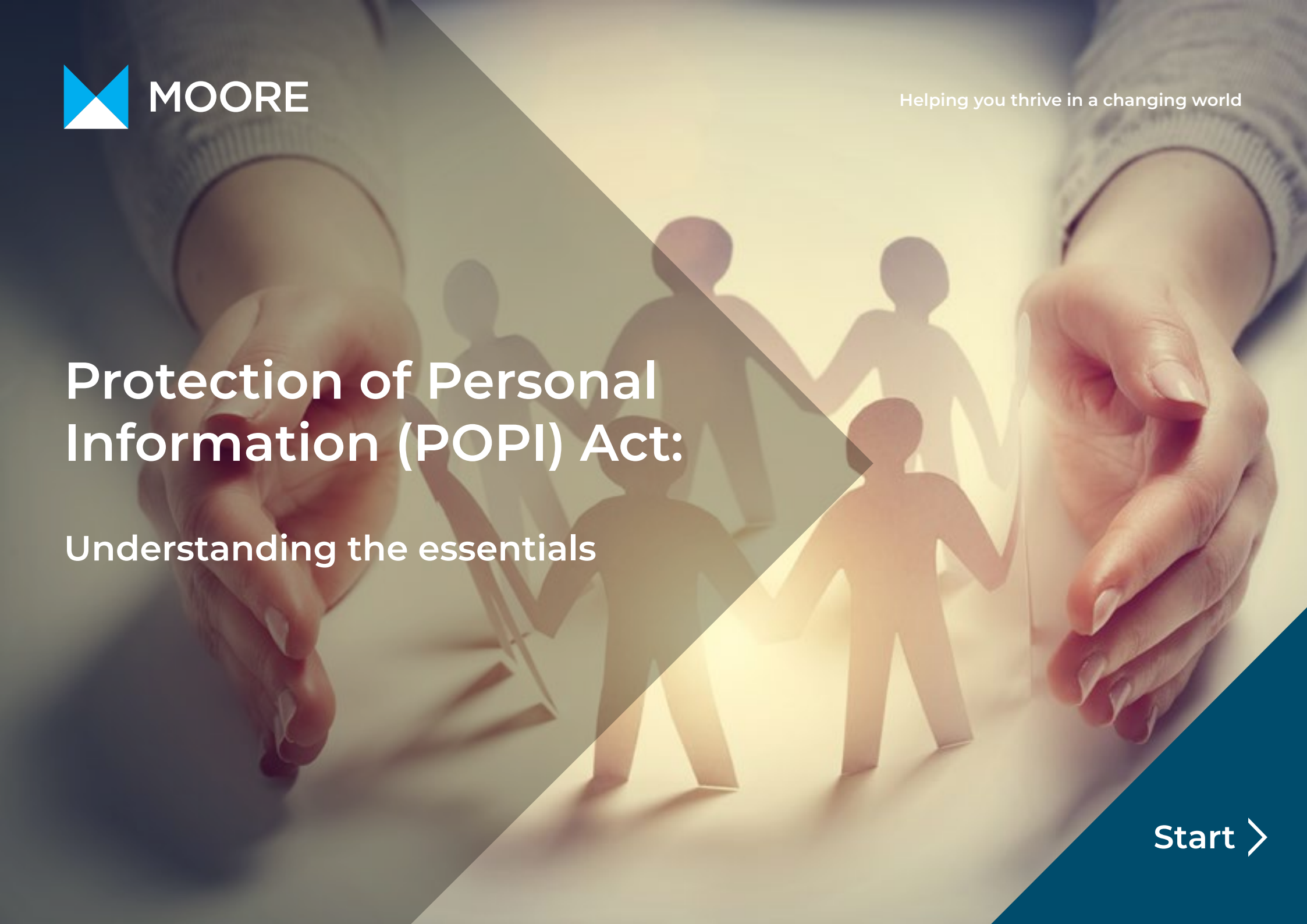

MOORE

Helping you thrive in a changing world

Protection of Personal Information (POPI) Act:

Understanding the essentials

Start

The context and purpose of this eBook

Context

The President of South Africa proclaimed the commencement date of the Protection of Personal Information Act 4 of 2013 (hereinafter referred to as the POPI Act), to be 1 July 2020. A grace period of one year was granted for all parties who process personal information to comply with the Act. This means that the effective date for compliance is 1 July 2021.

The POPI Act will change the way businesses deal with information in an information-driven economy and society.

The purpose of this Act is to:

1. Give effect to the constitutional right to privacy, by safeguarding the processing of all personal information in such a way that it
   - balances the right to privacy against other rights (such as the right of access to information), and
   - protects important interests, including the free flow of information within South Africa and across international borders.

2. Regulate the manner in which personal information may be processed lawfully, through conditions which are in harmony with international standards.
3. Provide persons (natural and juristic) with rights and remedies to protect their personal information from being processed in an unlawful manner.
4. Establish measures (such as the Information Regulator) to ensure that the rights that are protected in this Act are respected, promoted, enforced and fulfilled.

Purpose of this eBook

An understanding of this Act will benefit all individuals, organisations and businesses.

Therefore, the purpose of this eBook is to:

1. Provide an overview of the most important parts of the Act.
2. Offer practical guidance towards compliance with the Act.

Index

1. Does the POPI Act apply to my business?

The POPI Act applies to all **processing** of **personal information** which is entered into a **record** by a **responsible party** who is domiciled in South Africa, or who makes use of means in South Africa (except when those means are only used to forward information through South Africa).

Personal information (PI) is any information relating to

- an identifiable, living natural person, or
- an identifiable juristic person.

Ordinary PI includes:

- Gender, marital status, age, language
- Identifying numbers (e.g. ID / passport)
- Email addresses, physical addresses, telephone numbers, social media handles
- Location information (e.g. GPS)
- Communications
- Opinions
- Preferences or eccentricities
- Information that, if found together with a person's name, would say something about that person (e.g. name on a maintenance defaulters list).

Special PI includes more sensitive information such as:

- Sexual orientation
- Ethnicity
- Trade union membership
- Religion
- Political views.

Processing includes anything that is done with personal information, such as:

- Collecting it
- Receiving it
- Organising it
- Collating it
- Recording it
- Updating it
- Modifying or altering it
- Consulting it
- Using it
- Retrieving it
- Distributing or transmitting it
- Discarding or destroying it.

A record is any recorded information, regardless of the medium. It includes:

- Writing on any material
- Any information on a tape recorder, video recorder or computer equipment
- Labels, markings or other writings
- Books, maps, plans, graphs or drawings
- Photos, films, negatives, tapes or other devices which store and/or enable reproduction of the information.

A responsible party is any public or private body who decides

- to process information
- how to process the information, and
- what the information is used for.

A responsible party can be a

- natural person
- juristic person, or
- government body.

It can also be a group of these bodies.

Therefore, the POPI Act will have an impact on all businesses!

Even if a business is not processing personal information in its day-to-day activities, it will always process information about its employees and/or suppliers and/or clients.

1. Does the POPI Act apply to my business? (Continued)

Answer the following four trigger questions to determine whether the POPI Act applies to your business:

1 Is the business processing personal information?

2 Is the PI entered into a record?

3 Is the PI processed by a responsible party?

4
- Is the PI processed in South Africa?
- Or does the responsible party have a place of business in South Africa?
- Or does the responsible party make use of means in South Africa to process the information?

If the answer to all four questions is "yes", the POPI Act will apply.

The exceptions: When the POPI Act does not apply

1 If the PI is processed as part of a purely personal and household activity.

2 If the information is de-identified and cannot be re-identified by any foreseeable, reasonable method.

3 If PI is processed by certain functions of public bodies, as long as adequate measures to protect the PI are implemented, including:
- National security
- Department of Justice
- Judicial functions of the courts
- SAPS
- Cabinet, its committees and Provincial Executive Councils.

4 If the information is processed
- for purely journalistic, literary or artistic purposes
- to reconcile the right to privacy with the right to freedom, and
- in the interest of the public.

5 If the Information Regulator has granted an exemption.

6 If the responsible party's lawful function is to protect the public against certain acts, some sections of the POPI Act will not apply.

2. POPI Act: The parties

During the processing of personal information (PI), four main parties are potentially involved. Depending on their role in the process, certain POPI Act rights and obligations become applicable.

1 Data subject

The person to whom the PI relates.

This includes:
- living, natural persons
- identifiable juristic persons.

- Data subjects are given specific rights to allow them some measure of influence over the processing of their personal data.
- We will provide an overview of these rights as a dedicated topic in this eBook (5. The rights of data subjects).

2 Responsible party

Any public or private body who decides:
- to process PI
- how to process the PI, and
- what the PI is used for.

A responsible party can be a:
- natural person
- juristic person, or
- government body.

It can also be a group of these responsible party bodies.

- The responsible party is ultimately accountable for the lawful processing of PI.
- The Act primarily imposes obligations, duties and liabilities on the responsible party.
- Responsible parties may make use of operators in the processing of PI, but cannot outsource their own ultimate accountability.
- Responsible parties must have written contracts with their operators to ensure that these operators process PI in a lawful manner, in accordance with the Act.

2. POPI Act: The parties (Continued)

During the processing of personal information (PI), four main parties are potentially involved. Depending on their role in the process, certain POPI Act rights and obligations become applicable.

3 Operator

A person (natural or juristic) who processes PI for a responsible party.

An operator:

- Processes PI solely in the interest of, and on behalf of, another.
- Does so according to the responsible party's instructions, but without coming under their direct authority.
- Does so in terms of a written contract.
- Would dispose of the PI after the contract period ends.
- Is merely a service provider.
- Does not use the PI for any of the operator's own purposes.

The operator must:

- Only process PI with the knowledge or authorisation of the responsible party.
- Treat the PI as confidential, and may not disclose it, unless required by law or to properly perform their duties.
- Under their contract with the responsible party, process PI in a lawful manner (in accordance with the Act), and must establish and maintain security measures to safeguard the PI.
- Notify the responsible party immediately where there are reasonable grounds to suspect unauthorised access of PI.

4 User

Anyone processing PI on behalf of a responsible party, or on behalf of an operator.

For example, an employee of either of these parties.

The user must:

- Only process PI with the authorisation of the responsible party / operator.
- Treat the PI as confidential, and may not disclose it, unless required by law or to properly perform their duties.
- Take all reasonable and practicable steps to secure the safety of PI in his/her possession.
- Notify the responsible party / operator immediately when they suspect a data breach.

3. The legal basis for processing personal information

The POPI Act requires that personal information (PI) be processed for a lawful purpose.

The Act specifies six justifications that are sufficient to render the processing of the PI lawful:

1	**To conclude or perform in terms of a contract**	If the PI must be processed to conclude or perform in terms of a contract, the processing is considered lawful.	**eg:** A customer buys a product and pays an additional amount for delivery to a specific address. In this case, the explicit consent to use the PI (the address) is not required, as the information is required to perform according to the sales contract.
2	**To comply with an obligation imposed by law**	If the law requires that a specific processing activity takes place, the processing activity is lawful.	**eg:** The Employment Equity Act and Basic Conditions of Employment Act provide justification for specific employee PI to be processed.
3	**To protect the legitimate interest of the data subject**	A legitimate interest is one that is sanctioned by law or other rules.	**eg:** If a person's medical history is disclosed to a hospital's Emergency Unit treating them after a serious road accident, it would be justified.
4	**To perform a public law duty, as a public body**	Public law regulates the relationship between the state and persons. If the processing of PI is necessary to perform in accordance with public law, the processing activity will be lawful.	**eg:** The processing of PI by municipalities in order to provide us with water and electricity is lawful.

3. The legal basis for processing personal information (Continued)

The POPI Act requires that personal information (PI) be processed for a lawful purpose.

5 **To pursue the legitimate interests of the responsible party or third party to whom the PI is given**

If the purpose is to pursue the legitimate interests of the responsible party (or a third party to whom the information is supplied), the processing of the PI can also be justified. The processing of such PI must, however, be fair and lawful, and must comply with all the data protection principles.

eg: A finance company is unable to locate a client who has stopped making payments under a hire purchase agreement. The finance company engages a debt collection agency to find the client and seek repayment of the debt. It discloses the client's PI to the agency for this purpose. The PI is therefore processed for the purpose of the finance company's legitimate interests – to recover the debt.

6 **If the data subject has consented**

Data subjects can legitimise the purpose for which their PI is processed by giving consent. But the consent must be voluntary, specific, informed and an expression of their will.

eg: If a person provides their contact details to an online retailer, in order to be notified when a particular product is back in stock.

Fast fact

One of the common misconceptions about POPI is that data subjects must give their explicit consent in order for their personal information to be processed lawfully.

This is not the case.

It can be seen from the list that, even if consent was not explicitly obtained, the processing will be lawful if a legitimate justification exists.

4. The eight general conditions for lawful processing of personal information

The majority of the duties and obligations established by the POPI Act are grouped under eight general conditions for the lawful processing of personal information (PI). Practical compliance with these conditions comes down to good business practices that will improve the controls and processes of businesses. It is critical that all responsible parties are aware of these minimum threshold requirements as non-compliance carries heavy penalties. These conditions will require a thorough review of the business operations and how personal information is processed.

1 Accountability

The responsible party is accountable for complying with the full POPI Act. Its obligations cannot be contracted out by outsourcing the processing of PI.

Questions to ask

- Who will be tasked with the responsibility of compliance in our organisation?
- How will this individual ensure that we are POPI compliant?

2 Purpose specification

PI may only be processed for specific, explicitly defined and legitimate reasons.

Questions to ask

- For what specific, explicit and lawful purpose do we process PI?
- Are data subjects aware of the purpose for which we process their data?
- Can we link all PI processed to legitimate reasons for doing so?
- For what time period may we retain specific PI?
- How will we keep track of when PI must be destroyed?
- How will we ensure that we destroy PI in a manner that prevents reconstruction?

3 Processing limitation

PI must be processed in a fair, reasonable and lawful manner, and only with the consent of the data subject. Only the minimum-required and relevant PI should be processed.

Questions to ask

- Do we obtain PI directly from data subjects?
- Are data subjects aware that we are processing their PI and have they given us permission to do so?
- If we obtained the PI from a third party, have the data subjects consented to this PI being shared with, and used by, us?
- Is the amount of information we gather excessive?

4 Further processing limitation

PI may not be processed for a secondary purpose, unless that processing is compatible with the original purpose.

Questions to ask

- If we intend to reuse PI, is it compatible with the purpose for which it was originally collected?
- Is the data subject aware of the continued use of their PI?

4. The eight general conditions for lawful processing of personal information (Continued)

5 6 7 8

5 Information quality

The responsible party must take reasonable steps to ensure that the PI collected is complete, accurate, not misleading and updated where necessary.

Questions to ask

- How do we ensure that PI is reliable and accurate at all times?
- What processes do we have in place to allow data subjects to update or amend their information?
- What processes do we have in place to allow data subjects to withdraw consent?

6 Openness

Responsible parties are required to ensure that data subjects are aware that their PI is being collected, and for what purpose the PI will be used.

Questions to ask

- How do we gather PI from data subjects?
- What processes do we have in place to get their consent to process their PI?
- How do we inform the data subject of the purpose for which their information is being gathered and used?
- What evidence do we have that data subjects have consented to the processing of their PI?
- Do data subjects know who to contact in our organisation regarding their PI?
- How do we inform data subjects of their right to lodge a complaint with the Information Regulator?
- Have we advised all data subjects of their rights in terms of the POPI Act?

7 Security safeguards

PI must be kept secure against the risk of loss, unlawful access, interference, modification, unauthorised destruction and disclosure. These safeguards include physical, technical and organisational safeguards.

Questions to ask

- Are we identifying foreseeable internal and external risks to PI in our possession?
- How do we prevent PI from falling into unauthorised hands?
- How do we maintain appropriate safeguards?
- How do we determine who gets access to which PI?
- How would we know when PI has been accessed or modified without authorisation?
- How will we identify the source of a data breach?
- How will we rectify and respond to a data breach?
- How do we ensure that safeguards are continually updated?
- How do we ensure the protection of shared PI?
- How will we inform data subjects of data breaches?
- How will we inform the Information Regulator of any security breach?

8 Data participation

Data subjects are entitled to some measure of influence over the processing of their personal data. Their rights include to know whether their PI is held, as well as to request the correction and/or deletion of any PI.

Questions to ask

- Who is responsible for managing and responding to data subject requests?
- What data subject requests can we expect to receive?
- How will we handle and adhere to requests from data subjects?
- Will we charge a reasonable fee for certain data subject requests?
- What processes do we have in place to allow data subjects to correct PI or withdraw consent to process their information?

5. The rights of data subjects

If any of your personal information (PI) is processed by another party, you are a data subject. As a data subject, you have specific rights under the POPI Act.

This is true for all living, natural persons, as well as for juristic persons.

Remember that "processing" includes the collection, receipt, organisation, collation, recording, updating, modification, alteration, consultation, use, retrieval, distribution, transmission, destruction and/or discarding of personal information.

1 The right to be informed

You have the right to be informed if your PI is processed.

2 The right of access

You have the right to establish if any of your PI is being processed by a specific party. You have the right to request access to the PI being processed.

3 The right to rectify

You have the right to request that your personal data be corrected or amended.

4 The right to erase

You have the right to request that your PI be deleted or destroyed.

5 The right to restrict

You have the right to request that your PI only be used for specific (restricted) purposes.

6 The right to object

You have the right to object (on reasonable and lawful grounds) to your PI being processed. You have the right to specifically object to your PI being processed for direct marketing purposes.

7 The right against automated processing decisions

You have the right to not be subject to decisions which affect you to a substantial degree and which are based solely on the automated processing of your PI.

8 The right to be notified

You have the right to be notified if any of your PI was accessed by an unauthorised person/s.

9 The right to complain

You have the right to submit a complaint to the Information Regulator if you feel that your right to the protection of your PI has been breached.

10 The right to civil proceedings

You have the right to institute civil proceedings if you feel that your right to the protection of your PI has been breached.

6. The role of the Information Officer

Who is the Information Officer (IO)?

- The POPI Act identifies the head of the business as the IO. Depending on the type of business, the IO will therefore be the sole trader, a partner in a partnership, or CEO (or equivalent) in a company or CC.
- The CEO or equivalent may authorise another senior person in the entity to act as IO.
- Each subsidiary of a group of companies must register its own IO.
- The IO required by POPI is, or may be, the same IO referred to in PAIA (Promotion of Access to Information Act 2 of 2000).

May an Information Officer (IO) delegate his / her duties?

- The IO may appoint as many Deputy Information Officers as necessary.
- Deputy Information Officers (DIOs) should report to the highest management office within the organisation and should, therefore, be employees.

When may IOs and DIOs take up their duties?

- IOs and DIOs must register, and may only take up their duties once registered, with the Information Regulator.
- Register online by using the Information Regulator Portal (https://www.justice.gov.za/inforeg/portal.html).

What are the duties and responsibilities of IOs and DIOs?

- Encourage and ensure compliance with the full POPI Act.
- Deal with any POPI-related requests made to the organisation, including data subject requests.
- Work with the Information Regulator on any POPI-related investigations.
- Develop, implement, monitor and maintain a compliance framework.
- Do a personal information impact assessment to ensure the lawful processing of personal information.
- Develop, monitor, maintain and make available a POPI / PAIA manual.
- Provide copies of the manual to anyone who asks for it.
- Develop measures and systems to process requests for access to information.
- Conduct internal awareness and training sessions on the POPI Act.
- Provide the Information Regulator with access to records, on request.
- To perform any other duties prescribed by the Information Regulator (i.e. keep an eye on https://www.justice.gov.za/inforeg).

7. Does the POPI Act affect direct marketing?

Yes, definitely!

How does the POPI Act affect the regulation of direct marketing?

Pre-POPI, direct marketing was regulated by the Consumer Protection Act (CPA). Post-POPI, the CPA still regulates all forms of direct marketing activities, but the POPI Act regulates direct marketing involving *electronic communication.*

Electronic communication includes:

- emails
- text and voice messages
- electronically-sent images and footage
- automatic calling machines
- faxes
- newsletters
- etc.

Which legislation prevails?

If both the POPI Act and the CPA apply, the Act which provides greater protection will prevail.

What does the POPI Act require?

Direct marketing to non-customers may only be done once they gave their consent to receive such communications.

What does consent look like?

Consent must be

- voluntary
- specific
- informed
- an expression of will (i.e. some action must be taken).

Consent can, therefore, not be hidden within T&Cs.

A good rule of thumb is to ask, "Will this person be surprised to hear from us?". If the answer is "yes", you have not yet received the required consent.

Are the consent requirements the same for existing and non-customers?

In short: Some requirements differ, whilst others are the same.

Existing customers	Non-customers
Electronic direct marketing may only be sent if the customer's contact details were obtained • in the context of the sale of a product or service, and • for the purpose of direct marketing of similar products or services. **The customer must be given a reasonable opportunity to object to the direct marketing** • at the time the personal information is first collected, and • on every subsequent communication.	Electronic direct marketing may only be sent if the non-customer had given their voluntary, specific, informed consent, explicitly. Non-customers may only be contacted *once* to obtain this consent.
• The sender's name and contact details must be made available with each direct marketing request and communication. • An unsubscribe option must always be included: easy-to-see, easy-to-understand and easy-to-execute.	

7. Does the POPI Act affect direct marketing? (Continued)

Opt-in or opt-out?

The Opt-in method of consent requires the customer to take the positive step of ticking to grant consent. The default position is that direct electronic marketing may not be sent until consent is given.	The Opt-out method is one where consent has been pre-ticked and where the customer must untick it to withdraw consent. The default position is that direct electronic marketing may be sent until consent is withdrawn.
☐ I want to receive marketing via email. (must be ticked)	☑ I want to receive marketing via email. (must be unticked)

Which records must be kept?

Responsible parties must keep record of:

- date of consent
- method of consent
- wording of the consent
- who obtained the consent
- proof that an opportunity was given to unsubscribe / withdraw consent on each marketing occasion
- customer information that was obtained in association with the consent
- unsubscribes.

Remember that additional regulation by the CPA still applies!

For example:

- Specific times at which customers may be contacted.
- A do-not-contact registry.

8. What to do when a data breach occurs

Below are suggestions on how to deal with data breaches, based on sensible governance principles. If you experience or suspect a data breach, it is critical that you immediately seek professional advice and assistance.

What is a data breach?

A data breach occurs when personal information (PI) was accessed or acquired by an unauthorised person.

What does the POPI Act require?

Condition 7: Security safeguards

A responsible party must secure the integrity and confidentiality of PI in its possession or under its control by taking appropriate, reasonable **technical** and **organisational measures** to prevent the

- loss of PI
- damage to PI
- unauthorised destruction of PI
- unlawful access to PI, or
- unlawful processing of PI.

The level of information security must be proportionately suitable and proper considering the type of PI being processed.

What is meant by technical and organisational measures?

Technical measures protect computerised or digital information. Inadequate technical measures could lead to cyber security breaches. But technical measures could also be compromised in the case of a lost laptop/phone/tablet, a lost backup, forgetting to wipe the disc of a discarded machine, an employee leaving your firm with PI on a USB drive, or an online password being compromised.

Organisational measures include policies and procedures that specify how information (including physical records) is processed throughout the organisation's information lifecycle. It will also include tightening access control to areas where PI is kept, specifying who has access to which information, etc.

The requirement to notify

Where a data breach occurs, the POPI Act requires the responsible party to report the breach to both the Information Regulator and the affected data subject/s.

Take the following steps to achieve compliance:

8. What to do when a data breach occurs (Continued)

How do we notify the Information Regulator?

Notification to the Information Regulator must be in writing.

It should include sufficient detail about

- the breach itself
- the extent of the impact
- the identity of the unauthorised person who may have accessed or acquired the PI (if known)
- the measures the responsible party intends to take, or has taken, to address the security compromise (including notification to data subjects).

How do we notify data subjects?

The notification itself must be in writing and should be communicated in at least one of the following ways:

- Via E-mail
- Posted to the data subject's last known address
- Placed in a prominent position on the website of the responsible party
- Published in the media, or
- As directed by the Information Regulator.

The notification must include sufficient information to allow the person to take protective measures against the potential consequences of the compromise, including

- a description of the possible consequences of the security compromise.
- a recommendation on what measures the data subject should take to mitigate the possible adverse effects of the breach.
- a description of the measures the responsible party intends to take, or has taken, to address the security compromise.
- if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the PI.

Is there a timeline for notification?

The notification will have to be made as soon as reasonably possible after the discovery of the compromise.

The Act does not prescribe what this period must be. It will vary on a case-by-case basis, as it is dependent on the measures the responsible party needs to take to

- determine the scope of the compromise
- restore the integrity of the information system, and
- provide law enforcement with sufficient time to fulfil its obligations.

Notification to data subjects may only be delayed if a public body responsible for the prevention, detection or investigation of offences, or the Information Regulator, determines it will impede a criminal investigation.

What if we outsource the processing of PI (use operators)?

If an organisation, as responsible party, outsources certain services which involve the processing of personal information to a third-party (operator), that organisation remains liable for the protection of that PI – even though it is not processing the PI itself.

A third-party service provider may in some instances provide improved data security if it is a specialised service provider with stringent protection of PI measures in place. To the extent that organisations rely on third-party service providers, these third parties should be reputable service providers with a proven track record.

But remember that organisations cannot evade their data protection responsibilities simply by relying on a third-party service provider.

8. What to do when a data breach occurs (Continued)

Are there any other obligations that we should be aware of?

The Cybercrimes Act 19 of 2020 notes further obligations of specific organisations when they become aware that their computer systems have been involved in a cyber security breach, as defined by this Act.

Apart from any data breach notification obligations set out in legislation, there may be additional contractual obligations regarding what an organisation must do in the event of a data breach, as set out in agreements with its suppliers or customers, or as set out in its privacy policy.

What could happen if we do not issue a data breach notification?

Failure to notify is a contravention of the POPI Act and may result in imprisonment, a fine, or both. Damages may also be awarded against the responsible party.

To the extent that there are notification or other obligations in contracts, an organisation must ensure adherence to these obligations to avoid a contractual breach.

What can we do now, proactively, to prepare for the eventuality of a data breach?

1. Do a thorough risk assessment, and put preventative measures in place.
2. An organisation could incur costs and losses as a result of a data breach. Therefore, organisations should consider purchasing tailored liability insurance which covers the losses associated with data breaches or cyber-attacks.
3. Have a comprehensive Incident Response Plan that sets out:
   - How potential breaches must be reported internally.
   - To whom potential breaches must be reported internally (recommendation: to the Information Officer, or Deputy Information Officer).
   - The required timeline for reporting potential breaches internally.
   - Who is assigned to respond to data breaches.
   - The steps to be followed once a potential data breach has been reported.
   - The internal response time.
   - How internal notification will be handled.
   - How, and by whom, all employees (including frontline employees such as receptionists) will be instructed to respond to any enquiries.
   - How, and by whom, insurers will be notified (if applicable).
   - How notification to the Information Regulator will be made, and by whom.
   - How notification to data subjects will be made, and who will take responsibility for this.
   - How notification to any other authorities or persons will be made.

9. Enforcement and penalties

The clock is ticking!

The commencement date of the POPI Act was 1 July 2020. A grace period of one year was granted for all parties who process personal information (PI) to comply with the Act.

This means that the effective date for compliance is 1 July 2021!

How will POPI be enforced?

Sections 39 to 54 of the POPI Act (which came into effect on 11 April 2014) establish an Information Regulator who will enforce both POPI and PAIA.

What happens when a complaint is submitted to the Information Regulator?

Any person (whether they are the data subject or not) may submit a complaint to the Information Regulator, alleging non-compliance with POPI or any approved POPI-related codes of conduct.

A Complaints and Dispute Resolution Committee has been established by the Information Regulator to ensure that a dispute resolution and complaints management system is in place to resolve grievances that arise from the processing of PI and the right of access to information, in an effective manner.

The Regulator itself may also initiate an investigation into any interference with the protection of personal information.

Which complaints can be submitted to the Information Regulator?

- Any breach of the conditions for the lawful processing of PI.
- Any non-compliance with any of the sections of the Act.
- Breaches of codes of conduct which may be established for particular industries or professional vocations.

Which offences, penalties, administrative fines and civil remedies does the Act provide for?

POPI creates less serious, as well as more serious offences and indicates penalties and administrative fines for each.

	Fine		Imprisonment
Less serious:	Not exceeding R10 million	OR	Not exceeding 12 months
More serious:	Not exceeding R10 million		Not exceeding 10 years

The penalty for both types of offences may include both a fine and imprisonment.

The Act also makes provision for a civil action for damages resulting from non-compliance with the POPI Act. This action can be brought by a data subject or by the Information Regulator acting on behalf of data subjects.

How does the Information Regulator determine appropriate penalties or fines?

The Information Regulator will take the following into account:

- The nature of the PI involved.
- The duration and extent of the contravention.
- The number of data subjects affected, or potentially affected.
- Whether or not the contravention raises an issue of public importance.
- Whether the responsible party or third party could have prevented the contravention from occurring.
- Any failure to carry out a risk assessment, or a failure to operate good policies, procedures and practices to protect PI.
- Whether the responsible party has previously committed an offence i.t.o. POPI.

10. Eight steps towards POPI compliance

1 Know what is required – get to know the Act!

2 Initiate POPI Act compliance.

- Identify all your relevant stakeholders.
- Determine who will manage, and take responsibility for, your journey towards compliance.
- Set a project plan: outline actions, due dates and resources (human and budgetary).

3 Appoint an Information Officer (IO).

- If you already have a Promotion of Access to Information Act (PAIA) IO, align this role to the role of the POPI Act IO.
- Decide whether the IO can fulfil the function alone, or whether one or more Deputy Information Officers (DIOs) should be appointed.
- Formally appoint IOs / DIOs, and agree roles and responsibilities.
- Register IOs and DIOs with the Information Regulator by using the required templates and submitting them via the designated channels.

4 Create awareness – conduct information and training sessions with all senior management and all employees.

5 Perform a POPI Act gap analysis: Do a personal information impact assessment and risk assessment.

- Determine your organisation's information lifecycle: what information is collected, how it is collected, by whom it is collected, what it is used for, how it is stored and processed, how it is retained and destroyed, and whether it was collected with the necessary consent.
- Compare this to the requirements of the Act.
- Identify compliance gaps.
- Identify and categorise risks.

6 Develop a compliance framework and take the necessary steps towards compliance.

- Determine corrective and preventative actions in response to the risks identified. This could include new and/or amended policies, procedures, processes, systems, registers, contracts and other documentation.
- Ensure that your compliance framework covers your organisation's full information lifecycle.
- Set an action plan, implement the actions, monitor implementation and close out actions.
- Set a review schedule to ensure future adequacy of policies, processes and systems implemented.

7 Remember to address specific focus areas.

- Conduct a thorough cyber security assessment.
- Develop and make available your organisation's POPI policy and PAIA manual.
- Review all your websites, social media platforms and marketing practices for compliance.
- Review all processing of special personal information and the personal information of children.
- Ensure compliance of all cross-border information flows, if applicable.
- Ensure the existence of Operator contracts.
- Structure processes for receiving and responding to data subject requests and complaints.
- Design your process to respond to potential data breaches.

8 Make POPI compliance "Our way of doing business"!

11. Important POPI Act-related contact details

Access the Information Regulator website: Click here

Access the Protection of Personal Information Act 4 of 2013, as well as any related regulations and notices: Click here

Access the online portal for the registration of Information Officers and Deputy Information Officers: Click here

For support in registering Information Officers and Deputy Information Officers: Click here

For general enquiries of the Information Regulator: Click here

To submit complaints to the Information Regulator: Click here

Physical address of the Information Regulator:

JD House
27 Stiemens Street
Braamfontein
Johannesburg
2001

Postal address of the Information Regulator:

P.O Box 31533
Braamfontein
Johannesburg
2017

12.1 Tips to stay safe online

1 Understand who is behind security incidents

Online criminals

They are really good at identifying what can be monetised. For example:

- Stealing and selling sensitive information.
- Holding systems or information hostage.

Honest mistakes

Sometimes people merely make mistakes. For example:

- Emailing sensitive information to the wrong address.
- Providing sensitive information on request, with the best intentions.

Malicious insiders

They use their access to systems and information for malicious intent. For example:

- Sharing sensitive information with competitors.
- Selling sensitive information for personal gain.

2 Defend yourself against phishing attacks

Phishing emails and messages appear genuine, but are actually fake. They trick you into accessing malicious links, or revealing sensitive information.

- Phishers use public information to tailor their messages convincingly. Review your privacy settings and think before you post something.
- Be aware of phishing luring techniques, such as urgency or authority cues that pressure you to act.
- Phishers exploit normal or generic business processes. Know your organisation's policies and processes, in order to spot unusual activity.
- If you've clicked on a phishing email, report it immediately to reduce potential harm.

3 Secure your devices

Attackers exploit smartphones, tablets, laptops and desktop computers both remotely and physically.

- Don't ignore legitimate software updates – they keep your devices secure.
- Always lock your device when not using it.
- Avoid downloading dodgy apps, and only use official app stores.

4 When in doubt, call it out

Reporting incidents promptly and comprehensively can reduce potential harm.

- Ask for guidance or support when something feels suspicious or unusual.
- Report attacks as soon as possible, with as much information as you can.
- Challenge security policies and processes that make your job difficult, rather than ignoring or bypassing these.

5 Use strong passwords

Attackers always try the most common passwords. And they exploit our tendency to use one password for everything.

- Create strong and memorable passwords for important accounts.
- Use separate passwords for different accounts.
- Avoid being predictable in selecting passwords.
- Avoid using publicly available information as passwords.
- Store passwords securely (if at all) and do not share it.
- Use two-factor authentication (2FA) for important sites such as banking and email.

Obtain information security advice from reputable industry experts and seek immediate professional advice in case of a breach.

12.2 Tips on USB device safety

What is a USB device?

A USB device is any external device that plugs into a computer via a USB port. This includes any device that can sync, store or charge via a USB port.

Examples:

- Memory sticks (USB drives)
- External hard drives
- Smart phones
- Smart watches
- Wearable fitness trackers
- Cameras
- Keyboards
- Computer mice

What are the pros...

The pros

- Convenient data back-up, data storage and data transfer.
- Fast, durable and reliable.
- Portable and some devices are relatively inexpensive.
- Easy to use, with nil or negligible power usage.
- Less risk of losing data due to dust, exposure to magnetic fields or shocks, scratches etc.
- Denser data storage in comparison to other removable media such as CDs or DVDs.
- Available in different storage capacities.
- A multitude of synchronisation options between devices.

and cons of USB devices?

The cons

- The biggest risk related to a USB drive is losing or misplacing the drive due to its small size – and then losing the information on it.
- Some USB drives have weaknesses or chinks in encryption that can pose security threats.
- USB drives and other USB devices can be used as pawns to infect computers, or spread infection between computers and/or other devices.
- Internet of Things (IOT) USB devices such as fitness trackers or smart watches, contain a lot of personal information and can be hacked.

12.3 Information security essentials for employees

What is information security?

Information security is the protection of information and systems from unauthorised access, disclosure, modification, destruction or disruption.

What are the objectives of information security?

Confidentiality	Integrity	Availability
Protect information from unauthorised access or disclosure. Ensure that those who are authorised to access information are able to do so, and those who are not authorised are prevented from doing so.	Protect information against unauthorised modification or destruction. Ensure that information and information systems are accurate, complete and uncorrupted.	Protect information and information systems from unauthorised disruption. Ensure timely and reliable access to, and use of, information and information systems.

What is your role in information security?

1. Know your information

Be mindful of the type of information you handle and the level of risk this entails:

- Public information
- Private information
- Restricted information.

2. Protect electronic information

- Avoid storing restricted, private or sensitive information on mobile devices.
- Keep personal and business devices, and personal and business information, separate.
- Use a risk-based approach in deciding whether to store information on a USB device.
- Don't transmit restricted, private or sensitive information via email or other insecure messaging solutions without the consent of the data subject.
- Don't use personal email for business communications, and vice versa.
- Use strong passwords and two-factor authentication wherever possible.
- Secure all your devices at all times.

3. Safeguard electronic communications

Electronic communications can be in the form of email, instant messaging, text messaging, social media posts, online communication, etc.

- Think before sending any information by way of electronic communication.
- Avoid opening attachments from an untrusted source.
- Avoid clicking on links in electronic communications from sources that you do not know.
- Be wary of phishing scams.
- Be sure to check the recipient's details before sending electronic communications.

4. Secure your computer and other devices

- Do not connect automatically to public wireless networks.
- Disconnect your computer from the wireless network when it is not in use.
- Use caution when enabling browser pop-ups.
- Use caution when downloading and installing software.
- Lock your devices when these are unattended.

12.3 Information security essentials for employees (Continued)

5. Safeguard your password

- Use strong passwords.
- Change your passwords periodically.
- Avoid using the same password for multiple accounts.
- Avoid predictable passwords.
- Avoid using publicly available information as your password.
- Don't write your password down or store it in an insecure manner.
- Don't share your password with anyone for any reason.
- Never let anyone use your password to log into a system.
- Never share your passwords with co-workers while on leave.
- Don't use automatic login functionality on public sites.

6. Keep information physically secure

- Locks only safeguard information if they are used.
- Locks only safeguard information if the key or code is also safeguarded.
- Close and lock your door when leaving your office unattended.
- Lock filing cabinets that store personal information.
- Don't leave information in plain view on your desk or on a whiteboard.
- Don't leave information sitting in a printer, copier, fax machine or other peripheral device.

7. Protect verbal communication

- Be mindful of your surroundings when discussing business-related information. This is as true for phone calls as it is for in-person discussions.
- Don't discuss information with individuals who do not need to have knowledge of it.
- Be careful with any information that you provide on request – remember that the POPI Act requires the data subject's permission for personal information to be shared.
- Be aware of who has line-of-sight to your device screens.

8. Discard data appropriately

- Dispose of information when it is no longer needed for business purposes, according to your document retention policy and procedure.
- Use an appropriate computer programme to dispose of electronic data in such a way that it cannot be reconstructed.
- Be cautious of using external devices for temporary storage or data transfers, and remember to wipe the discs once the reason for using an external device is no longer valid.
- Use a cross-shredder to dispose of paper-based and written information.

9. Avoid risky online behaviours

- Be cautious when using file sharing applications.
- Be cautious when browsing the web.
- Be cautious when clicking on shortened URLs.
- Avoid responding to questions or clicking on links in pop-up windows.

10. Report suspected security breaches

- Report any potential security breach as soon, and as comprehensively, as possible.
- Report the loss or theft of any of your devices as soon as possible.
- Report any compromises of any of your passwords as soon as possible.

Remember:

Information security is the responsibility of everyone in the organisation!

CONTACT US

For more information, please email info@mooresa.co.za or
Visit: www.moore-southafrica.com to locate your nearest firm.

MOORE South Africa

www.moore-southafrica.com

Disclaimer

Moore South Africa (Pty) Ltd makes selected training material and other guidance resources available to clients and contacts of Moore South Africa firms, and visitors to its website, free of charge. Moore South Africa is not a registered or accredited training provider. Training material and guidance resources are compiled by the network's internal Learning & Development team.

Training material and guidance resources are intended for general informational purposes only.

The *POPI Act: Understanding the essentials* guide is intended purely as general information to assist clients and contacts of Moore South Africa firms in navigating their way towards compliance with the Protection of Personal Information Act, 4 of 2013 (POPI). Whilst we endeavour to compile all our material from research that include reputable and reliable sources, its contents should not be viewed as advice of a legal nature. We cannot, and do not, warrant or guarantee the accuracy of any information contained in the material.

We have endeavoured to make the material generic in nature. We do not warrant or guarantee that the material is suitable to any particular type of business or person. Should any person use the material, or adapt the material in any way, they do so entirely at their own risk. Moore South Africa will not be held liable for any loss, damage or other claim that may flow, directly or indirectly, from the use of the material by any person, including the use of any adapted or amended material.

Users of the material are required to familiarise themselves with the full Protection of Personal Information Act 4 of 2013, and have a responsibility to ensure that they are fully aware of the contents of this law, and any related laws and regulations, including how these apply to them and their business. Parts of the material may be extended, amended, or partly or completely deleted by Moore South Africa without announcement.

Our Privacy Policy and Disclaimer, available on the Moore South Africa website (https://www.moore-southafrica.com), applies.