PROTECTION OF PERSONAL INFORMATION LEGISLATION

The Act and Regulations came into effect on 1 July 2020 and provided a 12-month grace period for implementation through to the 1 July 2021

This Protection of Personal Information guide is made up of three documents.

Document 1 – Broad guidelines on how to go about implementation - ten key steps

Document 2 – Simplified summary of the key sections provided for in the POPIA legislation

Document 3 - Combined Act and Regulations

The contents of document 1 are set out below and the contents of documents 2 and 3 can be viewed and downloaded from the FEDHASA website.

Document No 1

Broad implementation guidelines – 10 key steps

Introduction

The Protection of Personal Information legislation [POPIA] will affect businesses in varying ways – unfortunately it is not a case of one size fits all. The first two documents, as mentioned above, serve as basic guides and are intended to point you in the right direction as far as compliance and implementation is concerned.

The various comments, observations and recommendations set out in these guides have been provided with small business in mind rather than the large and or corporate establishments and organisations that undoubtedly have the expertise, manpower and financial resources to administer the requirements either internally or externally.

As legislative consultant to FEDHASA, it should be noted that I am not a lawyer and that comments expressed in this document does not represent a legal opinion but my own personal point of view.

WHERE DO I START?

Probably the first thought that will come to mind when confronted with this lengthy statute, is where to begin and in what order to address the multitude of requirements when it comes to the lawful processing of personal information.

Examples of personal information that you currently process and keep on record will likely be, amongst others,

- ✓ Employee personal information
- ✓ Owners, partners, directors and board members personal information
- ✓ Guest reservation and registration records,
- ✓ Guest invoicing and payment information,
- ✓ Guest marketing, sales and promotional information,
- ✓ Guest loyalty programme information,
- ✓ Guest COVID-19 personal contact records,
- ✓ Supplier information (if a natural or juristic person)

Below is a suggestion on how you might tackle the requirements of the legislation, set out in what I hope you will find as a logical sequence. But of course you are quite entitled to go about it in any manner that suites you and your business.

The various links in the 10 steps set out below will take you to the appropriate summarised section in document 2.

Step 1

Read through the definition of "Personal Information" and "Processing" (document 2 section 1) in order to familiarise yourself with the scope of the data defined as personal information and what the processing of this information entails. You will note that they cover just about every possible form of personal information imaginable and a multitude of processing activities.

Step 2

Have a quick look at Section 3 and section 4 (document 2) which provide for the application and interpretation of the act and the lawful processing of personal information; refer to the automated and or non-automated processing of personal information as it applies to all local and foreign organisations processing personal information in South Africa and to the conditions and prohibitions applicable to the processing of personal information.

Step 3

I would suggest that you now set aside some quiet time in order to read through the summary of Chapter 3 in document 2 which provides an outline in layman's language (where possible) of all of the conditions for the lawful processing of personal information. No need to make any notes at this stage unless you would like to. The idea is to read through it in order to familiarise yourself with the scope and content of the Chapter. Personally I found a number of headings to be a little misleading as they do not necessarily convey the extent and or specific content of a particular section.

Step 4

Having completed steps one to three now commence an audit by listing all of the types of personal information you currently process and or have on record, under the following suggested headings –

Business ownership/partnership personal information

Likely to be personal information set out in contact information, statutory registration requirements, insurance matters, financial matters, contractual agreements and general information concerning partners, owners, directors and or board members

Employee information

Likely to be personal information that relates to – contact details; employment & remuneration records; tax, PAYE, UIF, compensation fund registration information and payment records, employment equity & skills development records, job descriptions, bargaining council information if applicable, pensions, provident funds, medical aid, loan agreements, disciplinary information, professional driving permit & public operating licence applications and records and any other statutory requirement detailing personal information.

Guest reservation and registration information

Likely to be personal information that relates to – statutory registration requirements; COVID personal contact details; billing and payment details; loyalty programmes; marketing and promotional particulars and guest histories.

Supplier information

You need only review and list those suppliers for whom you have recorded and retained personal information – will probably be SMME's in the main. Likely to be personal details and contact information

Additional guest/other personal information

Any additional personal information that you have retained or continue to obtain besides those listed above.

How the information is arranged is up to you but it would be an idea to take into account the three headings listed in step five.

Step 5

Now take the audited personal information from step 4 and separate the various records into the following suggested categories –

- Statutory requirement (required by law)
- Operational necessity (an example would be account payment information)
- Marketing, promotional, nice to have, not sure why I have it or other?

Step 6

Once you have completed the above, the next suggestion would be for you to go through the statutory and operational necessity categories and ensure that the information recorded and retained is exactly as required by law and that the operational information is adequate, relevant and not excessive (document 2 section 10) and that no unnecessary additional personal information has found its way into the records over time.
Double check the validity of the information you have under these two categories by applying what could best be described as a litmus test "Consent, justification and objection" (document 2 section 11)

Step 7

Now it's time to take a close look at the remaining personal information category - "marketing, promotional, nice to have, not sure why or other". Firstly read through the provision dealing with "Direct marketing by means of unsolicited electronic communications" in section 69. (document 2). Then make use of section 11 "Consent, justification and objection" (document 2) as the litmus test once again.

Step 8

Now comes the challenging part.
Any personal information highlighted in "marketing, promotional, nice to have, not sure why or other", or "statutory" and or "operational necessity" that falls foul of any provision of the Act will need to be addressed.

Essentially there are only three options open to you –

1] Obtain the data subject's written permission to continue using the specific unauthorised personal information. Would probably need to email her/him if possible and or practical

2] Destroy or delete enough of the information in a manner that prevents its reconstruction any intelligible form.

3] Completely destroy the information

When it comes to deleting personal information recorded and retained by an automated IT processing programme/system/computer, it would be an idea 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.

The Act does not state how the information should be destroyed but requires that it should be in a manner that ensures that the data subject can no longer be identified. (Section 14)

Step 9

Having sorted out the current personal information you have on record you will no doubt have a good idea as to what personal information you intend lawfully recording and retaining into the future. With this in mind it would be an idea to set out a written policy for both you and your senior employees providing for the following –

1] The lawful personal information you intend to record/retain going forward under the following headings -

- Statutory requirement
- Operational necessity
- Other

2] Any changes you intend making to the method/format of recording personal information going forward (examples perhaps being your guest reservation and registration forms and contents of your employee files)

3] The method by which you intend notifying the data subject why certain statutory / operational / other information is being collected and the method by which you intend recording the data subject's permission in the event that "other/voluntary" personal information is collected.

4] The method by which you intend securing (document 2 section 19) all personal information currently on record and the information you intend recording in the future.

Suggestions –

- Reduce the number of employees handling or with access to personal information
- Audit current places of storage and the level of security
- Reduce the storage areas if possible
- Set up a secure storage system – if stored on line get some IT advice
- If stored manually audit the strength, access and safety of the system.

5] A record of persons/employees who have been given the responsibility to record, store and secure personal information. Section 20 and section 21 (document 2)

6] The manner in which you intend handling a breach of security and or if personal information has been accessed or acquired by an unauthorised person Section 22 (document 2)

Step 10

Finally you will need to read through the guidance and procedures applicable to information officers and in addition register the information officer and or deputy information officer (if applicable). See section 55 and 56 in document 3 and in addition download the recently published Guidance Note at - https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf
In order to register the information officer and or deputy information officer you can download the application form at https://www.justice.gov.za/inforeg/docs/InfoRegSA-eForm-InformationOfficersRegistration-2021.pdf

NB – The Information Regulators website currently (mid May 2021) states the following – *"The commencement for Registration of Information Officers is May 2021 and this is not the deadline for registration. Existing Responsible Parties may register until the end of June 2021 to ensure POPIA compliance, however, we encourage registration as soon as the portal is up and ready."*

At present the portal has not been activated so keep an eye open.

The Information Regulator website can be found at https://www.justice.gov.za/inforeg/
