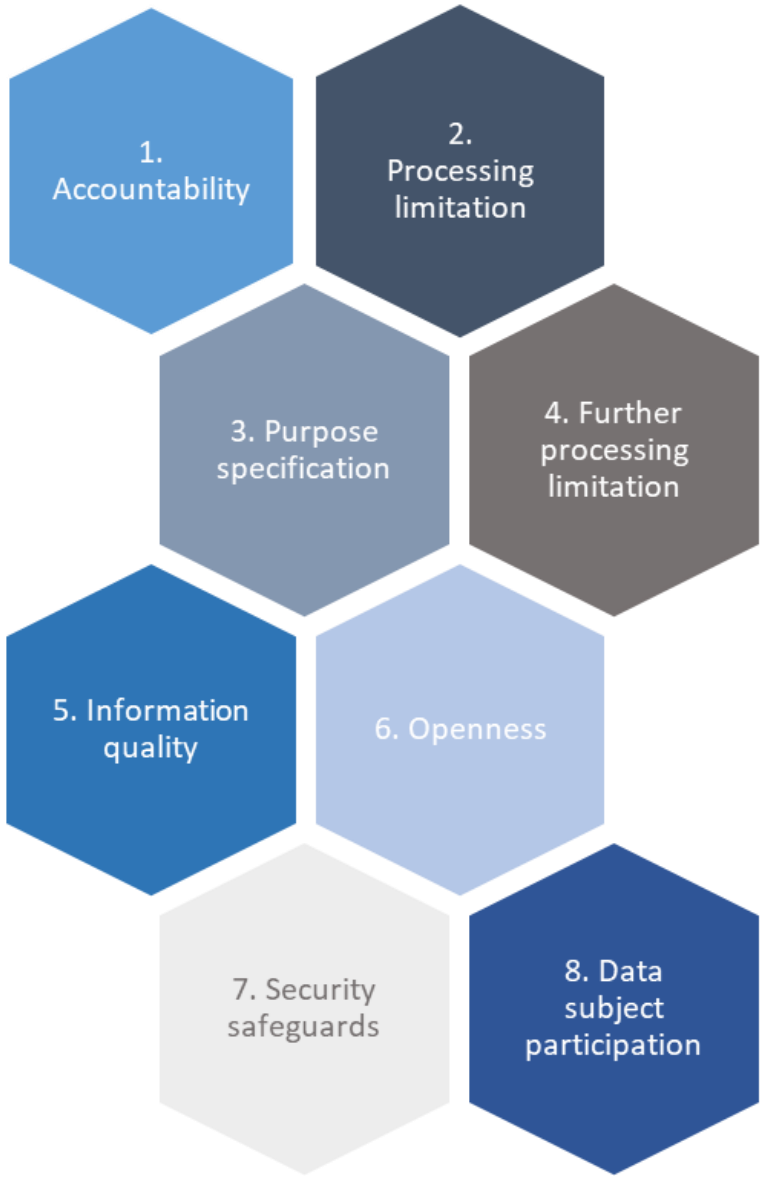
Pre-reading for the ASSA Sessional on Actuaries and the Protection of Personal Information Act to be held on 10 November 2020

ACTUARIAL SOCIETY OF SOUTH AFRICA

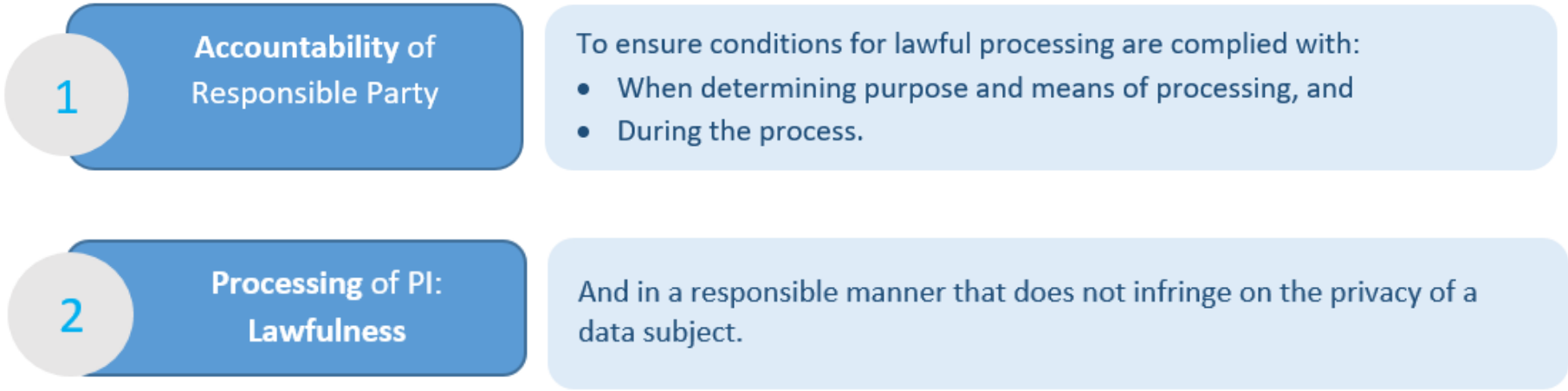
The Eight POPIA Conditions for Responsible Parties



The Eight Conditions are set out in the slides below
We have jumped around in the order a little

The Eight POPIA Conditions for Responsible Parties (RP)

Condition One – Accountability



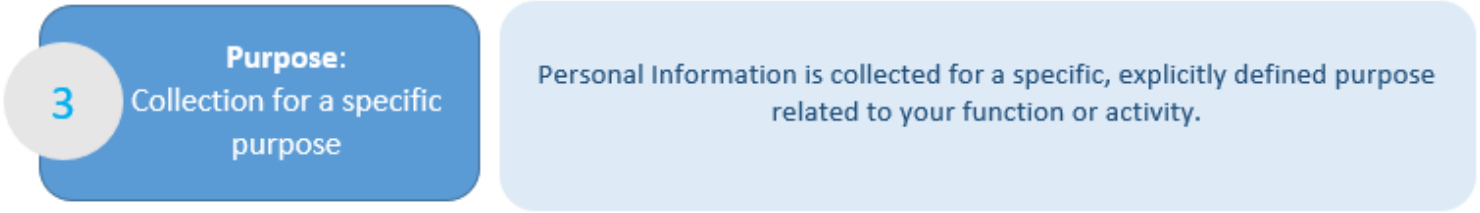
Condition 1 (accountability) and part of 2 (lawfulness) – general catch all

- RP is responsible for ensuring that personal information is processed, upfront and every time subsequently, in accordance with POPIA, lawfully and does not infringe on the privacy

- The RP must ensure that it and its operators comply with the conditions for lawful processing of personal information as set out in POPIA

The Eight POPIA Conditions for Responsible Parties

Condition Three - Purpose



- 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 RP must ensure that the data subject knows about the purpose (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)

The Eight POPIA Conditions for Responsible Parties Condition Two – Processing

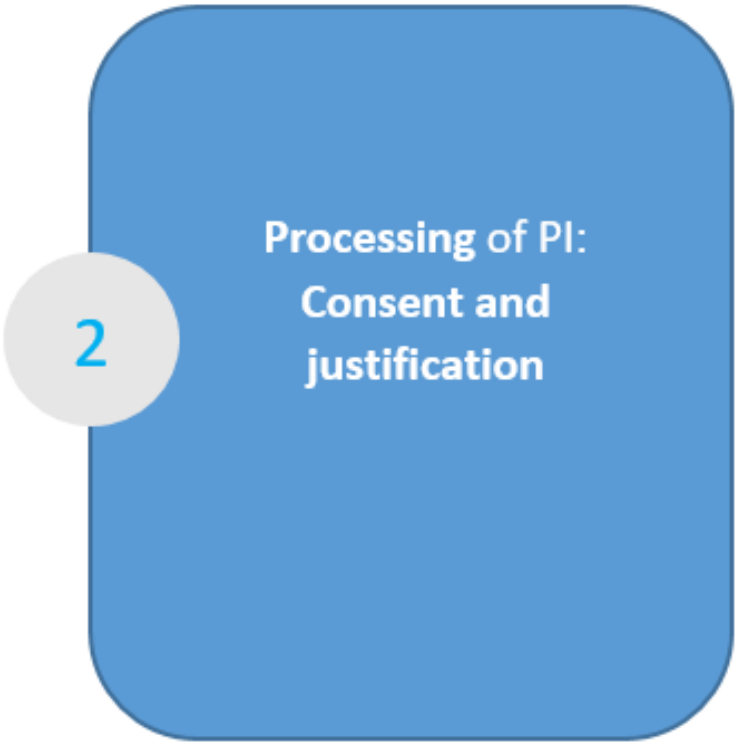
2 **Processing of PI: Minimality**

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 it 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

The Eight POPIA Conditions for Responsible Parties Condition Two – Processing



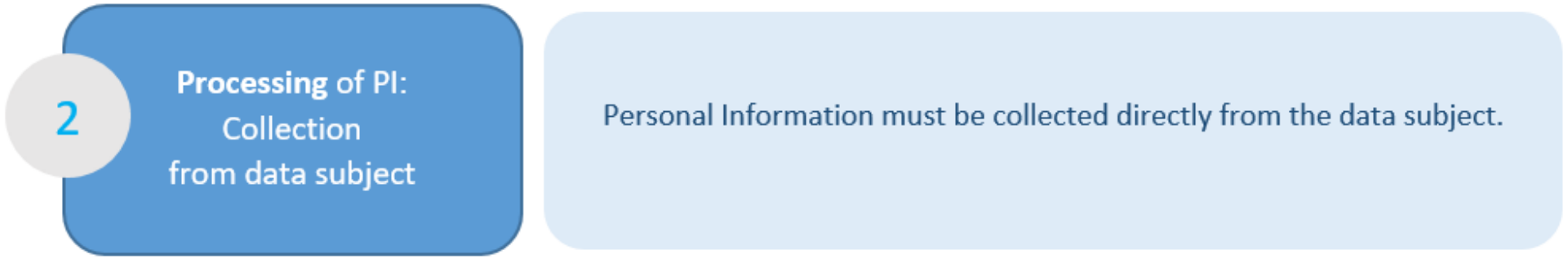
- **To process personal information the Responsible Party needs data subject consent** OR rely on one of the following:
- It's necessary to carry out actions for a contract with the data subject OR
- It complies with an obligation imposed by law on the RP, OR
- It protects the legitimate interest of 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 fund is going to process because it is pursuing its legitimate interests (performing the activities we are expected to perform) and we therefore don't need consent (but need to look at purposes/activities)

Identify
Document
Communicate

The Eight POPIA Conditions for Responsible Parties Condition Two – Processing



This is a difficult condition for funds to comply with as often funds receive personal information 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

The Eight POPIA Conditions for Responsible Parties

Condition Four – Further processing

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.

- We can only further process personal information (other than for its purpose) if the further processing is according to or compatible with the purpose for which we collected the information.

- A party must assess whether further processing of personal information is compatible with the original purpose for which it was collected by considering:

    - The relationship between the additional processing and the original purpose;
    - The nature of the information involved;
    - How the additional processing will affect the data subject;
    - How the information was collected; and
    - Any contractual rights and obligations between the parties.

The Eight POPIA Conditions for Responsible Parties

Condition Five – Information quality Condition Six – Openness

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.

Condition 5 means that if we are keeping personal information, we have continuing obligations with respect to it

Conditions 6 means that documentation must be kept by the fund for all processing operations (activities) that it has specified in its section 51 manual (fund manuals – end Deceber 2020)

The Eight POPIA Conditions for Responsible Parties

Condition Six – Openness

6 **Openness** – notification when collecting

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

When information is being collected, data subjects must be made aware of the information below

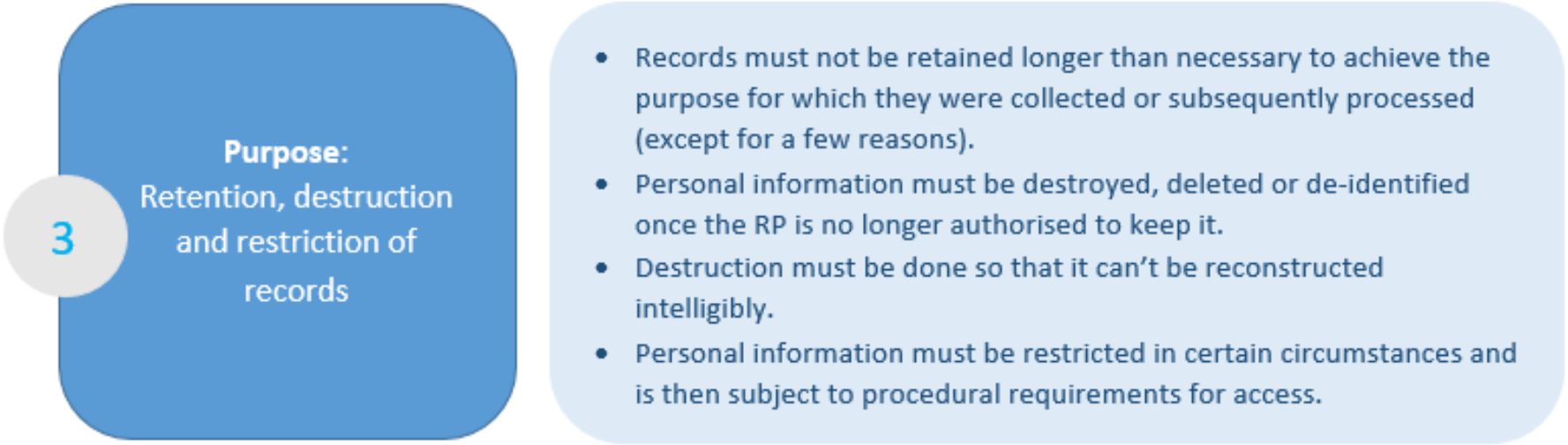
- the information that is being collected and if the information is not being collected from the data subject, the data subject must be made aware of the source from which the information is being collected;
- the name and address of the person/organisation collecting the information;
- the purpose of the collection of information;
- whether the supply of the information by the data subject is voluntary or mandatory;
- the consequences of failure to provide the information;
- whether the information is being collected in accordance with any law;
- if it is intended for the information to leave the country and what level of protection will be afforded to the information after it has left South Africa.
- who will be receiving the information;
- that the data subject has access to the information and the right to correct any details;
- that the data subject has the right to object to the information being processed;
- that the data subject has the right to lodge a complaint with the Information Regulator. The contact details of the Information Regulator must also be supplied.

- Before collection if directly from the data subject, or soon as reasonably practicable after if not collected directly from the data subject
- Unless the data subject is already aware (e.g. you have told them before).
- If you collect additional information from a data subject for a different purpose, you have to go through this process again

- Justifications not to comply include:
- Consent;
- Would not prejudice legitimate interest of dats subject;
- Not reasonably practicable for the particular case

The Eight POPIA Conditions for Responsible Parties

Condition Three - Retention



- 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

The Eight POPIA Conditions for Responsible Parties - Condition Seven - Security safeguards

- 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.

- We are required to safeguard personal information from loss, damage, unauthorised destruction and unauthorized access and use through technical and organisational measures
- This is both (i) a business function (i.e. 'organisational measures') and (ii) an IT function. In terms of POPIA, the steps a responsible party takes must:
    - Identify all risks to the personal information;
    - Create safeguards for those risks;
    - Check that those safeguards are working &
    - Update those safeguards for any new risks.
- Where an operator or third party processes personal information for us we have to ensure they establish and comply with the security measures
- Operators have similar requirements regarding security measures

The Eight POPIA Conditions for Responsible Parties - Condition Seven - Security safeguards

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.

The Eight POPIA Conditions for Responsible Parties - Condition Seven - Security safeguards

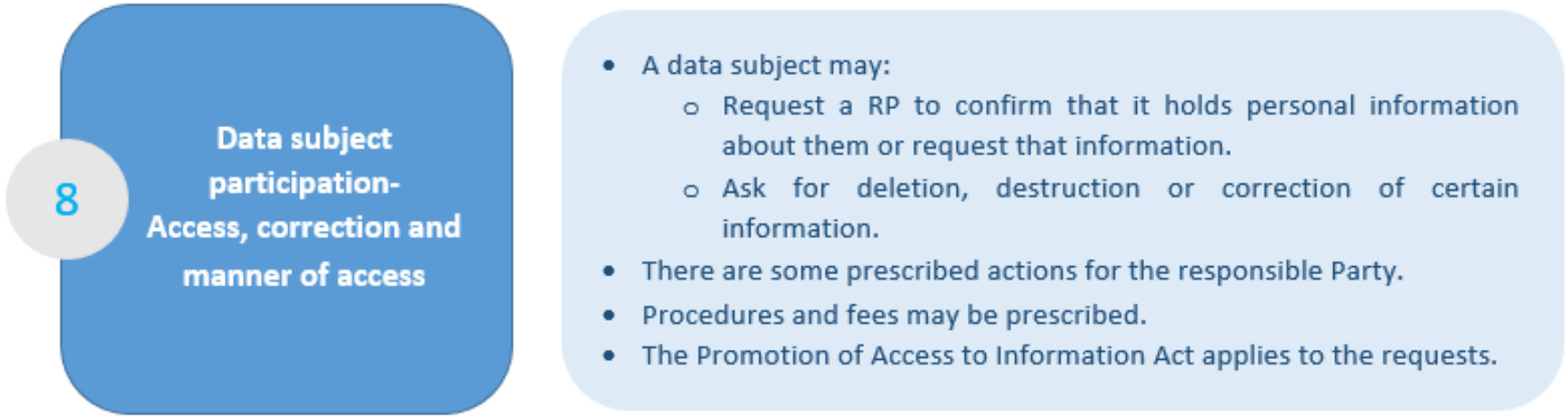
7

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.

The Eight POPIA Conditions for Responsible Parties –

Condition Eight: data subject participation



Data subject can:

- Ask what personal information we hold bout them and request access
- Ask for corrections, deletions, or destruction
- Object to our processing their personal information
- Procedures, forms and fees (manual/notice)
- Complain to the Responsible Party
- Complain to the Information Regulator