Masthead DIY POPI Act Compliance Toolkit

Guideline

All rights reserved. The material contained in this document is copyrighted and belongs to Masthead (Pty) Ltd, unless otherwise indicated. No part of the material may be reproduced, distributed, or transmitted in any form or by any means, including, photocopying, recording, or other electronic or mechanical methods without the prior written permission of Masthead.

Contents

Masthead DIY POPI Act Compliance Toolkit© 2020 Masthead (Pty) Ltd

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

Introduction to Masthead

Masthead (Pty) Ltd was launched in 2004 on the eve of the implementation of the Financial Advisory and Intermediary Services (FAIS) Act. We are specialists in the provision of compliance to Financial Services Providers and is the largest compliance services provider in South Africa. We have extended our offering over the years to include corporate FSPs in South Africa, including financial services businesses in Hong Kong, Singapore, and Dubai. The service delivery includes consulting, implementation support, monitoring, and training, and these services are delivered through a national network of compliance and practice management professionals.

Please see the Masthead website for further details regarding our full value proposition: https://www.masthead.co.za/.

Masthead extended its offering to include compliance with the POPI Act and has developed a DIY POPI Act Compliance Toolkit, to provide guidance to a business and its employees in this regard.

Compliance with the Requirements of the POPI Act

The President of South Africa has proclaimed the commencement date of most of the sections of the Protection of Personal Information Act, 4 of 2013 (the 'POPI Act' or 'the Act'), to be 1 July 2020. As per section 114 of the Act, all processing of personal information must, within one year after commencement, be made to conform to the Act. A grace period of 12 months from 1 July 2020 is hence given to comply with the Act – therefore, all persons and entities must be fully compliant with the provisions of the Act by 1 July 2021.

The Act requires everyone, especially businesses and organisations, to lawfully process the personal information of data subjects (both natural and juristic persons).

Since the POPI Act is more principle-based than rule-based, it is important to bear in mind that there is more to compliance than checking a few boxes. POPI Act compliance is about applying the very best standards in taking responsibility for clients' personal information to avoid regulatory sanctions and maintaining the trust and respect of clients and the general public. Although the term compliance is used, it is all about effective and ongoing Data Privacy Management and breaches risk reduction.

To achieve this, it is important to study the POPI Act, Regulations and Regulatory Guidelines (all available on the Information Regulator's website (https://www.justice.gov.za/inforeg/) to familiarise the business with the detailed requirements thereof in conjunction with using the guidelines provided in this DIY Toolkit.

The Purpose of the DIY POPI Act Compliance Toolkit

Welcome to the implementation journey to become POPI Act compliant. Although the DIY POPI Act Compliance Toolkit cannot ensure the business' full compliance with the Act (since compliance is achieved by continuous implementation and review of all activities and mitigation mechanisms), it should greatly assist with the process. The DIY POPI Act Compliance Toolkit includes a POPI Act Compliance Framework in an Excel spreadsheet format which consists of a checklist of 49 (forty-nine) activities that, depending on the size and scope of the business, need to be implemented to ensure mitigation of data breach risks, effective Data Privacy Management and compliance with the POPI Act. The business can

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

use the templates, descriptions, and guidelines provided to implement the relevant activities suitable to the business.

The examples used in the DIY POPI Act Compliance Toolkit may not be suitable for different industries and business sectors.

Description of the DIY POPI Act Compliance Toolkit contents

Toolkit Item	Documentation	Reference Tool	Step
1	Status Quo Needs Analysis Questionnaire	1	1
2	A Practical Understanding of POPI Act Implications and Opportunities for Your Business	2	2
3	POPI Act Compliance Framework Activity Checklist Template	3	3
4	A Standard POPI Act Privacy Policy Statement Template	4	3
5	Practical Communication Tips and Considerations Guideline Reference Document	5	3
6	Personal Data Inventory Template	6	3
7	Information Flow and Risk Mitigation Assessment Template	7	3
8	Data Privacy Risk Impact Assessment Considerations Guideline Reference Document	8	3
9	Managing Third-Party Risks and Third-Party Operator Engagement Strategy Guideline Reference Document	9	3
10	Procedure for Handling Requests for Personal Information Reference Document	10	3
11	Breach Management Considerations Guideline Reference Document	11	3
12	Bank of Frequently Asked Questions Reference Document	12	3

Introduction to the DIY POPI Act Compliance Toolkit

The DIY POPI Act Compliance Toolkit is aimed at starting and/or supporting the business' POPI Act compliance processes. Ensure that the business understands the purpose of each activity and document, as well as the contents thereof. The DIY POPI Act Compliance Toolkit can be used in the following manner:

1. Assess the current status quo of the business by completing the Status Quo Needs Analysis Questionnaire (Reference Tool 1). Assess the information obtained from the questionnaire and discuss this with the management team and employees (where applicable), agree and communicate the best options for the business, taking into account the risks for the business.
2. Consider and take employees through the presentation: A Practical Understanding of POPI Act Implications and Opportunities for Your Business (Refer to Reference Tool 2). When communicating with the employees regarding the POPI Act it is important to stress that it should be seen as part of everyday business and a good business (governance and risk management) practice and function, involving opportunities to retain the trust of existing clients and business partners and gain the trust of potential new clients, including all other business stakeholders.
3. Complete the POPI Act Compliance Framework Activity Checklist Template (Reference Tool 3). Ensure that the business understands what each activity means and requires and plan the compliance journey and process using the template.

Masthead DIY POPI Act Compliance Toolkit© 2020 Masthead (Pty) Ltd

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

4. Implement and constantly maintain and review the activities in the POPI Act Compliance Framework Activity Checklist Template (Reference Tool 3).
5. Incorporate the POPI Act requirements into the business' Operations Manual and maintain and review policies and procedures on an ongoing basis.
6. Monitor and record processes at least weekly or bi-weekly at the start.

A step-by-step guideline is provided below on how to use each reference tool provided in the DIY POPI Act Compliance Toolkit below.

Step 1: Status Quo Needs Analysis and Questionnaire

This document is used to establish the current business status quo, level of understanding, capacity, and needs, to enable an efficient compliance process.

Step 2: A Practical Understanding of POPI Act Implications and Opportunities for Your Business

The presentation, A Practical Understanding of POPI Act Implications and Opportunities for Your Business (Reference Tool 2) is used to establish awareness with management and the employees about the POPI Act and Data Privacy Management.

Here are some important highlights in this regard:

The main purpose of the POPI Act is to give effect to section 14 of the Constitution of the Republic of South Africa, which makes provision for the right to privacy and, therefore, imposes an obligation on a responsible party to put measures in place to safeguard personal information when processed by a responsible party and to regulate the use of personal information (as defined by the POPI Act and summarised below) and to provide for adequate security measures to protect personal information and the manner in which the different parties in a relationship will have to comply with these measures. Therefore, these roles are important to consider as they have a profound impact on the relationships between responsible parties and operators and also affect the way in which information is processed and used.

What do the following terms mean[1]?

- '**responsible party**' means 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.
- '**operator**' means 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.
- '**processing**' means any operation or activity or set of operations, whether or not by automatic means, concerning personal information, including–
  (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
  (b) dissemination by means of transmission, distribution or making available in any other form; or
  (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
- '**personal information**' means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to–

[1] Chapter 1 Definitions in the Protection of Personal Information Act 4 of 2013

Masthead DIY POPI Act Compliance Toolkit© 2020 Masthead (Pty) Ltd
Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b) information relating to the education or the medial, financial, criminal or employment history of the person;
(c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) 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;
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Conditions for lawful processing

The POPI Act provides **eight conditions for lawful processing**. Think of these as legally binding principles that must underpin all processing of personal information within your business. (The S8 for example in Condition 1 refer to section 8 of the POPI Act, so does S9 refer to section 9, etc.).

The conditions for lawful processing can be summarised as follows:

- **Condition 1: Accountability:** S8 Responsible party to ensure conditions for lawful processing.
- **Condition 2: Processing limitation:** S9 Lawfulness of processing, S10 Minimality, S11 Consent, justification, and objection, S12 Collection directly from the data subject.
- **Condition 3: Purpose specification:** S13 Collection for a specific purpose, S14 Retention, and restriction of records.
- **Condition 4: Further processing limitation:** S15 Further processing to be compatible with the purpose of the collection.
- **Condition 5: Information quality:** S16 Quality of information.
- **Condition 6: Openness:** S17 Documentation, S18 Notification to the data subject when collecting personal information.
- **Condition 7: Security safeguards:** S19 Security measures on integrity and confidentiality of personal information, S20 Information processed by operator or persons acting under authority, S21 Security measures regarding information processed by an operator, S22 Notification of security compromises.
- **Condition 8: Data subject participation:** S23 Access to personal information, S24 Correction of personal information, S25 Manner of access.

- It is appropriate to consider the volume and types of personal information processed, stored, collected, and shared by the business and where it is stored e.g. the business may be **storing** personal information in paper files, on hard disks, on the web servers.
- The business might be **collecting** personal information via web forms, cookies, and email.
- The business could be **sharing** personal information with e.g. accountants, product suppliers, marketing companies, analytics providers, and mail carriers.

These are just a few examples. Think carefully about personal information flows within your business. You can't comply with the requirements of the POPI Act unless you know what personal information is in your control.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

The implementation of all compliance guidance activities must be done thoroughly, and it is important to understand that it will take time, resources, and responsibility for all management and staff.

Step 3: POPI Act Compliance Framework Activity Checklist

The POPI Act Compliance Framework Activity Checklist Template (Reference Tool 3) serves the purpose of guiding the implementation of compliance-related activities and related planning. Once it has been completed, the business will have a better understanding of what activities need to be addressed and the related capacity and time requirements to implement each activity. It can act as a framework for your compliance (as required by section 4(1)(a) of the December 2018 Regulations), effective Data Privacy Management, and breach risk reduction.

The activities in the checklist are addressed, in broad, below. Work through each of the activities and the applicable reference tools, and assign responsibilities within the business with clear timelines, and instructions on each of them where it applies to the business.

1. Governance

1.1 Confirm Information Officer or Designated Deputy Information Officer and register them with the Regulator

Notes:

Refer to the definition of an Information Officer in Chapter 1 of the POPI Act: 'Information officer' of, or in relation to, a–

(a) Public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or
(b) Private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act 2 of 2000 (PAIA).
(c) Section 1 of PAIA defines the 'head' of, or in relation to, a private body to mean–
    (a) In the case of a natural person, that natural person or any person duly authorised by that natural person;
    (b) In case of a partnership, any partner of the partnership or any person duly authorised by the partnership;
    (c) In the case of a juristic person–
        a. (i) the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or
        (ii) the person who is acting as such or any person duly authorised by such acting person.

Refer to the Responsibilities of Information Officers in section 4 of the Regulations relating to the Protection of Personal Information issued by the Information Regulator – Government Gazette 14 December 2018 and refer to the future Regulator Guidelines issued in this regard. Please use the following link: https://www.justice.gov.za/inforeg/

It is very important that compliance is not only the responsibility of the Information Officer and Deputy Information Officer, where applicable. Everyone in the business is equally responsible to ensure **compliance and breach risk reduction** since Data Privacy Management is a business function, not only a compliance process.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

Steps to follow:

- Confirm internally who the Information Officer is, as defined by the POPI Act and PAIA.
- Assign the Deputy Information Officer, if applicable (normally for larger businesses).
- Register the Information Officers with the Regulator in accordance with the prescribed process and templates issued by the Regulator.

1.2 Allocate roles and responsibilities

Notes:

Roles and responsibilities in this context are specific to allocating roles and responsibilities during the process of using the DIY POPI Act Compliance Toolkit item to ensure that specific activities are allocated to specific individuals who will be responsible to ensure that such an activity is fully implemented by the completion date. Therefore, ensure that each person involved in the business to whom responsibilities are allocated, is aware of their roles and responsibilities in this regard. They are accountable for the functions or activities, but compliance and effective Data Privacy Management is everyone's business. It should be stressed again that addressing the activities (or completing them once) will not ensure compliance but implementing and reviewing them continuously and effectively will.

Steps to follow:

- Allocate roles (e.g. who the Deputy Information Officer is, who deals with the Regulator, who addresses relevant queries, who is responsible for communication, etc.).
- Allocate responsibilities for specific activities and plan for their completion and maintenance. Continuously review and re-allocate roles and responsibilities, as and when required.

1.3 Draft a standard Privacy Policy Statement

Notes:

Draft a Privacy Policy Statement using the Standard POPI Act Privacy Policy Statement Template (Reference Tool 4) as a guideline. The template is designed to satisfy the requirements of the POPI Act regarding the way the business treats the processing of personal information of others and their privacy. It can be seen as a promise to clients regarding the way in which their personal information is treated. It should be written in clear, plain language and made available to all the clients of the business e.g. via the business website. By doing this, the business can use it as a mechanism to gain trust from their clients and business stakeholders. It is important to ensure that the business can commit and adhere to each statement in the policy statement.

Steps to follow:

- Draft or finalise the business Privacy Policy Statement and use it as a separate document and/or include it into other relevant business documentation.
- Share the policy document on the website, in newsletters, and other communication with the business' clients and stakeholders, as required.

Masthead DIY POPI Act Compliance Toolkit© 2020 Masthead (Pty) Ltd

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

1.4 Report to external stakeholders on the status of Data Privacy Management (e.g. clients, third parties), through newsletters, response to requests, etc.

Notes:
Keep clients and business stakeholders informed regarding the business' POPI Act compliance and good Data Privacy Management practices. Look at the Practical Communication Tips and Considerations Guideline Reference Document (Reference Tool 5) to implement mechanisms and possible templates to communicate with the business clients, third parties, and general queries.

Steps to follow:
- Decide to whom and how frequently reporting will occur.
- Decide on the mechanisms and possible templates for the reporting.
- Implement the above.

1.5 Develop and maintain Communication Protocols regarding your Data Privacy Management policy and procedures

Notes:
Standardise as far as possible communication messages and mechanisms regarding POPI Act compliance and related activities, requirements, and queries by using the Practical Communication Tips and Considerations Guideline Reference Document (Reference Tool 5). Communication in this regard can either be adding to business risks (if ineffective) or it can greatly reduce risks if addressed effectively and in a standardised manner. Communication Protocols include the following elements:
- Communication requirements: What are the different reasons for communication and who are the audiences?
- Standardised communication messages for each type of requirement.
- Standardised communication mechanisms (emails, newsletters, etc.).

Steps to follow:
- Develop Communication Protocols.
- Implement and maintain the protocols.
- Update the protocols as and when circumstances or requirements change.

1.6 Include Data Privacy Management into management meetings and relevant reports

Notes:
Ensure that Data Privacy Management (and, therefore, POPI Act compliance) is considered as a critical business function and part of business risk management, and is included in relevant meeting agendas and reports.

Steps to follow:
- Decide in which meetings and reports (internal or external – as may be required by other functions or stakeholders) the item should be added.
- Implement and maintain.

Masthead DIY POPI Act Compliance Toolkit© 2020 Masthead (Pty) Ltd
Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

1.7 Require employees to acknowledge and agree to adhere to the Data Privacy Management requirements

Notes:
To ensure employee commitment, accountability, and compliance, update job descriptions with the Data Privacy Management Requirements. This can be done by adding an addendum to their current employment contract.

Steps to follow:
- Review job descriptions for each employee.
- Formulate standard requirements for all employees, such as a commitment to adhere to the business policies and protocols in this regard.
- Formulate specific requirements for employees tasked with specific Data Privacy Management related activities, as allocated in the activity list or otherwise.
- Confirm accountability requirements and possible penalties (including disciplinary hearings and accountability for financial losses) for non-adherence of breaches, due to the high risk and implications of POPI Act penalties and fines.

2. Awareness and Training

2.1 Undergo data privacy awareness and training for management and employees

Notes:
Establish and maintain the knowledge and capacity required to understand the requirements and implications of the POPI Act and effective Data Privacy Management. Take note of the responsibilities of the Information Officer as per section 4(e) of the Regulation issued by the Regulator – Government Gazette 14 December 2018. Although this refers to 'internal awareness', a standard good Data Privacy Management requirement is also to undergo and provide proper training in this regard. Ensure that effective recordkeeping is maintained of said training and awareness sessions.

Steps to follow:
- Use the presentation, A Practical Understanding of POPI Act Implications and Opportunities for Your Business (Reference Tool 2) as an initial training and awareness document.
- Visit the Masthead Learning Centre website at https://portal.masthead.co.za/ and have a look at our Webinars and Online Learning. Enrol for either the Everything You Need to Know and Do to Become POPI Compliant Webinar or POPI Online Course for further training.
- Encourage further and more detailed (or in-depth on specific aspects) training, as may be identified and required, depending on the business resource capacity.
- Contact Masthead via the 'Get In Touch' option on our website should you require further training and assistance. Alternatively, should the business be a Masthead member, contact the relevant Masthead regional office.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

3. Personal Data Inventory

3.1 Develop and maintain an inventory of personal data

Notes:
The purpose of the Data Inventory is to record the type of personal information and by creating an inventory of the type, categories, and classification of the personal information, it assists the business to consider how it processes each of the categories noted in the Personal Data Inventory Template (Reference Tool 6). The POPI Act requires that 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.

Refer to page 6 for the definition of [1]Personal Information in Chapter 1, of the POPI Act.

Steps to follow:

- Map a list of all the processing activities in the business.
- Make a list of the following:
    - all the different specific types of personal data (for example email addresses, telephone numbers, and bank account numbers) that the business processes,
    - how much personal information is being processed, and
    - where it is stored (in files in a safe, in files on the business laptops or computers, in a system, or the Cloud).
- Use the Personal Data Inventory Template (Reference Tool 6) as a guideline and adapt, change, and add information where necessary.

3.2 Classify personal data by type

Notes:
As a business, ask the question: what types of information does it process? Any information that identifies a person is personal information. Any information that by itself or together with other information identifies a person, is personal information. If the information does not identify a person, it is not their personal information. In most businesses, most information is linked to a client and is, therefore, personal information.

Personal information covers more than a client's name, telephone number, and address. For example, it deals with financial, employment, and criminal history. It also includes “a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. It also deals with the issue of any correspondence that the business might send its client and whether it will be classified as personal information or not.

Many other types of personal information are not provided as examples. If the business is going to make a list of the types of personal information that is being processed, it needs to refer to the types of personal information collected by the business.

Masthead DIY POPI Act Compliance Toolkit© 2020 Masthead (Pty) Ltd
Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

Steps to follow:

- Complete this activity together with 3.1 and classify the personal information in categories, e.g. Personal Information, Special Personal Information, Financial Information, etc. (See sections 26–33 of the POPI Act).
- Use the list in the Personal Data Inventory Template (Reference Tool 6) and add or adjust where necessary.

3.3 If transborder data is processed, ensure compliance with the Act, but also with privacy legislation or regulations of affected countries

Notes:

Specifically, consider the processing of transborder data and if other countries' legislation needs to be complied with. Although there are many similarities between the requirements of the POPI Act and, for example, the European Union General Data Protection Regulation (EU GDPR), specific differences and requirements need to be carefully considered. See section 72 in the POPI Act on the processing of transborder data.

Steps to follow:

- Consider how transborder data is being processed.
- Record it in the Personal Data Inventory Template.
- Study and consider (and obtain specialist advice or support regarding, if required) the requirements of section 72 of the POPI Act and that of any other countries' legislation or regulations.
- Implement the requirements of the above legislation or regulation.

4. Embed Data Privacy into Operations

4.1 Record data flows (e.g. between systems, between processes, between countries, to and from third parties) and related mitigation activities

Notes:

Consider what personal information enters and flows through the business and how it is processed to assess and mitigate possible compliance and breach risks. This is a critical and time-consuming activity that needs to be given priority and focussed capacity and attention to ensure optimal breach risk reduction.

Steps to follow:

- Use the Information Flow and Risk Mitigation Assessment Template (Reference Tool 7) to record data flows and related risks and implement them.
- Identify, plan for, and implement risk mitigation and treatment activities.

4.2 Consider lawfulness of collection and processing of personal information in terms of minimality, purpose and prior authorisation and further processing requirements

Notes:

Ensure that personal information is lawfully and responsibly processed. This is a continuous privacy risk-based thinking and implementation approach. It is a continuous business function and not an ad-hoc compliance consideration.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

Steps to follow:

- Study and ensure a clear understanding of the requirements of the POPI Act and other relevant legislation or regulations.
- Use the Information Flow and Risk Mitigation Assessment Template (Reference Tool 7) to complete and maintain.
- Consider the lawfulness of the collection and processing of personal information on an ongoing basis.

4.3 Develop and maintain records of the transfer mechanism used for data flows

Notes:

Consider and record personal information data transfer flows.

Steps to follow:

- Use the Information Flow and Risk Mitigation Assessment Template (Reference Tool 7) to complete and maintain.

4.4 Assess software systems for compliance processing

Notes:

Consider potential risks when using software systems when processing personal information. Adapt to ensure compliance breach risk reduction. Consider obtaining inputs from Information Technology Specialists in this regard.

Steps to follow:

- Use the information captured in the Personal Data Inventory Template (Reference Tool 6) and the Information Flow and Risk Mitigation Assessment Template (Reference Tool 7) to identify what personal information is captured and processed through the use of software systems.
- Consider how the system processes personal information.
- Consider how secure access to the system and the data in it is.
- Consider with whom and how the system shares the personal information.
- Consider who the system developer and owner(s) are in terms of their reputation and their system security commitments.
- Consider potential risks in any of the above elements and identify system change requirements or mitigation mechanisms.
- If the system is the owner and is administered by an operator or third party, address the requirements with them as per 4.6 below.

4.5 Review all agreements for compliance with the Act

Notes:

Obtaining legal advice as part of this process is advisable.

Steps to follow:

- Consider all agreements where the processing of personal information may apply.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

- Consider all clauses in the agreements and measure that against the Conditions in the POPI Act and the lawful processing requirements, as addressed above.
- Consider potential risks in any of the above elements and identify system change requirements or mitigation mechanisms.
- Address possible required amendments to the agreements, as or if required, to comply with lawful processing or where personal information flow risks (done through the implementation of the agreement[s]) are identified, to mitigate such risks.
- Amend the agreements as required.

4.6 Conduct Privacy Risk Impact Assessments and update the Risk Register

Notes:
Consider and mitigate risks pertaining to Data Privacy Management as set out in the POPI Act, sections 19 and 109(3)(g). It should be noted that although section 19 of the POPI Act refers to 'security measures' it is self-evident and in line with international best practices in Data Privacy Management (of which Information Security Management is a subset) that considering risks pertaining to data breaches involve much more than only security considerations.

Steps to follow:
- Use the Data Privacy Risk Impact Assessment Considerations Guideline Reference Document (Reference Tool 8) as a guideline and assess and mitigate risks.
- Update the Risk Register.

4.7 Develop and maintain procedures for the de-identification of personal data

Notes:
Develop a process to de-identify personal information for processing, restriction, or deletion purposes as in section 14(4) of the POPI Act.

Steps to follow:
- Identify personal information that may need to be de-identified or restricted either:
    - For the purposes identified in section 14 of the POPI Act; and/or
    - Where personal information is no longer required for the initial purpose it was collected e.g. the client has moved to another provider and no longer engages in a relationship with the business.
- De-identify or restrict the personal information as defined by the POPI Act.

4.8 Review processing conducted wholly or partially by automated means

Notes:
If applicable to the business, identify which personal information is subject to automated processing and decision making and review the related processing to ensure compliance with section 71 of the POPI Act. The most pertinent requirements of the POPI Act regarding automated processing, however, relate to automated decision making, as highlighted by sections 5(g) and 71 of the POPI Act.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

Steps to follow:

- Identify which personal information is subject to automated processing and decision making.
- Where automated processing occurs, normally through the use of software systems, it is important to ensure the lawfulness of the automated processing and the security of the automated systems.
- Review the related automated decision-making processing to ensure compliance with section 71 of the POPI Act.

4.9 Review secondary uses or further processing of personal data

Notes:

Identify which personal information is subject to further processing and ensure that such further processing is lawful. Section 15 of the POPI Act describes the details of lawful further processing.

Steps to follow:

- Identify which personal information is subject to automated processing and decision making.
- Where further processing occurs, ensure compliance with section 15 of the POPI Act.

4.10 Develop and maintain procedures for notification to data subjects and/or the Regulator when collecting or processing personal information and obtaining valid consent

Notes:

Consent and notification are addressed in several sections of the POPI Act. Develop prescribed notification procedures for collecting or processing personal information and obtaining valid consent.

Steps to follow:

- Read and obtain the necessary information as set out in the POPI Act in sections 11–15, 18, 26–35, 57–58, 69, 70, 72, 99, and 106, and also in section 6 of the Regulations issued by the Regulator – Government Gazette 14 December 2018 to prescribed templates and procedures in this regard.
- Identify and record when notification to data subjects and the Regulator may be required.
- Confirm and implement the notification procedures as and when required.

4.11 Develop and maintain procedures for legal and secure retention, storage, and destruction of personal data

Notes:

Develop, implement, and maintain procedures for legal and secure retention, storage, and destruction of personal data. Sections 14 and 19 to 21 of the POPI Act describes the details and requirements.

Steps to follow:

- Develop and maintain procedures for legal and secure retention, storage, and destruction of personal data as required by the POPI Act.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

4.12 Integrate data privacy into business continuity plans

Notes:
Update and ensure that the Business Continuity Plan takes Data Privacy Management and related risks into account.

Steps to follow:
- Identify which business continuity elements are impacted by the processing of personal information and specifically potential breaches and the related risks and implications.
- Review existing and consider new business continuity planning and the potential risks and impacts.
- Update and maintain the Business Continuity Plan.

4.13 Integrate data privacy into health and safety practices

Notes:
Update and ensure that the Health and Safety practices take Data Privacy Management and related risks into account and form part of the Business Continuity Plan.

Steps to follow:
- Identify which health and safety elements or processes are impacted by the processing of personal information including the related risks and implications.
- Review existing and consider new health and planning and the potential risks and impacts.
- Update and maintain the Business Continuity Plan.

4.14 Integrate data privacy into direct marketing practices

Notes:
Consider the lawfulness of direct marketing practices. Some companies might incorporate these elements into standard permissions and disclosure-type documentation. This documentation might make provision for a wide range of consent which is often not always relevant to the required solution for the client. The business should consider the lawfulness of gathering information.

Steps to follow:
- Consider current and future marketing practices relating to unsolicited electronic marketing communications and ensure compliance with the requirements of section 69 of the POPI Act.
- Proactively inform clients that they have the right to object to direct marketing other than direct marketing by means of unsolicited electronic communications, as per sections 5(f) and 11(3)(b) of the POPI Act.

4.15 Integrate data privacy into the organisation's use of social media

Notes:
Consider effective and responsible Data Privacy Management when using social media. The primary and most obvious impact of the POPI Act on the business' regarding social media

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

activities is that any information collected via social media channels will be governed by the POPI Act similar to all other client information. The business should ensure at all times that its actions are not endangering the private information of its clients.

An example of a potential breach could be asking the client to directly message personal information to the business on Twitter or WhatsApp. The business runs the risk that when the client replies publicly, their personal information might be exposed.

Steps to follow:

- Consider social media policies and procedures in relation to the 8 Conditions of the POPI Act and lawful processing requirements.
- Update social media policies and procedures as or if required.
- Evaluate the business social data-capturing techniques and ensure the capture, storage, and use of the data complies with the overall business Data Privacy Management.
- Ensure there is a process to deal with the Regulator, and that complaints and security breaches are included in the social media policies and procedures.

4.16 Integrate data privacy into practices for hiring, managing, and monitoring employees or contractors

Notes:

Develop procedures to integrate data privacy into hiring, managing, and monitoring employees or contractors. It is important to establish measures and standards for the protection and lawful processing of personal information within the business. This will ensure the safeguarding of personal information of all employees and/or contractors. Only relevant and necessarily required personal information may be collected and processed.

Steps to follow:

- Use the Personal Data Inventory Template (Reference Tool 6) and Information Flow and Risk Mitigation Assessment Template (Reference Tool 7) to consider and record the lawful collection and processing of personal information as part of procurement and employee or contractor management.
- Address Special Personal Information (as per sections 26–33 of the POPI Act) of employees is in this regard.

4.17 Integrate data privacy into the use of CCTV or video surveillance (if applicable)

Notes:

CCTV or video surveillance is often used in business, including in lobbies, meeting rooms, and where employees or management process personal information.

Steps to follow:

- Ensure that if personal information is recorded or captured as such, it is secured.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

4.18 Integrate data privacy into the use of geo-location (tracking and/or location) devices (if applicable)

Notes:
Geo-targeting involves collecting users' location data, demographics, and interests, and then delivering advertisements based on that location data. Consider whether the business uses such methods and advise clients thereof.

Steps to follow:
- Consider if, when, and how geolocation data is collected or received (generally regarding clients) and if the collection and processing are lawful in terms of the POPI Act.

4.19 Integrate Privacy by Design into new procedures, system, and product development

Notes:
Privacy by Design includes proactively embedding data privacy and POPI Act compliance into the design and operation of new procedures, systems, and products. The Data Privacy Risk Impact Assessment Considerations Guideline Reference Document (Reference Tool 8) includes reference to Data Privacy Impact Assessments (DPIAs) as part of considering data privacy risks for new procedures, systems, and product development.

Steps to follow:
- Integrate Privacy by Design into new procedures, systems, and product development.

5. Manage Information Security Risk

5.1 Integrate data privacy into information security policies and procedures

Notes:
Data storage, archiving and loss, together with email security should be high on the agenda of the business. While the POPI Act places obligations on all businesses that process personal information, the implications for businesses can become quite onerous, depending on the industry and the nature of the information the business handle about their clients. Even small businesses are going to have to consider IT security more seriously in order to ensure compliance with the POPI Act.

Ensure that data security is integrated into the information security policies and procedures and are well defined to regulate the acceptable use of information by everybody in the business. Consider obtaining inputs or advice from an Information Technology and Security Specialist in this regard.

Steps to follow:
- Review information security policies and procedures to ensure that data privacy and the requirements of the POPI Act, sections 19–21 are adequately addressed.
- Update information security policies and procedures as or if required.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

5.2 Develop and maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)

Notes:
Technical measures must be developed and maintained to help protect personal information. This includes email security and security on laptops, firewalls, servers, and mobile devices, to control access to information and prevent data loss. Employees should also be given training to instil information security awareness across the business. Masthead does have an online Cybersecurity Online Course available at https://portal.masthead.co.za/ to assist with this training.

Steps to follow:
- Review information security technical measures to ensure that data privacy and the requirements of sections 19–21 of the POPI Act are adequately addressed.
- Update information security technical measures as or if required.
- Ensure the training and recordkeeping of such of all employees.

5.3 Develop and maintain measures to encrypt personal data

Notes:
Encryption is the method by which information is converted into a secret code that hides the information's true meaning. Although platforms such as WhatsApp claims end-to-end encryption of messages, it is not advisable to process personal information on such 'public' application platforms. Consider obtaining inputs from an Information Technology Specialist in this regard.

Steps to follow:
- Consider how personal information is processed electronically and if or how encryption may be required.
- Consider encrypting all business and employee-owned devices as a standard technology and security measure.

5.4 Develop and maintain a data-loss prevention strategy

Notes:
The implementation of a data-loss prevention strategy is crucial in today's business environment. Data-loss prevention can include layers of protection against data theft for example to ensure employees do not send sensitive or critical information outside the business. Against the backdrop of the ever-increasing need to keep personal information secure, data-loss prevention should also be seen as central to a strategy to ensure that, in the event of a disaster, lost data can be expeditiously recovered and restored. Again, consider obtaining inputs from an Information Technology Specialist in this regard.

Steps to follow:
- Consider how personal information is processed electronically and secured.
- Develop (document) and review the business' strategic approach and mechanisms to prevent data loss, including information security considerations, back-ups, etc.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

5.5 Conduct testing of data security

Notes:
Test back-up data and information security efficiency.

Steps to follow:
- Obtain inputs from an Information Technology and Security Specialist in this regard and test and enhance (if required) data security measures.

5.6 Use ISO27001, 27002, and 27701 as guidelines and references for effective data security management

Notes:
1. ISO 27001 is an international standard on how to manage information security.
2. ISO 27002 gives guidelines for organisational information security standards and information security management practices.
3. ISO 27701 is an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management, specifically.

Steps to follow:
- Procure and read the ISO guidelines (certification is normally only done by large organisations).
- Consider the guidelines when implementing this activity.

6. Manage Operator and Third-Party Risk

6.1 Review agreements with all operators and third parties, specifically

Notes:
- Use the Managing Third-Party Risks and Third-Party Operator Engagement Strategy Guideline Reference Document (Reference Tool 9) as a guideline. If needed, engage the assistance of an attorney to review all Operator and Third-Party Agreements.

Steps to follow:
- Review and amend all Operator and Third-Party Agreements as or if required.

6.2 Conduct due diligence around the data privacy and security compliance of operators and third parties

Notes:
It is advisable that the business as a responsible party should not only address the section 21 requirement in the POPI Act in an agreement with an operator or third party, but conduct due diligence to ascertain that contracted operators or third parties are compliant with the Act and have adequate data security and protection measures in place. Such due diligence could be done in any one or more of the following ways:
- Ensure that all types of personal information that is shared with existing operators or third parties are identified and recorded and confirm this with the operators or third parties in writing;

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

- Confirm and consider the mechanisms through which personal information is shared with and processed by operators or third parties;
- Communicate requirements regarding sections 21 of the POPI Act with operators or third parties;
- 'Vet' existing and new operators or third parties by getting a written response to the following typical questions, e.g.:
    - What information and data protection mechanisms do the business have in place?
    - Has the business' data protection or POPI Act compliance been independently professionally assessed and, if yes, can the business share the details or outcomes of such an assessment?
    - Did the business have any information security breaches or incidents pertaining to non-compliance to the requirements of the POPI Act?
    - Consider sharing the POPI Act Privacy Policy Statement of the business.
- Identify potential high-risk operators or third parties and reconsider their agreements.
- Ensure that sections 20 and 21 of the POPI Act requirements are included in the contract with the operators or third parties and that the contract can be immediately terminated, and damages suffered claimed, should a breach occur.

Steps to follow:

- Use the Managing Third-Party Risks and Third-Party Operator Engagement Strategy Guideline Reference Document (Reference Tool 9) as a guideline.
- Conduct and maintain due diligence.

7. Respond to Requests and Complaints

7.1 Develop and confirm procedures to respond to requests for access and correction to personal information

Notes:

Develop a procedure and policy on how to respond to a request for access to a client's personal information using the Procedure for Handling Requests for Personal Information Guideline Reference Document (Reference Tool 10) as a guideline. What is important here is when access and corrections are requested, to remember that the business must have a procedure in place to identify the client and that they have the right to request the information held.

If a request for a correction or deletion is received, the business as the responsible party must correct and/or delete the information as soon as possible as per the request and provide the client with credible evidence to their satisfaction that it was done.

Steps to follow:

- Use the Procedure for Handling Requests for Personal Information Guideline Reference Document (Reference Tool 10) and develop such a procedure with the necessary templates.
- Refer to section 2 of the Regulations issued by the Regulator – Government Gazette 14 December 2018 and the prescribed templates.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

7.2 Develop and maintain procedures to respond to requests to opt out of, restrict or object to processing

Notes:
Previous legislation and regulations before the arrival of the POPI Act in 2013 required businesses in South Africa to provide the opportunity for recipients of any marketing campaigns to unsubscribe from further communications (commonly referred to as 'opt out').

Section 11 of the Consumer Protection Act (CPA, Act 68 of 2008, Part B section 11) provides that an individual may refuse to accept, request the discontinuation of (opt out) or pre-emptively block direct marketing communications, and that any opt-out or pre-emptive block must be respected by the business (marketers), have their request confirmed in writing and that the exercise of these rights must be performed free of charge.

Section 11 of the POPI Act makes it clear that the business as the responsible party must keep adequate records to prove informed consent has been voluntarily given. Records should also be maintained where consent has been denied or is later withdrawn.

Steps to follow:
- Use the Procedure for Handling Requests for Personal Information Guideline Reference Document (Reference Tool 10) and develop such a procedure with the necessary templates.
- Refer to section 2 of the Regulations issued by the Regulator – Government Gazette 14 December 2018 and the prescribed templates.

7.3 Develop and maintain procedures to address complaints

Notes:
Develop a procedure on how to address complaints by using the Procedure for Handling Requests for Personal Information Guideline Reference Document (Reference Tool 10).

Steps to follow:
- Develop the procedure with the necessary prescribed templates as per sections 7–12 of the Regulations issued by the Regulator – Government Gazette 14 December 2018 to respond to complaints.
- Use the business' current Complaints Register, to record these complaints and the actions taken.
- Ensure that this procedure and register is maintained.

7.4 Develop frequently asked questions to respond to queries

Notes:
Develop a bank of frequently asked questions to respond to queries by developing standard answers for each one. Use the Bank of Frequently Asked Questions Reference Document (Reference Tool 12) as a guideline.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

Steps to follow:

- Continue to build on these questions on an ongoing basis.
- Develop standard answers to each type of question.

8. Breach Management

8.1 Develop a data privacy incident or breach response plan

Notes:

Handling data breaches can be extremely time and resource (including cost) intensive. Breaches also have a severe impact on business reputation and trust. Two examples of how the Information Regulator considers data breaches can be accessed in the links below:

- https://www.justice.gov.za/inforeg/docs/ms-20180622-LibertyHoldingsDataBreach.pdf
- https://www.justice.gov.za/inforeg/docs/ms-20200903-ExperianUpdate.pdf

Use the Breach Management Considerations Guideline Reference Document (Reference Tool 11) as a guideline to develop a data privacy incident or breach response plan with additional information security controls. Developing additional information security controls would be a natural result of a privacy assessment. But more importantly, it would be the timeous detection, containment, analysis, and remediation after a breach that would differentiate the business from the next.

Steps to follow:

- Develop a plan to implement more information security controls.
- Develop a plan that includes the business' response to an incident or breach.
- Implement mitigation plans on any incidents or breaches and maintain this plan.

8.2 Develop a breach notification and reporting or communication (to data subjects, the Regulator, and other relevant stakeholders) protocol

Notes:

In the event of a security compromise, the business must notify the Information Regulator as well as any parties whose personal information has been accessed or acquired by an unauthorised party. If the business takes into account the reputational and financial harm associated with a data breach, not to mention the disruption it can cause to a business' operations, the business should ensure that they have an adequate data-breach response plan in place.

Use the Breach Management Considerations Guideline Reference Document (Reference Tool 11) as a guideline to develop a communication plan to data subjects (clients), other stakeholders, and the Regulator.

Steps to follow:

Should a breach occur:

- Notify the data subject (client) and Regulator in writing as soon as possible.
- Urgently obtain legal advice, if appropriate before the above notification, take notice of section 22(2) of the POPI Act.

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

- Do not communicate to or on (the) media or to other parties until advice is obtained on how best to communicate regarding the incident taking cognisance of legal advice obtained.
- Be open and transparent and provide any support and cooperation possible to the data subject and as may be required by the Regulator.
- Do as much as possible to immediately secure or further secure the personal information and to track where the personal information could be leaked and take any possible further mitigation measures to prevent or limit further leakages or breaches.

8.3 Develop and maintain a log to track data privacy incidents or breaches

Notes:
A mechanism, in any form useful and efficient to the business, to log and track data breaches, should be developed and maintained. Use the Breach Management Considerations Guideline Reference Document (Reference Tool 11) as a guideline to develop a register to record incidents or breaches. Valuable risk reduction information can be gained from such a register.

Steps to follow:
- Develop a register using the Breach Management Considerations Guideline Reference Document (Reference Tool 11) to ensure compliance with all the details that must be contained in this register around incidents or breaches.

8.4 Investigate data privacy breach insurance coverage

Notes:
Although insurance against information security breaches (such as hacking) is quite common and personal indemnity insurance is a requirement for various business e.g. attorneys and Financial Services Providers, financial cover against normal business-process breaches (e.g. when a breach happens due to negligence of a staff member), should be investigated.

Steps to follow:
- Contact a Financial Services Provider who specialises in professional indemnity insurance to investigate adequate cover for breach of data privacy for the business.

9. Ongoing Maintenance and Review

9.1 Keep updated with ongoing privacy management compliance requirements e.g. law, case law, industry codes of conduct, seminars

Notes:
Ensure that new requirements and developments are identified and incorporated early.

Steps to follow:
- Study the POPI Act and Regulations and continuously stay abreast of new developments and regulatory guidelines, templates, and requirements.
- Stay updated with changes on the Information Regulator's website: https://www.justice.gov.za/inforeg/

Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.

9.2 Seek specialist and legal advice regarding specific uncertainties or new requirements

Notes:
Obtain legal advice as and when required.

Steps to follow:
- Seek specialist and legal advice regarding specific uncertainties or new requirements.

9.3 Consider external assessments to confirm compliance

Notes:
Do an independent review and obtain recommendations regarding compliance (as a risk-reduction consideration) and gain client and business stakeholder trust. There are currently no formal or POPI Act or Regulatory requirements to be audited on POPI Act compliance. An independent assessment is, however, highly recommended and can be seen as a proactive reasonable risk-reduction measure.

Steps to follow:
- Consider procuring Masthead to review your POPI Act compliance.

Masthead DIY POPI Act Compliance Toolkit© 2020 Masthead (Pty) Ltd
Disclaimer: While every reasonable effort has been taken to ensure the accuracy and soundness of the content of this material, Masthead does not accept any responsibility for the consequences of any actions based on any information contained herein. The content of this material does not constitute advice.