VERBATIM

August 2020

ISSUE 56

THE PROTECTION OF PERSONAL INFORMATION ACT

Finally, as of 1 July 2020, the remaining provisions of POPIA have become effective. We all now have one year to reach a state where we are compliant with this legislation. This period could possibly be extended, but we cannot rely on this occurring.

WHEN DOES POPIA APPLY?

POPIA applies (with exceptions) to the **processing** of **personal information** in a **record** by, or on behalf of, a **responsible party**.

It is important to understand the meaning of the words: 'processing', 'personal information', 'record' and 'responsible party'.

Personal information is widely defined and includes almost all information about a living, identifiable person (and where applicable juristic persons), including race, gender, pregnancy, marital status, medical history, contact details, biometric information, their personal opinions amongst other information (note for POPIA purposes, personal information about a deceased person is not personal information). It does not include de-identified information.

Processing is also widely defined and includes almost anything one does with personal information, including, receiving or collecting it, storing it (electronically or physically), filing it, or destroying it.

A **record** means any recorded information regardless of the form in which it is recorded. So a record includes electronic and paper information, x-rays, photos, labels, drawings, graphs, maps, etc which is in the possession of the responsible party (whether or not they created it).

As an example, a retirement fund's administrator (operator) processes personal information for and on behalf of a retirement fund (responsible party).

A **responsible party** means the person who determines the purpose and means for processing information. In the retirement funds context, it will be mainly retirement funds (and employers) that are responsible parties. Their service providers, such as administrators and consultants will be **operators**. Operators process information for, or on behalf of, responsible parties. As an example, a retirement fund determines how its operators will process the personal information of the fund's members (and others). Thus, the fund enters into an administration agreement with the administrator determining the purposes for which that administrator will process personal information on its behalf.

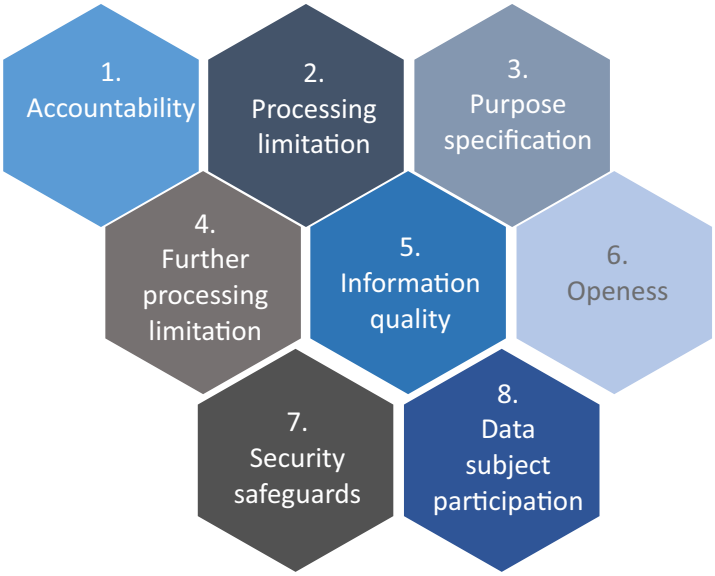
The Eight Conditions

Responsible parties are required to comply with the *Eight Conditions* when they process personal information for the first time and every time. Importantly, they must also ensure that their operators comply with the Eight

Conditions. Thus, it becomes important for responsible parties to ensure they are contracting with operators that are POPIA compliant. Many responsible parties will seek to contractually tie in their operators to ongoing POPIA compliance.

While POPIA provides us with Conditions it also provides a number of 'exceptions' or 'authorisations'. If your processing falls into one of these 'exceptions' or 'authorisations' the Condition then does not apply. This makes POPIA fairly complex to implement as one needs to understand the Conditions as well as the 'exceptions' or 'authorisations' that apply to the Conditions or one of the Conditions

The following are the Eight Conditions that responsible parties must comply with every time they process personal information:



This does not give us much information about each Condition. It is necessary to dig a little deeper to understand the Eight Conditions. The Eight Conditions consist of more than eight requirements which are just grouped into the Eight Conditions. In the diagram below the number corresponds to the Condition number and there is often more than one requirement per Condition.

So, in more detail, the Eight Conditions with which responsible parties must comply when processing personal information appear below.

1 Accountability of RP*

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 is required, 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 restiriction 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 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 Openess - documentation

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

6 Openess - notification when collecting

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

* RP stands for Responsible Party
** PI stands for Personal Information

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 Notifications 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.

THERE ARE MORE REQUIREMENTS IN POPIA THAN JUST THE EIGHT CONDITIONS

It is not enough to simply comply with the Eight Conditions. There are many other provisions of POPIA, which we need to understand and with which we need to comply, for example:

- Children's information
- Special personal information
- Account numbers
- Direct marketing
- Prior authorisation of processing
- Automated processing;
- Information Officers, and
- Personal information leaving the country,

With the exception of a brief discussion concerning special personal information and Information Officers, we have not discussed these other requirements in this note.

SPECIAL PERSONAL INFORMATION

Special personal information is personal information that is very confidential and requires special protection.

The classes of special personal information are:

- Religious/philosophical beliefs
- Race/ethnic origin
- Trade union membership
- Political persuasion
- Health
- Sex life
- Biometric information, and
- Criminal behavior

The general rule, under POPIA, is that the responsible party must not process special personal information. However, they may process special personal information if one of the following applies:

(a) The list of general authorisations that apply to all special personal information (for example they have consent from the data subject or the processing is necessary for the establishment, exercise or defence of a right or obligation in law); or

(b) One of the specific authorisations set out in POPIA which applies to a specific class of special personal information applies to the responsible party. For example: for the class of health information, pension funds (and their administrators) may process health information if the processing is necessary for the implementation of laws (e.g. the Pension Funds Act), pension regulations, etc. Thus, if we are a pension fund processing health information because we are required to do so by law, then we may process it.

It is probable that in the future the Information Regulator will consider setting further rules with respect to these specific authorisations, especially with respect to the class of health and sex life.

INFORMATION OFFICERS

Every responsible party must have an Information Officer. The Information Officer is automatically the head of a juristic person (like a company or a fund). The head of a juristic person is generally the Chief Executive Officer (CEO) or someone the CEO has authorised to be the Information Officer. In a retirement fund context this may be the Principal Officer of a fund or whomever the Principal Officer has authorised to hold this position.

Information Officers have to be registered with the Information Regulator and the Information Regulator has issued a draft notice concerning registration requiring these registrations to be done by 31 March 2021 on prescribed forms. The Information Officer can appoint Deputy Information Officers, but remains responsible for his/her statutory obligations. Information Officers and Deputy Information Officers must receive appropriate training and keep abreast of the latest developments in POPIA and the Promotion of Access to Information Act.

The draft notice referred to above sets out some of the statutory duties of Information Officers, which are:

- The *encouragement of compliance* by the body with the Eight Conditions for the lawful processing of personal information. For example, an Information Officer may develop a *policy* on how employees should implement the Eight Conditions for the lawful processing of personal information;
- Dealing with the various *requests* that can be made to the body pursuant to POPIA. Internal measures are developed together with adequate systems to process *requests for or access to information*;
- Submission of a detailed *report about requests* to the Information Regulator;
- Working with the Information Regulator in relation to *investigations* in relation to the body (including prior authorisations);
- A personal information *impact assessment* is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- A *manual* is developed, monitored, maintained and made available as prescribed in section 51 of PAIA, as amended by POPIA (this must be provided on request for a fee);
- A *compliance framework* is developed, implemented, monitored and maintained; and
- *Internal awareness sessions* are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Information Regulator.

IMPLEMENTATION

It is very clear that POPIA demands action. Responsible parties and their operators have much work to do in order to become and remain compliant with POPIA on an ongoing basis. This needs to be approached in a structured way that leads to compliance that can be demonstrated and that will protect customers and others from unauthorised and damaging processing of their personal information, which breaches their privacy rights.