Outline of Chapter 3 of the act

Chapter 3 expands fully on the lawful requirements provided for in the Act and is therefore fundamental to understanding what you may or may not do when it comes to the "processing of personal information" as defined.

NB - Once you commence applying the various prerequisites of the Act please note that the information provided below should then be read in conjunction with the applicable provisions of the Act before implementing any of the many requirements.

Part A

Processing of personal information in general

Part A of Chapter 3 provides for the lawful processing of personal information in general and sets out the 8 specific conditions under which processing may take place. These 8 conditions are fundamental to understanding the requirements of the Protection of Personal Information Act.

Condition 1 – Accountability

Section 8: Responsible party to ensure conditions for lawful processing

Pretty straight forward and essentially confirms the need to ensure that personal information is processed as set out in Chapter 3.

Condition 2 - Processing limitation

Section 9: Lawfulness of processing

Again straight forward - confirms the need to process the information lawfully and in a manner that does not infringe on the data subjects privacy

Section 10: Minimality

Short and to the point - personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

Section 11: Consent, justification and objection

Sets out a crucial principle -

The processing of personal information may only take place if –

- a competent person, where the data subject is a child, consents to the processing
- it is in the performance of a contract to which the data subject is party
- it complies with an obligation imposed by law
- it protects a legitimate interest of the data subject;
- the data subject consents to the collection
- it is necessary for the proper performance of a public law duty by a public body
- it is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

Important to note that the onus is on you, as the responsible party, for obtaining the data subjects consent when processing personal information and that if a data subject has objected to the processing on reasonable grounds, then you may no longer process the information providing that the lawfulness, if applicable, is not affected.

Section 12: Collection directly from data subject

Although Section 12 requires that you collect personal information directly from the data subject, it also provides you with various circumstances when this is not necessary.

For example, **amongst others**, when the information -

- is obtained from a public record
- has been made public by the data subject
- is obtained from another source and does not prejudice the legitimate interest of the data subject,
- maintains the legitimate interests of the responsible party to whom the information is supplied,
- is such that compliance would prejudice a lawful purpose
- is such that compliance is not reasonably practicable in the circumstances of a particular case.

Condition 3 - Purpose specification

Section 13: Collection for specific purpose

Section 13 provides that personal information be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the public or private body.

In addition, the public or private body must take steps to notify the data subject when collecting personal information in a manner as set out in section 18(1) to (3) unless the provisions of section 18(4) apply. [see condition 6 below]

Section 14: Retention and restriction of records

This section provides that personal information must not be retained any longer than is necessary for achieving the purpose for which it was collected or subsequently processed.

However there are a number of exceptions to this requirement as set out in subsections 1 to 8. An example of an exception would be the retention of a record that is required or authorised by law such as the specific information recorded on guest registration forms which, in terms of the Immigration Act and Regulations, must be retained for 2 years.

Section 14 is the key when it comes to the personal information that you currently have on record which may have been collected and stored over a number of years. It is a must that you read through subsections 1 to 8 and identify those exceptions and or conditions that apply to the personal information you currently retain and take the appropriate action.

Special note - subsection 14(4) & 14(5)

> 14(4) A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2).
>
> 14(5) Destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form

When it comes to deleting personal information recorded and retained by an automated IT processing programme/system, it would be wise to consult your IT service provider re the best way to "prevent its reconstruction in an intelligible form". Just deleting the information may not be sufficient.

Condition 4 - Further processing limitation

Section 15: Further processing to be compatible with purpose of collection

Deals with the processing of personal information in a manner which differs from what was intended when it was originally collected – referred to as "further processing"

If you plan to use any of the personal information you have on record for a purpose other than the one it was originally obtained for, then you need to read through section 15.

Condition 5 - Information quality

Section 16: Quality of information

You need to take reasonable steps to ensure that the personal information you have on record or plan to collect in the future is complete, accurate, not misleading and updated where necessary relative to the purpose for which it was collected.

Condition 6 - Openness

Section 17: Documentation

A responsible party (you) must maintain the documentation of all processing operations under its responsibility as referred to in section 51 of the Promotion of Access to Information Act. Section 51 deals with the compilation of a manual as provided for in the Promotion of Access to Information Act. An example of the Promotion of Access to Information Act manual can be obtained from your FEDHASA regional office.

Section 18: Notification to data subject when collecting personal information

An extremely important section if you collect any personal information from a data subject. You as the responsible party are obliged to ensure that the data subject is aware of the details as set out in sub-sections 1 (a) to (h). It would be wise, as an example, to take these requirements into account when setting out any terms and conditions or redesigning your guest reservation and or check in registration forms. Take specific note of subsection 1(h)(i) to (v).

Sub-section 4(a) to (f) provides exceptions to the compliance requirements set out in sub-section 1

Condition 7 - Security safeguards

Section 19: Security measures on integrity and confidentiality of personal information

You as the responsible party must protect personal information against unauthorised destruction, unlawful access and unlawful processing. In order to achieve this, you will need to identify all the reasonably foreseeable internal and external risks and implement appropriate measures to mitigate these risks. In addition, you will need to constantly review these measures and update them when required. You will also need to consider any general and or industry specific accepted information security practices and procedures.

Section 20: Information processed by operator or person acting under authority

Anyone processing personal information on your behalf must do so only with your express knowledge and consent and must treat the information as confidential and must not disclose it unless required to do so by law or in the proper performance of their duties.

Section 21: Security measures regarding information processed by operator

You must ensure that a written contract is in place with the authorised operator(s) confirming that they understand the need to maintain all of the measures as set out in section 19 above and that they, the operators, must notify you the moment they suspect that personal information has been accessed or acquired by an unauthorised person

Section 22: Notification of security compromises

If there are reasonable grounds to believe that the personal information has been accessed or acquired by an unauthorised person, the responsible party must notify the Regulator and the data subject (unless the identity of the data subject cannot be established). Notification must be made as soon as is reasonably possible taking into account the needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system. You may only delay the data subject notification if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation.

Section 22 Sub-sections (4)(a) to (e) and (5)(a) to (d) set out how you should contact the data subject and what information you must provide the data subject. Sub-section (6) sets out when the Regulator might require you to publicise the breach.