed by responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject.

(3) A responsible party that is permitted to process information concerning a data subject's health or sex life in terms of this section and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, must treat the information as confidential, unless the responsible party is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information in accordance with subsection (1).

(4) The prohibition on processing any of the categories of personal information referred to in section 26, does not apply if it is necessary to supplement the processing of personal information concerning a data subject's health, as referred to under subsection (1)(a), with a view to the proper treatment or care of the data subject.

(5) Personal information concerning inherited characteristics may not be processed in respect of a data subject from whom the information concerned has been obtained, unless—

- (a) a serious medical interest prevails; or
- (b) the processing is necessary for historical, statistical or research activity.

(6) More detailed rules may be prescribed concerning the application of subsection (1)(b) and (f).

Regulator will probably issue Rules around this - may be helpful

If I want to transfer personal information outside South Africa, can I do that and what do I need to do?

- ▶ We may not transfer personal information about a data subject **outside the country** unless we comply with specific requirements

- ▶ Country
- ▶ Agreements
- ▶ Binding corporate rules

Remember data stored in the cloud

SOLUTIONS ▾PLANS & PRICINGCONTACT SALESJOIN A MEETINGHOST A MEETING ▾SIGN IN

International Transfers

Zoom operates globally, which means personal data may be stored and processed (for example stored in a data center) in any country where we or our service providers have facilities or hold events. By using Zoom or providing personal data for any of the purposes stated above, you acknowledge that your personal data may be transferred to or stored in the United States or in other countries around the world. Such countries may have data protection rules that are different and less protective than those of your country.

If you are a resident of the European Economic Area (EEA), and your personal data is transferred outside of the EEA, we will:

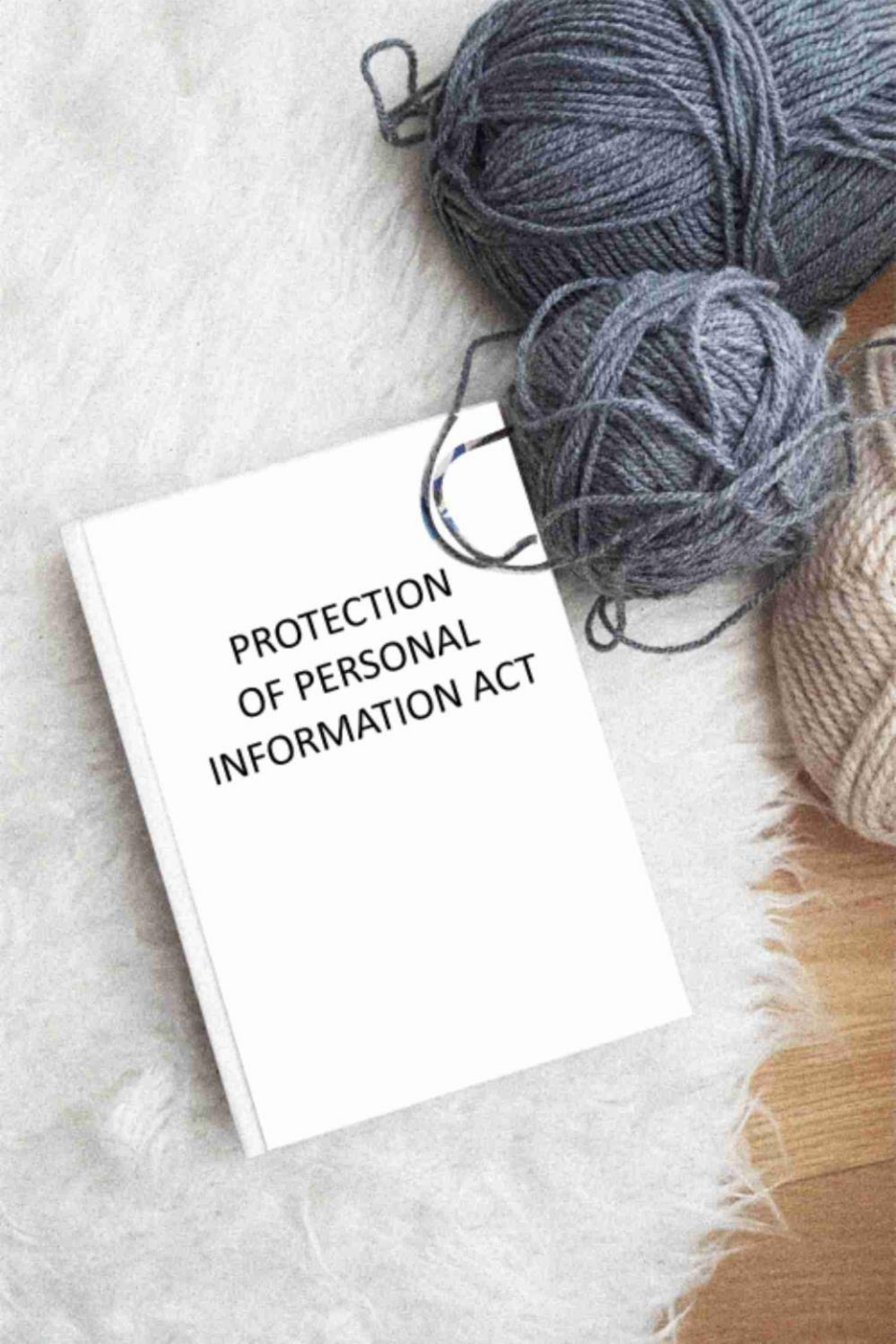
- Process it in a territory which the European Commission has determined provides an adequate level of protection for personal information; or
- Implement appropriate safeguards to protect your personal information, including transferring it in accordance with applicable transfer mechanism, including the European Commission's [standard contractual clauses](#).

Microsoft Teams

International Data Transfers Privacy Shield And Contractual Terms

SoapBox may transfer your Personal Data to countries other than the one in which you live. We deploy the following safeguards if SoapBox transfers Personal Data originating from the European Union or Switzerland to other countries not deemed adequate under applicable data protection law:

- E.U.-U.S. Privacy Shield and Swiss-U.S. Privacy Shield. To comply with European Union and Swiss data protection laws, SoapBox Innovations, Inc. ("SoapBox") self-certified under the E.U.-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield. These frameworks were developed to enable companies to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States. For more information, including the types of Information covered, see SoapBox's Privacy Shield Notice. To learn more about the Privacy Shield Program, please see <http://www.privacyshield.gov/welcome>.



PROTECTION
OF PERSONAL
INFORMATION ACT

What do I need to do,
what documentation
do I need and where
do I start?

Where do I start?

UNDERSTAND AND ANALYSE

- ▶ **Training**, buy-in, team, data base and budgeting
- ▶ Understanding where you fit in to the value chain across your major activities and where you are a responsible party or an operator
- ▶ **Map activities: understand and document your purposes and *main* activities and what personal information you process as well as – processing of account numbers, special personal information, children's information, automated processing and information leaving the country (precursor to other deliverables)**
- ▶ Understand if you are subject to law in foreign jurisdictions e.g. GDPR
- ▶ Identify and risk-rate your own operators and decide their requirements going forward
- ▶ Analyse who your responsible parties are and what they will require
- ▶ Gap analysis?

STATUTORY DELIVERABLES

- Do a privacy impact assessment (measures and standards to mitigate privacy risks and how you stack up against the Eight Conditions)
- Identify grounds and any justifications you are relying on to process (and communicate where required)
- A compliance framework – work POPIA into your existing compliance framework if you have one
- PAIA Manual
- Establish processes for data subject interaction
- Establish reporting requirements to Information Regulator
- Decide where you are going to need to make POPIA disclosures to data subjects
- Set up your awareness programme
- Retention and destruction processes
- Consider IT security measures
- Identifying any prior authorisations required

Where do we start?

For the activities where we are the Responsible Party

NON-STATUTORY DELIVERABLES

- Delegation from CEO to an Information Officer and register Information Officer
- Who is making use of information for direct marketing purposes?
- Data Protection Policy (including breach and incident management)
- Processes to identify and manage POPIA related complaints
- Review standard forms, booklets and communications – disclosures and consents (use standardised wording as far as possible)

Where do we start?

Whether operator or responsible party

Agreements

- ▶ POPIA wording for agreements. **Negotiating** amendments to agreements can take time
- ▶ Amendment of agreements to ensure it takes into account all your functions
- Amendment of agreements with employees as well as amendment of employment process documents and employment policies, where relevant
- Draft and implement an upfront plan and ongoing plan (compliance framework)
- Re-look your insurances
- Security measures (business and IT)
- Amendment of any standard procurement/tender documentation or processes
- Adding privacy and cybersecurity to any regular reviews and reports
- Communication to clients
- Sharing information between parties – document processes and put protocol in place

Stephen Walker

Retirement Fund Valuator

Old Mutual Corporate Consultants

swalker2@oldmutual.com

+27 (0)71 302 2022 (cell)

Leanne van Wyk

Director

ICTS Legal Services (Pty) Ltd

vanwykl@icts.co.za

+27 (0)83 257 8468 (cell)



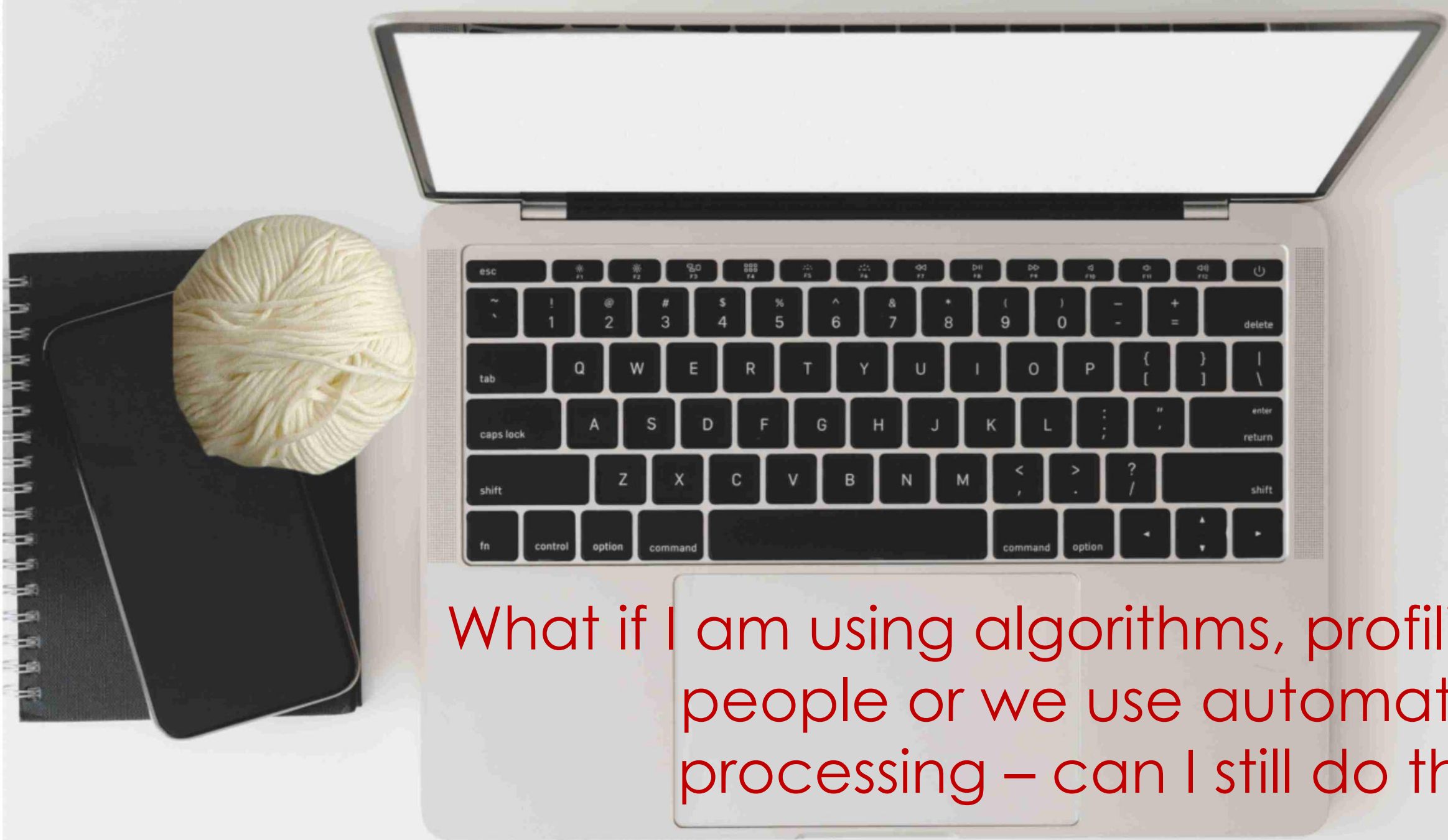
Actuaries and the Protection of Personal Information Act

Unraveling the strings...

Questions

Thank you

If we have time...



What if I am using algorithms, profiling people or we use automated processing – can I still do this?

Other requirements...

- (1) Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

Algorithms

Profiling

The data subject has the right not to be subjected to an (important) decision about her/him based only on the *automated processing* of her/his personal information intended to profile her/him

The way we analyse Personal Information for the purposes of risk assessment, scheme valuation and client reporting may involve profiling, which means that we may process your Personal Information using software that is able to evaluate your personal aspects and predict risks or outcomes. For example, we may conduct analyses on Personal Information to predict mortality rates which we use for the purposes of scheme valuation.



What must I
have in my
retention
policy – how
long may I
keep
personal
information
for?

The Eight POPIA Conditions for Responsible Parties

Condition Three - Retention

3

Purpose:
Retention, destruction
and restriction 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.

Retention:

- One of the 'exceptions' / 'authorisations' here is that if we are authorised by law to keep it, we may
- There are also provisions allowing **restriction** of records which allows use only in specified circumstances, such as for storage or proof and where a process must be followed before accessing the info
- Very difficult subject for retirement funds and thus, actuaries

My retention policy – how long may I keep personal information for?

Big actuarial
(and other) firm

We may retain your Personal Information for as long as we provide the Services to the Trustees. When we have ceased providing the Services, we will then retain your Personal Information for a period of time that reasonably allows us to comply with our regulatory obligations and to commence or defend legal claims. We may retain aggregated or anonymised data (which is not treated as Personal Information under this privacy notice) for longer.

Too vague?

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.

Retention – real examples of GDPR notices/policies of foreign pension funds

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 years³ 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

Questions

- What if administrators or funds send me personal information that I don't need for my fund activities?
- If I keep information, do I have to keep it updated?
- Who should de-identify the information and when?
- As an actuary I often sit through meetings and discussions which don't really have anything to do with my role, should I be there?