Nurture Health

POPIA POCKET **GUIDE**

THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 ("POPIA")

1.1. PURPOSE

POPIA impacts on the existing legal frameworks that relate to privacy and confidentiality. The right to privacy has its roots in the provisions of Section 14 of the Constitution of the Republic of South Africa, 1996. In addition to the right to privacy, there exists the right to access to information.

These human rights have been translated into two separate pieces of legislation: The Promotion of Access to Information Act, 2000 ("PAIA") and POPIA.

Apart from its importance as a human right, the right to privacy is also central in legislation pertaining to new and ever-evolving technologies, such as Wi-Fi tracking, geo-location, data analytics and telecommunications.

POPIA aims to:

(a) Ensure the right to privacy when personal information is processed.

(b) Provide persons with the correct remedies to protect their personal information.

(c) Promote and enforce the rights protected by POPIA.

(d) Regulate the manner in which personal information may be processed.

1.2. THE SCOPE AND OBJECTIVES OF POPIA

- To promote the protection of personal information processed by public and private bodies;
- To establish minimum requirements for the processing of personal information;
- To provide for the establishment of an Information Regulator: which exercises certain powers and functions in terms of both POPIA and PAIA;
- To provide for the issuing of codes of conduct, specifically industry specific codes of conduct;
- To provide for the rights of people regarding unsolicited electronic communications;
- To provide for the rights of people regarding automated decision making;
- To regulate the flow of personal information across the borders of South Africa; and
- To provide for matters which are in any way connected to the above.

1.3. KEY ASPECTS

- Definitions and purpose of POPIA
- Application and interpretation of POPIA
- The eight conditions for lawful processing of personal information
- Exemption from complying with the conditions for the processing of personal information.
- Supervision by the information regulator
- Prior authorisation to be obtained before processing of personal information.

Codes of conduct

- Rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making.
- Transborder information flows
- Enforcement of the provisions of POPIA
- Offences, penalties, and administrative fines
- General provisions

1.4. COMMENCEMENT DATE

Certain section of POPIA commenced on 11 April 2014:

- **Section 1** – Definitions;
- **Part A of Chapter 5** – Establishment of the Information Regulator;
- **Section 112** – The Regulations; and
- **Section 113** – Procedure for making the Regulations.
- **Section 144** – "The Window Period". This section provides for a window period of one year after the commencement of Section 114.

1.5. APPLICATION OF POPIA

To apply POPIA correctly, it is important to understand that the activities undertaken by the Nurture Care Group of Companies, fall within the ambit of POPIA.

1.5.1. Section 3 of POPIA

POPIA applies to the processing of personal information:

- Entered in a record by or for a responsible party by making use of automated or non-automated means;
- Where the responsible party is:
    - o Domiciled in the Republic; or
    - o Not domiciled in the Republic but makes use of automated or non-automated means in the Republic.

1.5.2. Point of departure

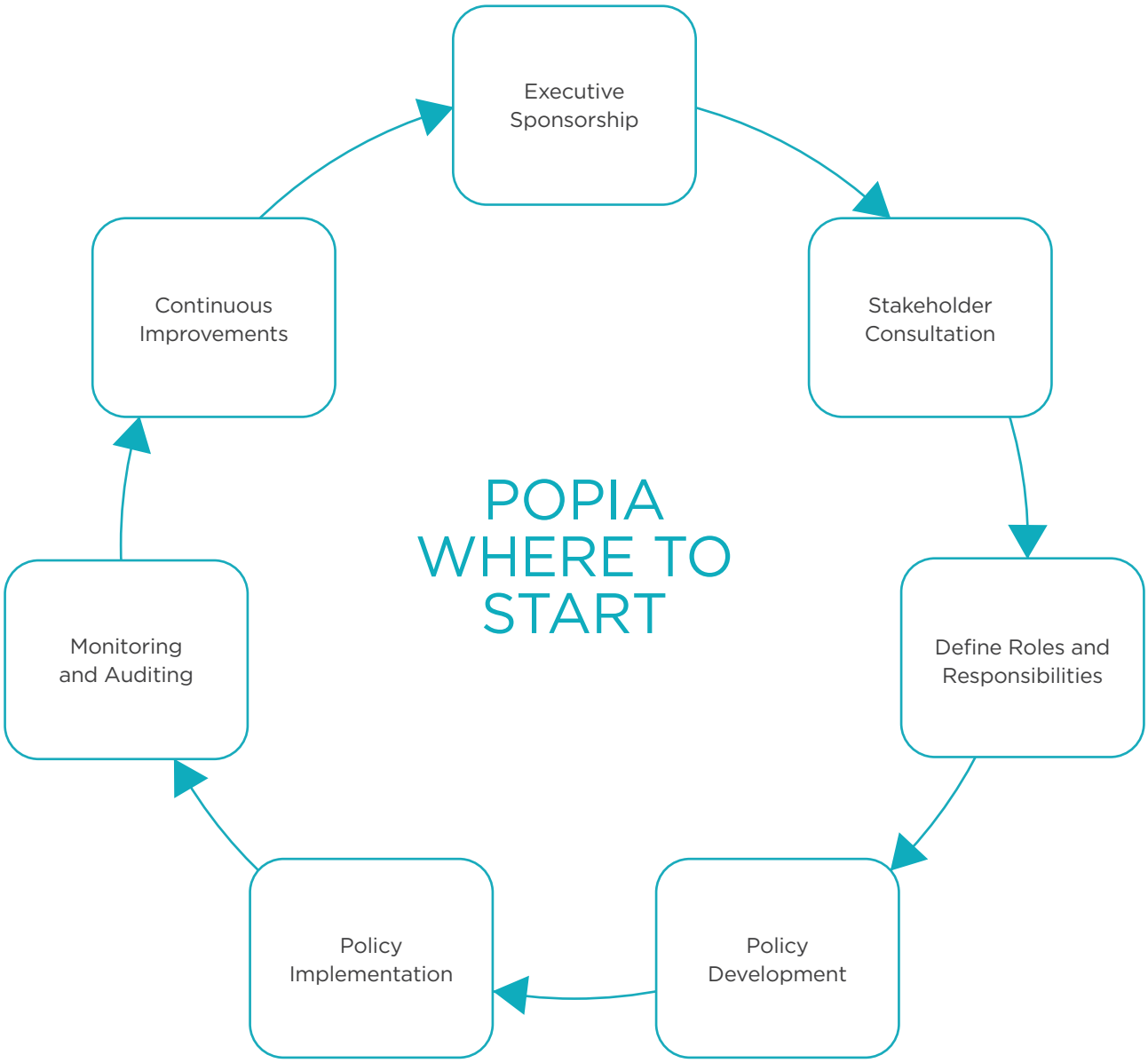
In any scenario where information is being processed and to ascertain whether POPIA would apply, it is important for all employees to ask themselves these three questions and to consider the definitions of the applicable terms in this Guide:

- Is this information in fact "Personal Information"?
- Are we (because of my processing this personal information) going to be processing the information as a "Responsible Party"?
- Is the personal information in fact going to be "processed" as contemplated in terms of the provisions of POPIA?

GENERAL EXCEPTIONS

POPIA does not apply to the processing of personal information:

- Relating to a purely personal or household activity;
- That has been de-identified (to the extent it cannot be re-identified again);
- By or on behalf of a public body and:
- which involves national security; or
- purpose of which is for prevention, detection of unlawful activity,
- By cabinet or executive council of a province; or
- Regarding judicial functions of court.


POPIA
WHERE TO
START
Executive Sponsorship
Stakeholder Consultation
Define Roles and Responsibilities
Policy Development
Policy Implementation
Monitoring and Auditing
Continuous Improvements

DEFINITIONS:

Data Subject: The person to whom the personal information relates.

Responsible Party: 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.

Personal Information: It is information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of a person;
- Information relating to the education or medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, e-mail address, physical address, telephone number, location, information, online identifier, or other assignment to the person.
- The biometric information of the person;
- The personal opinions, views, or preferences of the person;
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the person; and
- The name of the person if it appears with the other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Processing: Any operation or activity or set of operations, whether by automated means, concerning personal information, including –

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
- Dissemination by means of transmission, distribution or making available in any other form; and
- Merging, linking, as well as restriction, degradation, erasure, or destruction of information.
  – Section 1 of POPIA.

Direct Marketing: To approach a data subject, either in person, or by e-mail or electronic communication for the direct or indirect purpose of:

- promoting or offering to supply, in the ordinary course of business, any goods.
- requesting the data subject to donate in any way.

Electronic Communications: Text, voice, sound; or image message which is sent over an electronic communications network, and which

RECORD

Any recorded information, regardless of form or medium, including any of the following:

- Writing on any material;
- information produced, recorded, or stored by means of any tape-recorder, computer equipment (hardware or software) or other device and any material subsequently derived from such information;
- label, marking or other writing that identifies or describes anything which form's part or is attached by any means;
- book, map, plan, graph, or drawing;
- photograph, film, negative, tape or other device in which one or more visual images are embodies to be capable of being reproduced;
- in the possession or under control of a responsible party;
- whether or not it was created by a responsible party; and
- regardless of when it came into existence.

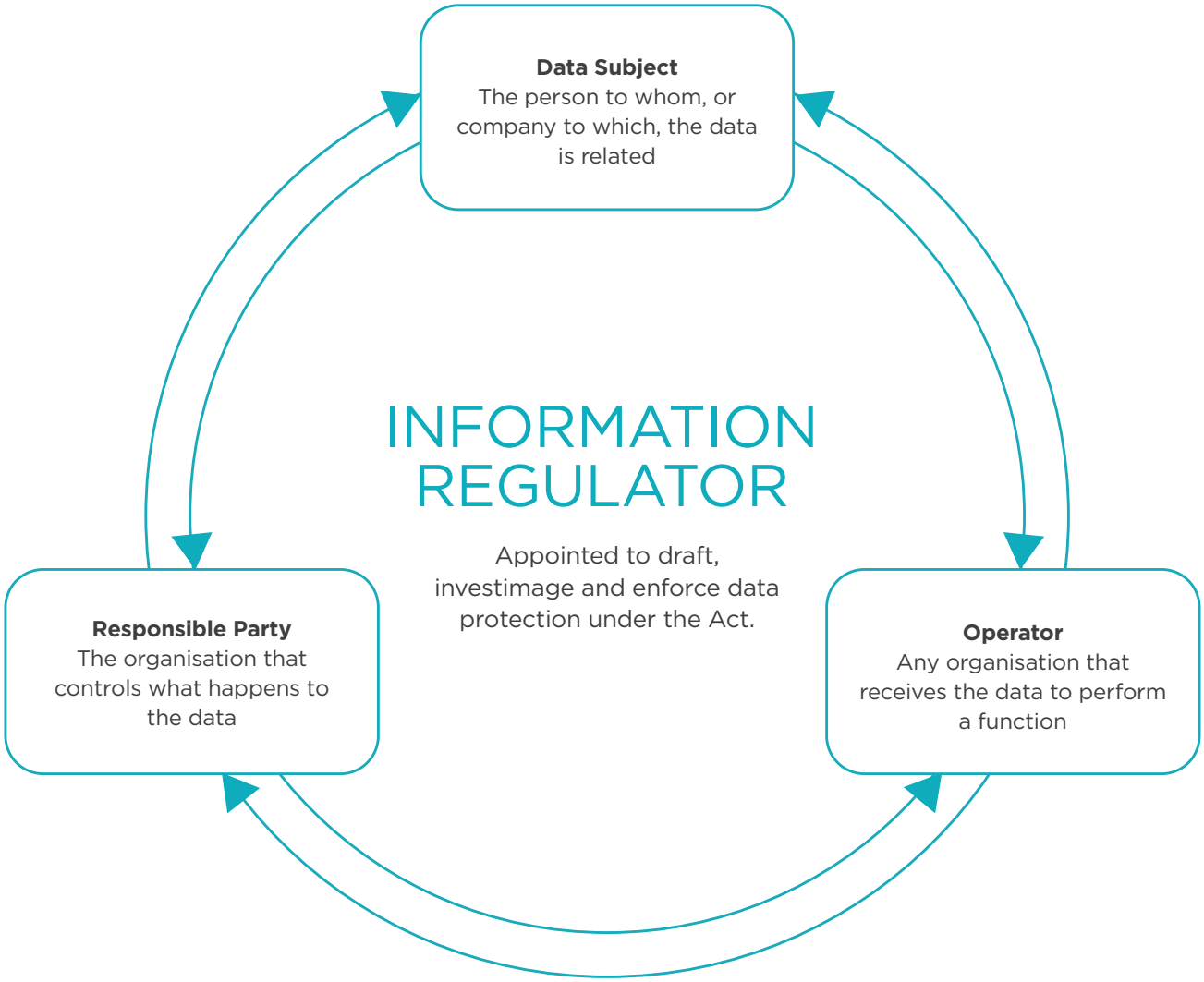
Operator: A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

1.6 QUALIFICATIONS

Where Personal Information is captured manually, the recording thereof will only be regarded as processing if the information relates to a data subject, e.g., an individual or a legal entity.

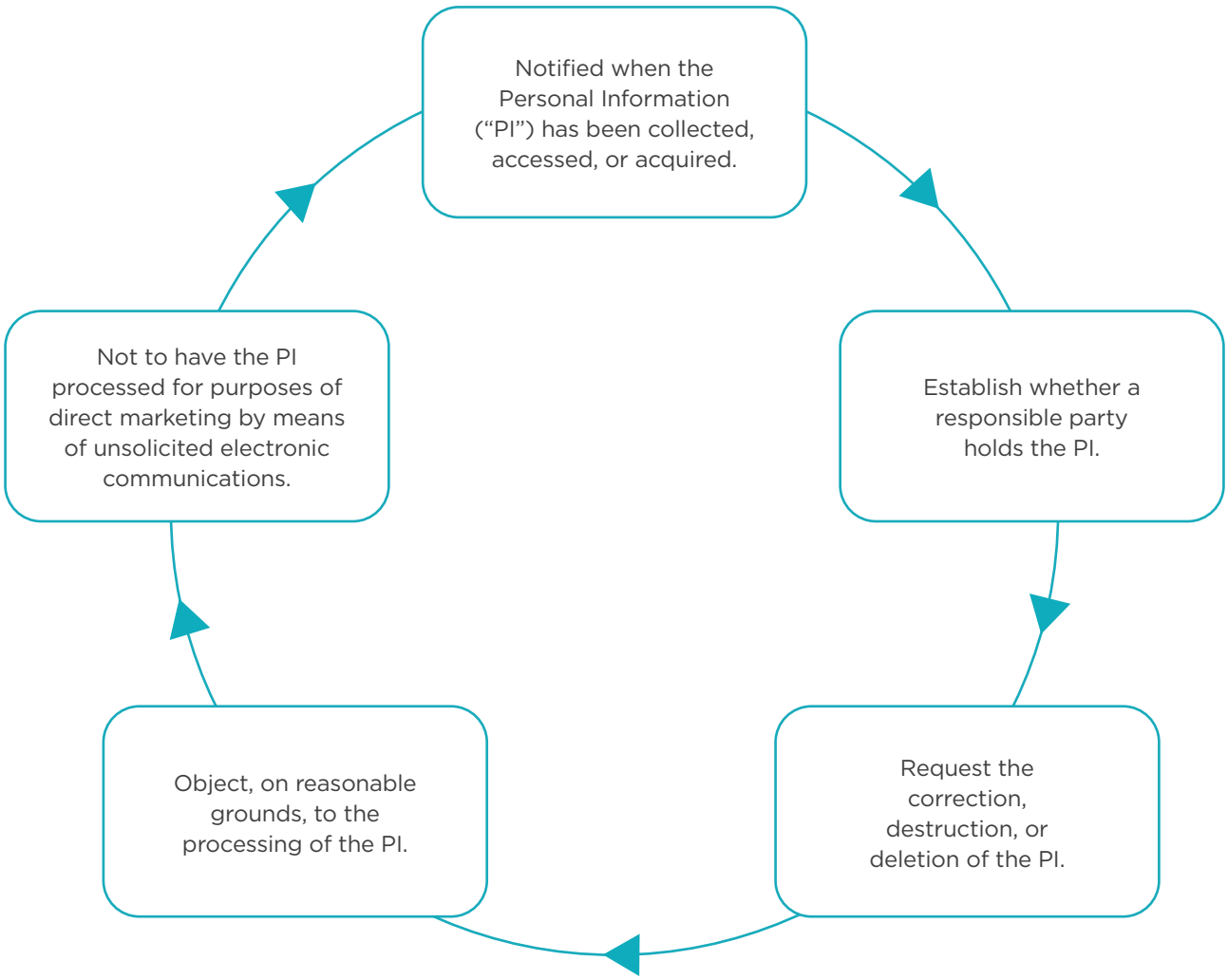
With regards to the capturing of data, all employees must take note of the following:

- the reference to "set" it the act, implies that there is more than one file in the filing system, or that specific information is grouped together according to some or other classification;
- the files do not have to be in the same geographical area to form a set because they can be centralised or decentralised;
- the set must be structured by reference to the personal information of the data subject, e.g., by name, employee number, type of job, credit history, age, type of criminal offence etc.


Data Subject
The person to whom, or company to which, the data is related
INFORMATION REGULATOR
Appointed to draft, investimage and enforce data protection under the Act.
Responsible Party
The organisation that controls what happens to the data
Operator
Any organisation that receives the data to perform a function

2. RIGHTS OF DATA SUBJECTS

Rights cycle



Rights breakdown

- Not to be subject to automated processing of his/her PI.
- To submit a complaint to the Regulator
- 02 regarding processing of his/her PI.
- To submit a complaint to the Regulator regarding 03 a decision by an adjudicator.
- Right to institute civil proceedings regarding the 04 interference with the protection of his/her PI.
- To have his/her PI processed in accordance with the 8 conditions 05 of lawful processing

3. THE 8 CONDITIONS OF LAWFUL PROCESSING IN TERMS OF POPIA

01	**Accountability**	- Section 8
02	**Processing Limitation**	- Sections 9 to 12
03	**Purpose Specification**	- Sections 13 to 14
04	**Further Processing Limitation**	- Section 15
05	**Information Quality**	- Section 16
06	**Openness**	- Sections 17 to 18
07	**Security Safeguards**	- Sections 19 to 22
08	**Data Subject Participation**	- Sections 23 to 25

3.1. 1st condition: Accountability (Section 8)

The responsible party must ensure that the 8 Conditions of Lawful Processing and all the measures that give effect to those conditions are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

Reflections

- Is there currently a person and/or department in our business responsible for overall information security compliance?
- Are our daily operations being monitored with the necessary information security safeguards?

1. Accountability | **2. Processing limitation**

3. Purpose specification | **4. Further processing limitation**

5. Information quality | **6. Openness**

7. Security safeguards | **8. Data subject participation**

3.2. 2nd condition: Processing limitation (Sections 9 to 12)

3.2.1. Section 9 – Lawfulness of processing

Personal Information may only be processed.

- lawfully; and
- in a reasonable manner that does not infringe the privacy of the data subject.

3.2.2. Section 10 - Minimality

Personal Information may only be processed if, given the purpose for which it is processed, it is -

- adequate;
- relevant; and
- not excessive.

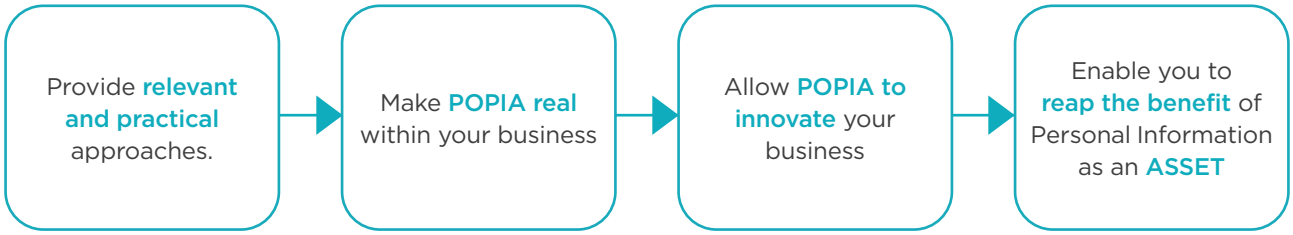
3.2.3. Personal information processing

Personal information may only be processed if:

S11(1)(A)	S11(1)(B)
The data subject (or a competent person in the case of children) consents to it.	Processing is necessary for the conclusion or performance of a contract.
S11(1)(C)	**S11(1)(D)**
Processing complies with an obligation imposed by the law on a responsible party.	Processing protects the legitimate interests of a data subject.
S11(1)(E)	**S11(1)(F)**
Processing is necessary for a public body to perform a public duty.	Processing is necessary for pursuing the legitimate interests of a responsible party or a 3rd party to whom PI is supplied.

REFLECTIONS

- Is there a formal policy for the processing of personal information?
- Does the policy identify the grounds upon which to process?
  - o Consent
  - o Contract
  - o Legislation
- What is the purpose, and do we process different categories of information?
- Is the information gathered excessive for these purposes?
- What are our de-identification mechanisms/processes?
- Is consent obtained before processing takes place?
- Precisely how and when is the consent obtained?
- Do we supply personal information to 3rd parties and if so, is consent obtained first?
- Is personal information obtained directly from individuals?
- If applicable, is our use of intermediaries/agents to collect personal information?



3.3. 3rd condition: Purpose specification (Sections 13 to 14)

The third condition sets out two requirements:

1. Personal information must be collected for a specific, explicitly defined, and lawful purpose, related to a function or activity of the responsible party; and
2. Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected, or subsequently processed.

3.3.1. Explicitly defined and lawful purpose

Specific purpose: a proper description of the specific purpose for which the personal information is collected, must be provided, even if it is obvious, e.g., for research or marketing purposes.

Explicitly Defined purpose: under this requirement it is expected from the responsible party to go even further and give more information regarding the purpose, e.g., details about the type of research which is being conducted or marketing intended.

Lawful purpose: the responsible party must consider whether there are any other statutory or common law rules which must be observed in addition to those imposed by POPIA, which relate to the way in which personal information is processed (e.g., confidentiality provisions in statutes, copyright law, or discrimination laws)

3.3.2. Retention of records

In terms of Section 14(1), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected, or subsequently processed, unless:

- retention of the record is required or authorised by law;
- the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
- retention of the record is required by a contract between the parties thereto; or
- the data subject, or a competent person where the data subject is a child, has consented to the retention of the record.

Exceptions to the general rule: Records of personal information may be retained for periods more than that which is reasonably necessary for achieving the purpose for which the information was collected or subsequently processed if such personal information is retained for historical or statistical research purposes and the responsible party has established appropriate safeguards against the records being used for any other purposes.

3.3.3 Refusal of information retention:

Steps to be taken when we are no longer entitled to information retention:

- A responsible party must destroy or delete a record of personal information, or
- de-identify it as soon as reasonably practical, after we no longer authorised to retain the record of personal information.

3.3.4 What amounts to deletion or de-identification?

- The destruction or deletion of a record of personal information in terms of POPIA must be done in a manner that prevents its reconstruction in an intelligible form.

REFLECTIONS

- For what do we collect personal information? Do we classify it once it has been collected?
- Do we inform customers of the purpose for which their personal information is collected?
- Do we clearly identify the names and categories of all people and organisations to whom the information will be supplied?
- When and how do we inform the relevant persons?
- Do we allow people the opportunity to select for what purpose their personal information will be processed?
- Do we have a document/information retention policy, and if so, what does it say?
- Do we inform people about the duration for which their records will be retained?
- What mechanisms or systems do we employ pursuant to destroying or de-identifying information after the retention period?

3.4. 4th condition: Further processing limitations (Section 15)

3.4.1. Processing

Processing means any operation or activity or set of operations, whether by automated means, concerning personal information, including –

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

3.4.2. Further processing

- POPIA provides no definition of the term “further processing”.
- The concept, however, presumably refers to the further processing of information following the original collection thereof for a purpose other than that for which it had originally been collected.
- Any further processing of personal information must be in accordance, or compatible with the specified purpose for which that information was originally collected.

In determining whether any further processing of personal information is compatible with the specific purpose for which that information was originally collected, we must have regard to the following:

- the relationship between the purpose of the intended further processing, and the purpose for which the information has been collected;
- the nature of the information concerned;
- the consequences of the intended further processing for the data subject;
- the way the information has been collected; and
- any contractual rights and obligations between the parties.

EXPECTATIONS

The further processing of personal information shall not be regarded as incompatible with the (original) purpose of collection if:

- the data subject, or a competent person where the data subject is a child, has consented to the further processing of information;
- the information is available in or derived from a public record (e.g., the Deeds Registry Office), or has deliberately been made public by the data subject;
- further processing is necessary:
- to avoid prejudice to the maintenance of the law by any public body, including prevention, detection, investigation, prosecution, and punishment of offences;
- to comply with an obligation imposed by law, or to enforce legislation concerning the collection of revenue as defined in Section 1 of the South African Revenue Service Act, 1997 (Act no 34 of 1997);
- for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
- in the interests of National Security.
- the further processing of the information is necessary to prevent or mitigate a serious or imminent threat to:
- Public Health or Public Safety; or
- the life or health of the data subject or another individual;
- the information is used for historical, statistical or research purposes, and we ensure that the further processing is carried out solely for such purposes, and will not be published in an identifiable form.

REFLECTIONS

- Do we process personal information for any other purpose than that which we disclose to our users?
- What type of personal information do we primarily process?
- Does further processing affect the data subject?
- Do we inform the data subject when the information is processed for any other purpose than that which was originally disclosed?
- What mechanism or process is employed to communicate further processing to the individual?

3.5. 5th condition: Quality of information (Section 16)

We must always take reasonably practical steps to ensure that the personal information processed is:

- **complete** – i.e., all information regarding the data subject which is necessary to be processed to fulfil the purpose for which the information is collected, must be processed;
- **accurate** - information is inaccurate if it is factually incorrect;
- **not misleading** - information is misleading if it causes someone to believe something that is not true; and
- **updated where necessary** - there are certain exceptions, e.g., where a bank keeps records of previous transactions. This is historical data and must remain as they were at the time when those transactions were captured.

REFLECTIONS

Do you implement a process for checking the accuracy and completeness of records containing personal information?

- Do we give members an opportunity to update their personal information?
- How and when are our members made aware of these processes?
- Do we make use of a mechanism to monitor and track updates to personal information?
- Do we as employees ensure that records are, and remain, relevant, accurate and up to date?

3.6. 6th condition: Openness (Sections 17 & 18)

3.6.1. Notification

Section 17

A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in the Provisions of PAIA.

- This essentially entails the compilation and making available of a PAIA Manual in terms of section 51 of PAIA.

Section 18

If personal information is collected, except under certain limited circumstances where non-compliance with the provisions of POPIA is condoned, the responsible party must take reasonably practical steps to ensure that the data subject is aware of:

- the information being collected, and where the information is not collected from the data subject, the source from which it is collected;
- the name and address of the responsible party;
- the purpose for which the information is being collected;
- the name and address of the responsible party;
- the purpose for which the information is being collected;
- whether or not the supply of the information by the data subject is voluntarily or mandatory;
- the consequences of failure to provide information;
- any law authorising, or requiring the collection of the information;
- the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation, and the level of protection afforded to the information by that third country or international organisation; and
- any further information such as the:
    - recipient or category of recipients of information;
    - nature or category of the information;
    - existence of the right of access to and the right to rectify the information collected;
    - existence of the right to object to the processing of personal information as referred to in Section 11(3); and
    - right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator.

When must notification take place?

Directly from the data subject:

- before the information is collected, unless the data subject is already aware of the information referred to above.
- this could for instance be the case where the information that is collected is so obvious to the data subject that he must already know the identity of the responsible party and the purpose for the processing, e.g., where a data subject

Source other than data subject:

- As permitted in terms of Section 12(2) of POPIA.
- Before the information is collected, or as soon as reasonably practical after it has been collected.

Content of the notice:

The information required by POPIA in terms of condition 6 to be provided to a data subject will be included in a notice/notification given to the data subject. The information to be provided is unique to each responsible party (e.g., depending on the purpose for which it is collected), but the information to be provided to the data subject must be:

- necessary to enable the processing to be reasonable to the data subject, having regard to the specific circumstances in which the information is or is not to be processed; and
- must, as a minimum, contain the basic information referred to in section 18 of POPIA.

Way the notice is given:

The information included in the notice can be provided in many ways:

- Verbally;
- In writing;
- in a prominent position on an application or registration form;
- over the telephone where it is read to the data subject and the conversation is recorded;
- on a website when asking for updates or as part of the privacy policy, provided that the privacy policy which includes the notification is not merely an option which the member may or may not access - the notification should be visible on the screen and the member or prospective member must not be able to ignore it before he takes any further action such as asking for an update or submitting a request on the website to the responsible party, etc.

GENERAL EXPECTATIONS

Section 18(3) states that when a responsible party has previously complied with the steps required for notification and when he thereafter collects:

- The same information or information of the same kind;
- From the data subject; and
- Provided the purpose of collection of information remains the same, that responsible party will be deemed to have complied with the steps required for notification when the subsequent collection takes place.

SPECIFIC EXPECTATIONS

Section 18 (4) states that it is not necessary for a responsible party to comply with the steps required for notification, if:

- the data subject, or a competent person (e.g., his guardian) where the data subject is a child, has given consent for the non-compliance;
- non-compliance would not prejudice a legitimate interest of the data subject in terms of POPIA, (e.g., where a doctor in an emergency collects medical information of a runner from the Comrades Association);
- non-compliance is necessary:
    - to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences
    - to comply with an obligation imposed by law.
    - for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
    - in the interests of National Security (e.g., to fight terrorism).
- compliance would prejudice a lawful purpose of the collection, (e.g., where a hospital collects personal information regarding a patients' HIV status to purchase sufficient medication to treat patients and they suspect that the patients will not provide them with truthful information regarding their HIV status);
- compliance is not reasonably practical in the circumstances of the case, or
- the information will:
    - not be used in a form in which the data subject may be identified; or
    - be used for historical, statistical or research purposes.

IMPORTANT QUALIFICATION

Where personal information collected will NOT BE USED IN A FORM IN WHICH THE DATA SUBJECT MAY BE IDENTIFIED - no notification steps will be required

Information will be de-identified when such steps are taken which PREVENT ITS RECONSTRUCTION IN AN INTELLIGIBLE FORM

3.6.2. Anonymisation

Exclusions and Exemptions - Section 6

POPIA does not apply to the processing of personal information that has been deidentified to the extent that it cannot be re-identified again.

How is personal information de-identified in practice?

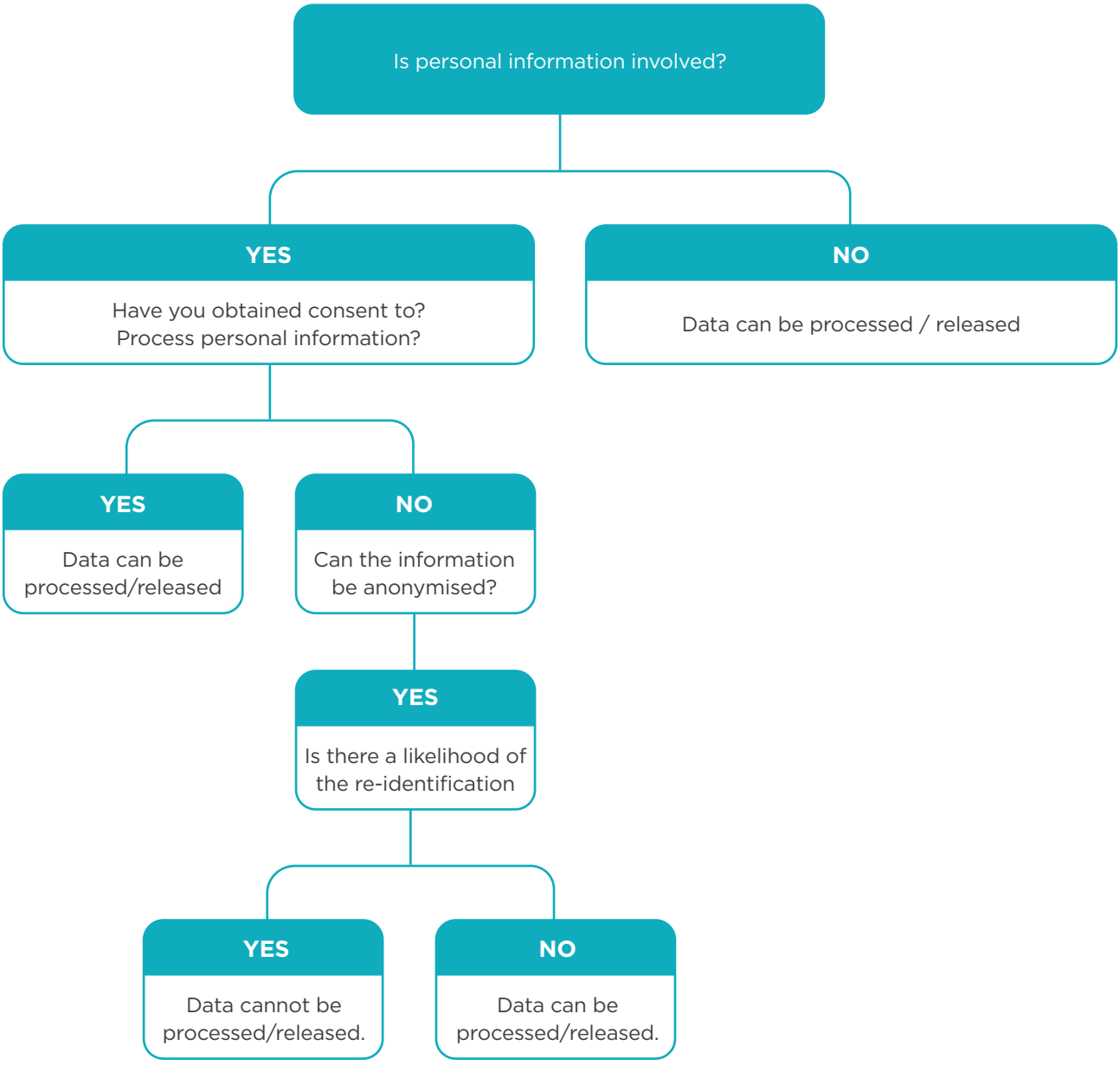
The first thing to consider is whether a complete anonymisation can be achieved in practice? For instance, what if we retain two sets of information, viz. the original personal information (before it has been stripped from personal identifiers) and a second set being the 'anonymised' information. One may argue that the fact that we are in possession of the 'anonymised' information which, if linked to the 'unstripped' personal information, will enable a natural person to be identified, means that all the information (stripped and unstripped), remains personal information to which POPIA applies.

The fact that we may have no intention of linking the two sets of information is irrelevant. On the other hand, if we destroy the original set of personal data then we probably ensure that there is no way of identifying individuals from the anonymised data. If the result of stripping is that information is produced which can no longer identify a particular individual, then such information ceases to be personal information which is subject to POPIA.

Direct & indirect identification

- There is a distinction between direct and indirect identification:
- Direct identification: Identity numbers, names, and surname etc.
- Indirect identification: Personnel numbers, e-mail addresses etc. in which it is possible that a person would use such information to identify a person.
- It can be difficult to determine whether data has been anonymised or is still personal information. This can call for sensible judgment based on the circumstances of the case in hand. In some cases, it will be relatively easy to determine whether it is likely that a release of anonymised data will allow the identification of an individual. In other cases, it will be much harder. A distinction must however be made.

DECIDING WHEN AND HOW TO PROCESS ANONYMISED DATA



REFLECTIONS

- Do you have a PAIA manual?
- Do you regularly review and update the manual?
- Have you appointed someone to be in contact with the information regulator in terms of PAIA?
- Do you use personal information for historical, statistical and research purposes?

3.7. 7th condition: Security safeguards (Sections 19 to 22)

Section 19:

This provision requires a responsible party to secure the integrity and confidentiality of personal information in its possession by taking appropriate, reasonable, and technical measures to prevent:

- Loss, damage, unauthorized destruction, unlawful access, or processing of personal information.

3.7.1. Key concepts:

Appropriate

This means that the measures to be taken to resist a specific risk which threatens the integrity and / or confidentiality of personal information should be suitable to provide that protection against unauthorised or unlawful processing of personal information.

Example: if the identified risk is a virus attack, then appropriate anti-virus software should be installed. It also means that if the personal information is of a very confidential nature, the greater the measures should be that are taken to protect the information.

Reasonable

The measures taken need to be proportionate to the nature of the personal information that will be processed, the possibility of confidentiality being breached and the damage that may be suffered resulting from any breach of confidentiality.

Technical Measures

This means password protection, biometric means of gaining access to information, firewalls, anti-virus software, encryption etc.

Organisational Measures

High security buildings/rooms where servers/files are stored, proper training of operators, implementing security policies, having proper back-up systems, employing operators who are reliable - not only the persons who process (e.g., collect or capture) the information but even those who provide technical support to the responsible party if they have access to the information.

3.7.2. What must the responsible party do?

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 (e.g., by regular testing of systems) that safeguards are effectively implemented; and
- ensure that the safeguards are continually upgraded in response to new risks or deficiencies in previously implemented safeguards, e.g., the updating of software such as anti-virus packages or back-up systems.

3.7.3. Security measures regarding 3rd parties

Where a responsible party uses the services of a 3rd party (described as an operator) to process personal information on its behalf, that operator, must:

- Process that information only with the knowledge or authorization of the responsible party; and
- Treat such personal information as confidential and may not disclose it, unless required by law. or during the proper performance of its duties.

Section 21 of POPIA:

- The responsible party must in terms of any written contract between it and any operator, ensure that the operator which processes personal information for it, establishes and maintains the same security measures as the responsible party is obligated to do in terms of POPIA.
- The operator must, in turn, notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

Agreements with 3rd parties:

All agreements with service providers must attempt to, inter alia, incorporate clauses dealing with the following:

- suitable indemnities;
- confidentiality clauses;
- warranties regarding the expertise of those service providers in safeguarding personal information;
- a clause obliging them to comply with Section 18 on a responsible party's behalf, i.e., to give the required notice (as prepared by the responsible party) to the data subject making him aware of the matters referred to in Section 18;
- reserving the right to audit compliance with service providers;
- including suitable undertakings whereby the service provider undertakes to comply with those obligations imposed on him in terms of POPIA;
- ownership in the personal data should be reserved by the responsible party and at termination of the agreement, the service provider should be obliged to return/ destroy such information; and
- an obligation should also be imposed on the service provider to assist the responsible party in giving access to or edit the personal information of a data subject at his request.

3.7.4 Information saved in the cloud.

A responsible party may not transfer personal information about a data subject to a third party who is in a foreign country UNLESS:

- the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that effectively upholds principles for reasonable processing of the information that are substantially like the conditions for the lawful processing of persona information;
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the responsible party; or
- the transfer is for the benefit of the data subject; or
- it is not reasonably practicable to obtain the consent of the data subject to that transfer and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

3.7.5. Notification

Where there are reasonable grounds to believe that personal information of a data subject has been accessed or acquired by an unauthorised person, the responsible party must notify:

- the Regulator; and
- the data subject unless the identity of such data subject cannot be established.

Notification must be made as soon as possible after discovery of the compromise, considering:

- The legitimate needs of law enforcement agencies (e.g., Hawks or the SAPS); or »»
- Any measures reasonably necessary to:
    - determine scope of security breach; and
    - restore integrity of the responsible party's information system.

What must the notice contain?

Notification to the data subject concerned must be in writing and communicated in terms of Section 22(4) – The notice must state:

- a description of the possible consequences of the security breach;
- a description of the measures that the responsible party intends to take, or has taken to address the security breach;
- a recommendation about the measures to be taken by the data subject to mitigate the possible adverse effects of the security breach; and
- if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

REFLECTIONS

- Do we appropriately manage the risks associated with processing personal information?
- Do we have an information security policy?
- Do we back up information on a regular basis?
- Do we employ sufficient identification and authentication control measure to limit access to personal information?
- Do 3rd parties process personal information on our behalf?
- How do we ensure that 3rd parties are able to process personal information?
- What manner of notification do we use in the event of personal information breaches?

3.8. 8th condition: Data subject participation (Sections 23 & 24)

Section 23 of POPIA

A data subject, having provided proof of his/her identity, has the right to:

- Request a responsible party to confirm (free of charge) whether it holds personal information about the data subject; and
- Request from it, the record or description of the personal information about the data subject held by it, including information about the identity of all 3rd parties (or categories) of 3rd parties who have, or have had access to the information:
    - Within a reasonable time;
    - At a prescribed fee, if any;
    - In a reasonable manner and form; and
    - In a form which is generally understandable

3.8.1. Prescribed fees

The responsible party is entitled to charge a prescribed fee for the disclosure of a data subject's personal information. They must then:

- Give the applicant a written estimate of the fee before providing the information; and
- May require the applicant to pay a deposit for all or part of the fee prior to such.

disclosure.

3.8.2. Refusal of access to records

In terms of section 23(4)(a) of POPIA:

- If the grounds for refusal of access to records set out in PAIA apply, then the responsible party may or must refuse (as the case may be), to disclose any of the requested information.
- Sections 62 to 70 of PAIA deal with the grounds for refusal of access to records of private bodies.

3.8.3. Correction of personal information

In terms of section 24(1), a data subject may request a responsible party to:

- Correct or delete personal information about a data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or
- Destroy or delete a record of personal information about the data subject that the responsible party is no longer authorized to retain.

In terms of section 24(3), if a responsible party has taken steps to correct, destroy or delete information as requested by a data subject and such actions will impact on decisions that have been, or will be taken in respect of the data subject in question, the responsible party must (if reasonably practical) inform each person or body or responsible party to whom the information has been disclosed, of the steps taken by it.

A responsible party, upon correcting, destroying, or deleting personal information, must:

- Notify the data subject that their request has been attended to – Section 24(2) (c);
- Notify the data subject concerned of the action taken – Section 24(4);
- Where an agreement cannot be reached between it and the data subject, and if the data subject so requests, then the responsible party must provide an indication that the correction of information has been requested but not made.

REFLECTIONS

- Do we afford your users an opportunity to amend their personal information?
- Do we notify individuals about the way they may access and update personal information?
- Do we charge any fees for accessing personal information?
- How do we verify the identity of persons who request access?
- Do we track requests for access to personal information?
- Do we verify the accuracy and completeness of personal information?
- Do we notify 3rd parties of updates, corrections, or deletion of personal information?

4. PROCESSING OF SPECIAL PERSONAL INFORMATION

4.1. Definition

In terms of section 26 of POPIA, "Special Personal Information" is defined as personal information comprising of information relating to a data subject's: »» religious or philosophical beliefs;

- racial or ethnic origin;
- trade union membership;
- political persuasion;
- health or sex life;
- biometric information; and
- criminal behaviour to the extent that such information relates to –
    - o an alleged commission of any offence; or
    - o any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

GENERAL EXPECTATIONS

As per section 27 of POPIA, the prohibition on processing special personal information does not apply if the:

- Processing is carried out with the consent of the data subject;
- Processing is necessary for the establishment, exercise, or defense of a right or obligation in law;
- Processing is necessary to comply with an obligation of international public law;
- Processing is for historical, statistical or research purposes to the extent that:
    - o The purpose serves a public interest and is necessary for the purpose concerned; or
    - o It would be impossible to ask for consent and sufficient guarantees are provided to ensure processing does not adversely affect the data subject's right to privacy.
- Information has deliberately been made public by the data subject; or
- The provisions of Sections 28 to 33 (as the case may be) are complied with.

4.2. Authorisations

Concerning data subject's:

SECTION 28	SECTION 29	SECTION 30
Religious or philosophical beliefs	Race or ethnic origin	Trade union membership

SECTION 31	SECTION 32	SECTION 33
Political persuasion	Health or sex life	Criminal behaviour or biometric information

4.3. Children

As per section 34 of POPIA, a responsible party may not process personal information concerning a child unless such processing complies with the provisions of section 35 of POPIA.

In terms of section 35, this prohibition does not apply if the processing is:

- carried out with prior consent of a competent person;
- necessary to comply with an obligation of international public law;
- for historical, statistical or research purposes to the extent that —
    - the purpose serves a public interest, and the processing is necessary for the purpose concerned; or
    - 0t appears to be impossible or would involve a disproportionate effort to ask for consent,
    - and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- of personal information which has deliberately been made public by the child with the consent of a competent person

GENERAL EXPECTATIONS

The Regulator may, by notice in the Government Gazette, authorise a responsible party to process the personal information of children. But only if the processing is in the public interest and safeguards have been put in place to protect the personal information of children.

4.4. The Regulator's condition.

The Regulator may impose conditions with regards to how a responsible party must upon request of a competent person provide a means for that person to: »» review the personal information processed; and

- refuse to permit its further processing.

The Regulator may impose conditions with regards to how a responsible party must provide notice:

- regarding the nature of the personal information of children that is processed; »» how such information is processed; and
- regarding any further processing practices

The Regulator may also impose conditions which dictate that a responsible party must:

- refrain from any action that is intended to encourage or persuade a child to disclose more personal information about himself than is reasonably necessary given the purpose for which it is intended; and
- establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.