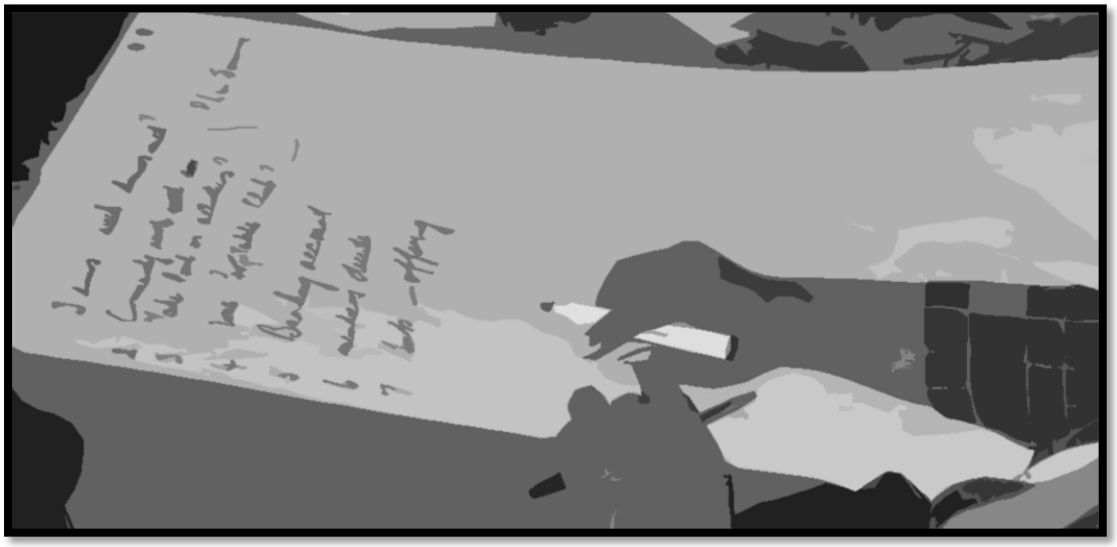
GUIDELINES FOR ATTORNEYS ON THE PROTECTION OF PERSONAL INFORMATION ACT

LAW SOCIETY
OF SOUTH AFRICA



LAW SOCIETY
OF SOUTH AFRICA

Contents

DISCLAIMER and IMPORTANT NOTICE:

This guide and checklist is a basic guide to POPIA AND IS NOT DEFINITIVE. Practitioners are required to apply their mind to the practice, the clients, the nature of legal services and the transaction conducted. This will be unique to each practice.

The information contained in this document is general in nature and should not be interpreted or relied upon as legal advice. The information may not be applicable to specific circumstances. Professional assistance should be obtained before acting on any of the information provided in this document.

The LSSA guide on POPIA which was updated in 2018 has not been removed from the resources on the website as it contains essential information on more complex practices and considerations and is recommended that practitioners consult this resource when in doubt

Prepared by:
Law Society of South Africa
Website: www.LSSA.org.za

Chapter 1: Introduction to POPIA

a. The Constitutional Origin of POPI

The constitutional Right to Privacy
Section 2 of the **Protection of Personal Information Act**, 2013 (POPIA) sets out its purposes. The first purpose of POPIA is to:

Give effect to the **constitutional right to privacy** by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at:

a) Balancing the right to privacy against other rights, particularly the right of access to information, and
b) Protecting important interest, including the free flow of information within South Africa and across international borders.

The constitutional right to privacy is contained in section 14 of the Constitution:

> **Section 14 of the Constitution**
>
> Everyone has the right to privacy, which includes the right not to have:
> a) their person or home searched;
> b) their property searched;
> c) their possessions seized; or
> d) the privacy of their communications infringed.

POPIA gives content to the right to privacy as captured in the Constitution. It is not an absolute right and can be limited pursuant to the Limitations Clause in the Constitution. POPIA is an attempt to balance the right to privacy with the rights of others, including the right to access information.

POPIA's preamble recognises that:

a) Section 14 of the Constitution provides that everyone has the right to privacy,

b) The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information, and

c) The state must respect, protect, promote and fulfil the rights in the Bill of Rights.

Section 7 (2) of the Constitution

The state must respect, protect, promote and fulfil the rights in the Bill of Rights.

The enactment of POPIA is, in essence, the state's way of protecting, promoting and fulfilling the right to privacy as captured in the Bill of Rights.

The Limitations Clause

The right to privacy is not an absolute right. Constitutional rights may be limited, consistent with the Constitution.

Section 7 (3) of the Constitution

The rights in the Bill of Rights are subject to the limitations contained or referred to in section 36, or elsewhere in the Bill.

POPIA also recognises that the removal of unnecessary impediments to the free flow of information, including personal information, is required within the context of:

- Constitutional values of democracy and openness, and
- The need for economic and social progress.

Section 36 of the Constitution (the Limitations Clause) captures the manner in which constitutional rights may be limited. All limitations of the right to privacy must be consistent with the Limitations Clause.

Section 36 of the Constitution – The Limitations Clause:

(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including-
   a. the nature of the right;
   b. the importance of the purpose of the limitation;
   c. the nature and extent of the limitation;
   d. the relation between the limitation and its purpose; and
   e. less restrictive means to achieve the purpose.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.

b. The Right to Privacy as interpreted by the Courts

The right to privacy has also been recognised by the South African courts before the Constitution was in existence. A person's 'dignitas' has been interpreted to include personality and reputation, which was widely interpreted as including the right to privacy.

A Personality Right
The Constitutional Court in **Bernstein vs Bester NO**[1] confirmed that the common law recognised the right to privacy as a personality right included under someone's *dignitas*. The Court confirmed the following important aspects:

a) A right to privacy is recognised as an independent personality right which is included within the concept of dignitas.

b) Every right is already limited by every other constitutional right.

c) It is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community.

d) As a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrink accordingly.

c. The Purpose of POPIA

As stated above, the first purpose of POPIA is to give effect to the constitutional right to privacy. In doing so, it must be also deal with the limitations inherent with this right. The further purposes captured in POPIA are to:

a. Regulate the manner in which personal information may be processed;

b. Provide persons with rights and remedies to protect their personal information from processing that is not consistent with POPIA; and

c. Establish measures, including an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by POPIA.

d. The Application of POPIA

POPIA applies to the **processing** of **personal information** entered into a **record** by or for a responsible party.

The scope of this sentence can only be understood once we look at the definitions of the following key terms.

[1] *Bernstein and Others v Bester NO and Others 1996 (4) BCLR 449*

Processing:

Processing is defined as any operation or activity or any 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.

Examples of **processing** would include; doing a video recording of a person, storing personal information in the firm's records and collecting the name, address and phone number of someone at an event.

Personal Information:

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

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 medical, financial, criminal or employment history of the person;

c) any identifying number, symbol, e-mail 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.

Examples of **personal information** would include someone's home, postal and email addresses, fingerprints, views expressed in an evaluation form at a workshop and their information captured in a curriculum vitae.

Record:

Means any recorded information:

(a) Regardless of form or medium, including any of the following:

i. Writing on any material,
ii. Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
iii. Label, marking, or other writing that identifies or describes any thing or which it forms part, or to which it is attached by any means;
iv. Book, map, plan, graph or drawing;
v. Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(b) In the possession or under the control of a responsible party;

(c) Whether or not it was created by the responsible party; and

(d) Regardless of when it came into existence.

Examples of **personal information** would include taking pictures of someone, writing down and storing their details, scribbling down a person's identity number on a piece of paper.

The responsible party must in essence be domiciled in South Africa or, if not domiciled in South Africa, making use of a means of recording in South Africa – unless those means are only used to forward personal information through South Africa.

KEY ISSUES TO REMEMBER:

- ✓ POPIA gives effect to the constitutional right to privacy.
- ✓ The right to privacy is recognised as an independent personality right.
- ✓ POPIA applies to the processing of personal information entered into a record by or for a responsible party.
- ✓ POPIA is aimed at safeguarding personal information when processed.
- ✓ The right to privacy is subject to justifiable limitations.
- ✓ POPIA captures rights and remedies to protect personal information.

Chapter 2: ATTORNEYS AND POPIA

POPIA is relevant to attorneys as personal information is ordinarily processed by them as part of their service-offering. POPIA imposes a number of obligations on attorneys when processing personal information.

a. POPIA's application to Attorneys

POPIA is a law of general application that applies to the processing of personal information and defines a person as a natural or juristic person.

Personal Information:

Means information relating to an **identifiable, living, natural person**, and where it is applicable to, an **identifiable, existing juristic person**, including but not limited to - ….

Attorneys would ordinarily process and possess personal information.

b. Examples of attorneys processing Personal Information

Attorneys may process different personal information of data subjects for different purposes. Below are some situations which would ordinarily qualify as the processing of personal information:

PURPOSE	DATA SUBJECT*
Employment Contracts	Employees
Service Provision	Consultants, Service-Providers, Experts
Trading Activities and marketing	Clients and Customers
Recruitment	Job applicants
Information Dissemination	Subscribers and website participants
Customer Relations	Complainants
Emergency Contacts	Relatives of certain data subjects
Legal Services	Clients
FICA Client Verification	Clients and Potential Clients

*A **data subject** is the person to whom the personal information relates.

c. Verification of Clients according to Financial Intelligence Centre Act

According to the Financial Intelligence Centre (the FIC), there are essentially three forms of control measures contained in the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act), i.e.[2]:

1) knowing with whom they are doing business;

2) preserving the paper trail of relevant transactions; and

3) reporting possible money laundering transactions to the FIC and the investigating authorities.

Section 42 of the FIC Act provides that each individual attorney, as accountable institution must:

- develop
- document
- maintain
- implement

  Risk Management and Compliance (RMC) Programme for anti-money laundering and counter-terrorist financing.

The RMC Programme must enable the attorney to:

- identify
- assess
- monitor
- mitigate
- manage

In terms of the RMC Programme, attorneys must, before entering into a client relationship, **establish and verify** the identity of prospective clients to engage in a business relationship or conclude a single transaction.

This means that the attorney must collect and process personal information from a potential client.

Even after the client relationship has commenced, the attorney must conduct ongoing due diligence and account monitoring regarding business relationships. This would also include the examination of complex and unusually large transactions.

[2] Guidance Note 05B on Cash Threshold Reporting to the Financial Intelligence Centre in terms of Section 28 of the Financial Intelligence Centre Act, 2001, page

KEY ISSUES TO REMEMBER:

- ✓ Attorneys ordinarily process personal information.
- ✓ Attorneys must, before entering into a client relationship, establish and verify the identity of prospective clients to engage in a business relationship or to conclude a single transaction

Chapter 3: Conditions for Lawful Processing

a. Setting the tone for POPIA compliance

POPIA introduces additional legal responsibilities for managing and processing personal information under its control. Compliance with POPIA will:

1. Help the attorney to protect the personal information within his or her possession;
2. Increase stakeholder confidence and relations;
3. Minimise exposure to unnecessary risks; and
4. Help to protect the attorney's reputation.

Non-compliance with POPIA, on the other hand, may lead to:

1. Exposure to unnecessary financial and reputational risks;
2. Adverse media publicity;
3. Negative public perceptions;
4. Fines issued by the Information Regulator; and
5. Civil action by the data subject.

How the attorney manages the personal information of people is vitally important for all involved.

b. The Rights of Data Subjects

The rights of data subjects are defined in POPIA. As indicated earlier, a **data subject** is the person to whom personal information relates.

Section 5 of POPIA captures the following rights, amongst others, of data subjects:

1. To be notified of the collection of their personal information,
2. To be notified that their personal information has been accessed or acquired by an unauthorised person,
3. To establish if the attorney holds personal information about them,
4. To request access to their personal information,
5. To request the correction, destruction or deletion of their personal information,
6. To object, on reasonable grounds, to the processing of their personal information,
7. To object against the processing of their personal information for purposes of direct marketing (including solicitation of funding) through unsolicited electronic communication, and
8. To institute civil proceeding regarding the alleged interference with the protection of their personal information.

c. The conditions for lawful processing of personal information

As indicated in Chapter 2, processing includes the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use of personal information and dissemination thereof by means of transmission, distribution or making available in any other form.

The processing of information must be done in accordance with the provisions of POPIA to be considered lawful. Section 4 of POPIA lists the **eight conditions** for lawful processing of personal information, which are:

1. Accountability
2. Process limitation
3. Purpose specification
4. Further processing limitation
5. Information Quality
6. Openness
7. Security Safeguards
8. Data subject participation

In some instances, the processing of personal information may be **excluded** from the application of POPIA. In other instances, POPIA may **exempt** the processing of personal information from one or more of the above conditions.

d. CONDITION 1: Accountability

Section 8 of POPIA requires that the responsible party ensure compliance with above eight conditions. This includes all measures that give effect to such conditions. Compliance must happen:

- When determining the purpose and means of processing
- During processing.

Who is the responsible party?
POPIA defines a responsible party as a public or private body or any other person who, alone or with others, determines the purpose of and means for processing personal information. The private body will be the attorney in the context of this Guide.

There are two important aspects of this responsibility:

- The eight conditions set out in Chapter 3 of POPIA; and
- The measures that give effect to those eight conditions.

What are the key steps that the attorney should take?

The attorney should:

- Accept responsibility to comply with the responsibilities under POPIA;
- Approve suitable policies and systems for the management and processing of personal information;
- Ensure that policies and systems are understood, embraced and complied with;
- Ensure that staff members are properly equipped and trained to comply with POPIA;
- Ensure that contracts with employees third parties capture relevant POPIA responsibilities; and
- Regularly monitor and review the effectiveness of policies and systems.

e. CONDITION 2: Processing Limitation

Section 9 requires attorneys to process personal information **lawfully** and in a reasonable manner that does not infringe the data subject's privacy.

In essence, there must be a legal basis for the processing of personal information of any data subject. The clearest way perhaps is to establish such a lawful basis, is through the consent of the data subject.

The **PURPOSE FOR PROCESSING** personal information must be:

- Adequate
- Relevant
- Not Excessive

When is the processing of personal information lawful?
Personal information may only be processed (including, collected, received, recorded, organised, collated, stored, updated, altered, disseminated) if:

a. The data subject consents to it;

b. A competent person (parent or guardian) where the data subject is a child, consents to it;

c. It is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;

d. It complies with an obligation imposed by law on the responsible party;

e. It protects a legitimate interest of the data subject; or

f. It is necessary for pursuing the legitimate interests of the responsible party (attorney, within this context) or of a third party to whom the information is supplied.

Can a data subject withdraw consent to and object to processing?
Yes, a data subject (or a parent or guardian of a child) may at any time withdraw his or her consent in situations where consent was given.

Processing that is not based upon consent remains lawful if based upon one of the other grounds listed above.

A data subject may, unless the law allows for such processing, object on **reasonable grounds** to the processing of personal information by an attorney in situations where the processing:

a. Protects a legitimate interest of the data subject, or

b. Is it necessary to pursue the legitimate interests of the attorney or a third party to whom the information is supplied.

This objection must be done in the prescribed manner.

A data subject may also object to the processing of personal information for purposes of direct marketing (including solicitation of funding).

Withdrawal of consent and objection against the processing
POPIA requires the attorney to stop processing the personal information of a data subject that has objected thereto. POPIA does not specifically explain what will happen in the event that there is a dispute between the parties as to the grounds on which the objection is based.

f. CONDITION 3: Purpose Specification

POPIA requires that **PURPOSE FOR COLLECTING** personal information must be:

- Specific
- Explicitly Defined
- For a Lawful Purpose related to the function or activity of the attorney

Attorneys must not keep personal information for longer than necessary for achieving the purpose for which it was collected or processed unless:

a) The law requires such a retention period,

b) The attorney requires such a record for lawful purposes,

c) Retention is based upon a contract between the parties,

d) The data subject has consented to such retention, or

e) A competent person on behalf of a minor has consented to such retention.

Personal information may be retained for historical, statistical or research purposes for longer periods provided that the attorney establishes appropriate safeguards for the records being used for other purposes.

Attorneys must destroy, delete, or de-identify personal information once they are no longer authorised to retain such records.

De-identifying:

De-identifying means to delete information that—
a) Identifies the data subject;
b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject.

The attorney must restrict the processing of personal information in situations where amongst other:

- It no longer needs the information for its original purpose, except for purposes of proof,
- The accuracy of the personal information is contested, or
- The processing thereof is unlawful, but the data subject opposes its destruction and requests the restriction of its use.

g. CONDITION 4: Further Processing Limitation

What is further processing?
POPIA requires that further processing of personal information must be consistent with the purpose for which it has been collected, being:

- Specific
- Explicitly Defined
- For a Lawful Purpose related to the function or activity of the attorney

In essence, the attorney should not collect personal information for one purpose and then process it for another. To assess the compatibility between the purpose for collection and the purpose for processing, the following factors must be taken into account:

a) The relationship between the purpose for the collection and the purpose for further processing;

b) The nature of the information concerned;

c) The consequences for the data subject of the further processing;

d) The manner in which the personal information has been collected; and

e) Contractual rights and obligations between the parties.

Further processing of personal information is permissible in certain instances, including, where:

- The data subject has provided consent;
- The personal information is available on a public record; or
- The data subject has deliberately made public such personal information.

h. CONDITION 5: Information Quality

Attorneys must – having regard to the purposes for collection and processing - take reasonable practicable steps to ensure that the personal information is:

- Complete
- Accurate
- Not misleading
- Updated, where necessary

i. CONDITION 6: Openness

Attorneys must, when collecting personal information, take reasonably practical steps to ensure that data subjects are aware of:

a. The information being collected;

b. The source from which the information is collected;

c. The name and address of the responsible party (the person who determines the purpose of and means for processing personal information);

d. The purpose for the collection of the information;

e. Whether or not the supply of the information is voluntary or mandatory;

f. The consequences of failure to provide the information;

g. Any law authorising or requiring the collection of the information;

h. Intention to transfer the information to a third party or an international organisation and the level of protection afforded to the information in such instances; and

i. Any further information that will enable reasonable processing, including:

- Recipients of the information
- Nature of the information

The data subject has consented to non-compliance	
Non-compliance is necessary to comply with a legal obligation	
Non-compliance is necessary for the conduct of court proceedings	
Non-compliance is necessary in the interests of national security	
Compliance would prejudice a lawful purpose of the collection	
Compliance is not reasonably practicable in the circumstances	
The information will not be used in a way to identify the data subject	
The information will be used for historical, statistical or research purpose	

j. CONDITION 7: Security Safeguards

POPIA requires attorneys to properly safeguard personal information in its possession. Attorneys must secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent:

a. Loss of, damage to or unauthorised destruction of personal information; and

b. Unlawful access to or processing of personal information.

Attorneys must:	**X**
Identify all reasonably foreseeable risks to personal information	
Establish and maintain appropriate safeguards against risks	
Regularly verify that safeguards are effectively implemented	
Ensure that safeguards are continually updated.	

Attorneys must have regard to the accepted security practices and procedures which may apply to it generally or be required in terms of the specific industry or professional rules and regulations.

k. CONDITION 8: Data Subject Participation

A data subject has the right to request the attorney:

a. to confirm whether or not it holds personal information about the data subject;

b. to provide the record or a description of the personal information of him or herself held by the attorney within a reasonable time, at a prescribed fee; and

c. to provide information of all third parties who have or have had access to the information.

Attorneys:	X
Must advise data subject of the right to request the correction	
Where applicable, provide a written estimation of fee for services	
May require the data subject to pay a deposit for the fee	
May refuse disclosure of information pursuant to PAIA	
Must disclose parts of information that cannot be refused ito PAIA	

A data subject may request the attorney to:

a. Correct or delete personal information about the data subject in its possession or under its control. The information must be inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, and

b. Destroy or delete a record of personal information about the data subject that the attorney is no longer authorised to retain.

The attorney must, upon receipt of a request, as soon as reasonably practicable:

a. Correct the personal information,

b. Destroy or delete the information,

c. Provide the data subject with credible evidence in support of its information, or

d. Take reasonable steps to attach to the information an indication that a correction of the information has been requested but not made if the attorney and the data subject are unable to reach agreement on the issue.

The attorney must, after having made changes to the personal information:

- Inform the data subject of those changes, and

- Inform each person to whom the personal information has been disclosed of those changes, if reasonably practicable if such changes have an impact on decisions that have been or will be taken in respect of the data subject.

KEY ISSUES TO REMEMBER:

✓ Section 4 of POPIA lists the following eight conditions for lawful processing:

- Accountability
- Process limitation
- Purpose specification
- Further processing limitation
- Information Quality
- Openness
- Security Safeguards
- Data subject participation

✓ Attorneys must secure the integrity and confidentiality of personal information in their possession.

Chapter 4: POPIA and IT Governance

a. Safeguarding Personal Information

Attorneys are required to properly safeguard personal information in their possession. Processing includes automated and non-automated means. Attorneys should take appropriate measures to prevent:

a) Loss of, damage to or unauthorised destruction of personal information, and

b) Unlawful access to or processing of personal information.

Personal information may get lost, damaged or unlawfully accessed in a variety of ways, including:

a) Theft of documents or electronic records,
b) Computer viruses,
c) Computer crashes,
d) Hacking of databases,
e) Accidental damage caused by employees or contractors, or
f) Natural disasters.

Attorneys should take a comprehensive approach to prevent the loss, damage, and unauthorised personal information access through the above processes. As some personal information usually gets processed electronically, it is important to have an effective IT system in place. This chapter focuses on the key steps in relation to Information Technology (IT) Governance.

b. The Board's role in IT Governance

The King IV Report on Corporate Governance recognises that: 'Information and technology overlap but are also distinct sources of value creation which pose individual risks and opportunities.'[3] As a result, these two concepts are referred to separately by King IV. Principle 12 provides: 'The governing body should govern technology and information in a way that supports the organisation in setting and achieving its strategic objectives.'[4] King IV recommends that the Board should exercise oversight of technology and information management and, among others, proactively monitor intelligence to identify and respond to social media events.

[3] King IV Report, Fundamental Concepts: Technology and information, page 30.
[4] King IV Report, Principle 12, page 62.

The attorney should take the following factors into account when developing the IT Governance framework:

- The available resources
- The nature of personal information collected by the attorney
- The attorney's IT infrastructure
- The exposure to risk
- The nature of legal services being rendered by the attorney

With the above in mind, the IT Governance framework should be easily understood and comply with. The roles and responsibilities of employees should be clearly defined.

c. IT Security

An effective IT security system involves safeguarding the computer hardware and the personal information stored on the hardware.

The following steps are listed in POPIA

Identify all reasonably foreseeable risks to personal information. A risk assessment on personal information would be valuable, and the LSSA proposes that attorneys implement it. The risk assessment should basically cover the following:

- Identify the nature of the personal information in the attorney's possession,

- Identify key risks involved with the collection, storing and processing of personal information, and

- The implications for the data subjects should their personal information get lost, unlawfully accessed or destroyed.

Once the attorney is clear on the risks involved with personal information, he or she should decide on appropriate safeguards. The attorney may have identified a large number of risk factors. Not all of those risks may have the likelihood of materialising. The safeguards will depend on several factors, including:

- The potential impact to the attorney and the data subjects if a risk event occurs;

- Whether the consequences will impact on reputation, people, assets or income;

- The likelihood of the risk factors materialising;

- What it will cost to put appropriate safeguards in place; and

- What will the cost and impact be if the risk materialises without appropriate safeguards.

Once the attorney has considered the above, the practice can decide what safeguards would be appropriate to avoid or minimise those risks. IT safeguards may include:

Appropriate IT safeguards may include:	**X**
Anti-virus Software and Firewall Protection which are regularly updated - **Protocols to regularly update and review the effectiveness of software** - **Files are quarantined** -	X
Password Protection - **Passwords are regularly changed** - **Re-use of passwords are prohibited** - **Passwords are complex enough** - **Passwords are not shared** - **Passwords are stored securely** - **Passwords are changed when employees leave the practice.**	X
Access Control Protocols - **Clear protocols determining who can access which information** - **Accounts locked on multiple failed login attempts** - **Administrator required to unlock accounts** - **Policies and control to download or transfer personal information** - **Identification of unlawful access to personal information** - **Record and review account logs** - **Mobile devices, laptops, phones etc. should have anti-virus software that is updated and secure when linked to the network and are monitored** - **Thumb drives and removable disks etc. must have appropriate protection, similar to mobile devices** - **Only vetted mobile devices and removable drives, disks etc. are allowed to connect to the network**	X
Ongoing Training of Employees - **Regular training on the content of POPIA and related-policies** - **Employees appreciate the importance of protecting personal information** - **Employees trained to ensure IT safeguards are implemented**	X
Adopt Suitable Policies	X
Safekeeping of hardware	X
Conduct Regular Security Audits and ensure business continuity plans and disaster recovery process are in place and effectively tested.	X
Backups - **Backups regularly made of personal information** - **Backups stored offsite to protect against onsite damage or theft** - **Backups regularly monitored to ensure lawful personal information stored** - **Backups protected against unlawful access or use**	X

Include IT safeguards in Job Descriptions and Service-Contracts - **Employees know to implement IT safeguards** - **Included in Job Descriptions of employees** - **Consultants required to implement appropriate IT safeguards** -	X

d. Cloud Computing

Cloud computing has become increasingly popular in recent years. Cloud computing takes various forms and will ,inevitably result in the processing of personal information of data subjects.

It will be important for the attorney to assess to what extent personal information is being processed by means of cloud computing. Should cloud computing involve processing personal information, the attorney must ensure that cloud computing service provider is POPIA compliant.
Cloud computing ensures back-up and disaster recovery are effective and latest updates of software is in plaace. Beware online services are not the same as cloud computing. The LSSA has an IT guide on its website resources section provides more information in this regard.

The attorney would usually appoint a service-provider to process information through cloud computing. This cloud service-provider would, in our view, fall within the definition of '**operator**' under POPIA.

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.

Section 20 of POPIA provides that an operator or anyone processing personal information on behalf of a responsible party or an operator must:

a. Process such information only with the knowledge or authorisation of the responsible party, and

b. Treat personal information which comes to their knowledge as confidential and must not disclose it.

The above duties are imposed upon the operator (cloud service-provider). The attorney, as the responsible party, must provide the authorisation for such processing.

Another clause that may potentially impact cloud computing service-providers, is found in Chapter Nine of POPIA, which is entitled *Transborder Information Flows*. Chapter Nine only has one section, being section 72.

Section 72 provides that a responsible party may not transfer personal information about a data subject to a third party (cloud service-provider) who is in a foreign country unless:

a. The cloud service-provider is subject to a **law**, **binding corporate rules** or **a binding agreement** which:

   - provide adequate and similar protection of personal information as captured in POPIA, and

   - include similar provisions as contained in section 72 of POPIA should the personal information be transferred to a third party in a foreign country.

b. The data subject has consented to such transfer;

c. The transfer pursuant to a contract between the data subject and the responsible party;

d. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject; or

e. The transfer is beneficial to the data subject, and he or she would have likely given consent or it is not reasonably possible to obtain such consent from the data subject.

The above requirements are generally found in standard contract conditions [SCC] in the agreement with the service provider agreement or SLA.

KEY ISSUES TO REMEMBER:

- ✓ An effective IT security system involves safeguarding the computer hardware and the personal information stored on the hardware.
- ✓ Cloud computing takes various forms and will in most cases, inevitably result in the processing of personal information of data subjects.
- ✓ Attorneys can only transfer personal information about a data subject to a third party (cloud service-provider) who is in a foreign country subject to the specific conditions listed in section 72 of POPIA.

ANNEXURE A: POPIA CHECKLIST

A. APPOINT AN INFORMATION OFFICER

1. It is advisable for small firms to appoint the same Information Officer for both PAIA and POPIA.
2. Appoint the same Deputy Information Officer for both PAIA and POPIA.
3. Formally agree the Information Officer and Deputy Information Officer's roles and responsibilities, including reporting structures and mandatory reporting regularly [maximum timeframe should be monthly, larger firms report weekly]
4. Complete the formal appointment process by issuing a letter of appointment with role and responsibility.

B. PROCESS

1. The process followed should be a similar process followed by a basic Risk Management process.
2. Risk and Opportunities must be considered, and cost-effectiveness should be the guide.
3. Various scenarios with multiple mitigation actions must be developed
4. Mitigation in this instance will be the action that ensures compliance to key risks identified.

C. GAP ANALYSIS

1. Ensure key internal stakeholders are part of this process or a cross-section of staff from different sections
2. Assess and review existing process and risks against POPIA
3. In consultation with stakeholders, targets should set. [NB: regularly review targets at least quarterly and build this into the Policy]
4. Set interim and final targets for compliance with the POPI Act.

5. Use an evidence-based approach[5]
6. Regular Assessment and reviews to be completed at least quarterly and reported published as part of compliance monitoring

D. ANALYSIS OF THE PROCESSING AND STORAGE OF PERSONAL INFORMATION

1. This section is the critical part of the Policy.
2. Utilise the POPIA definitions and record types.
3. POPIA requires at the minimum[6]: consent, purpose, source, sharing, destruction.
4. Capture only necessary information.
5. Ensure the right to access and capture information is necessary [refer to POPIA, which details the rights to access and the link to business information required].
6. Consider user rights and the management thereof in terms of the ICT Policy
7. Digital data storage must be considered in terms of access [passwords], limitation of users [access] and password policy [mandatory expiry requiring change, defined structure – minimum length, special characters] etc.
8. Paper-based information must be securely stored and when information is not needed [subject to SARS, Financial Intelligence-FICA requirements etc.]

E. IMPLEMENT POPIA COMPLIANCE POLICIES

1. Review all current policies that POPIA impacts.
2. Ensure the policies and procedures are appropriate and adequate.
3. Policies are only of use if they are monitored and enforced. Failure is negligence on the part of management.
4. Ensure the Policy is distributed and included in all policy manuals for all staff.

[5] Using a rational method for reaching reliable and reproducible conclusions in a defined and systematic process. The approach outcomes or estimate must be relevant, sufficient and verifiable.

[6] These must be detailed as per the requirements of POPIA

5. Ensure the Policy is explained to all staff and fully understood with staff signing that they have understood the objectives and the processes to confirm when and how data is captured and stored.
6. The framework must be discussed with staff at least quarterly to ensure the safeguards and risk mitigation is still applicable and relevant.
7. Stakeholder groups must receive an appropriate notification that is specifically designed for various target groups.
8. Third-party[7] risks must be specifically managed.

F. WEBSITES AND OTHER SECURED WEB AND ONLINE STORAGE SITES

1. Establish a process for reviewing websites.
2. Ensure disclaimers are adequate.
3. Ensure no personal information is outward-facing [i.e. visible to users].
4. Ensure cache information and personal information is protected against malware, cyber and other digital intrusions.
5. Develop a schematic approach to red flag high risk and priority info.
6. Ensure benchmark standards ICT are employed and get formal assurance from hosting providers and other website services used.
7. All risk mitigation requires a crisis plan, ensure this is developed for POPIA – these are generally standard and encompasses a communication plan should there be a breach.

G. POPIA MANUAL

1. Ensure your POPIA manual is ready and staff trained by 1 July 2021
2. If already in place, review your POPIA manual
3. Ensure your manual follows the prescribed format as per the POPiA and minimum standards.

[7] This refers to outsourced suppliers and service providers which encompasses unique risks as they have access to personal information and in many instance has access to digital files and information. Outsourced paper storage requires its own risk mitigation

H. POPIA BUSINESS EXCELLENCE MODEL

1. Develop your business excellence model[8]
2. Develop reasonable and appropriate processes and systems for ongoing compliance
3. Review acquisition, processing, retention, storage and destruction practices
4. One of the most significant risks is that staff keep their lists with potential personal information. There should be a single shared database of information [various options are available, small firms can access limited Client Relationship Management software [CRM].

   Alternatively, firms can use the Financial system or Practice Management database as the primary source of shared information.
5. Review the integration of all policies and systems within the firm by internal audit or other types of review.
6. Consolidate your reports and develop a schematic summary that highlights key areas and significant lapse of controls. Act on 'outliers[9]' in the consolidated report.

I. TRAINING IN POPIA COMPLIANCE

1. Training is tailored to each firm's needs and requirements
2. Training like other risk training [cyber, ICT etc.] must be continuous and adapt to the changing environment and the evolution of risks.
3. For large firms, the pace of changes of digital risks is highly volatile and can happen within a few hours or days, as the digital world is interconnected and risk management at the high end is done in real-time with the use of AI and algorithms.
4. Post-COVID, online, and hybrid training is the norm, and there can be no excuse for lack of training.

[8] Business excellence Model sample slide is attached for engagement with all staff who are involved with data and personal information.

[9] Results or statistics that are abnormal compared to the majority of results [standard]

J. POPIA COMPLIANCE IS INTEGRATED INTO THE BUSINESS PROCESS

1. POPIA must be treated as other risk management in the firm and must be integrated into all relevant business processes.
2. The processes and systems must be seamlessly integrated into all business process.
3. Like all risk management, it requires vigilance and review to ensure trends, regulations; legislation is reviewed for both risks and opportunities.
4. Risk management must be reviewed on how it impacts the practice achieving its objectives, both negatively and positively.
5. The potential negative impact may require mitigation, and opportunities can be grasped. However, ultimately these are all business decisions.