



# POPIA Handbook

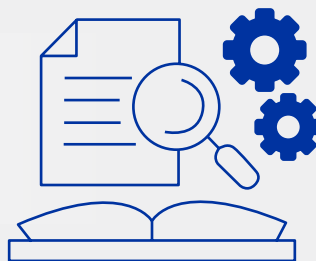
POPIA is effective from 1 July 2021.

In response we have prepared this handbook for our Estate Agent clients on important and relevant POPIA information and its potential impact on the way you conduct business.

**JULY 2021**



# POPIA Overview



## POPIA Highlights

**There's so much conflicting information out there about this new law, and there is so much to know.**

### What is POPIA actually?

Our constitution gives everyone the right to privacy. The Protection of Personal Information Act (POPIA) is the data protection law that gives force to this constitutional right. It gives everyone the right to privacy and the right to have a say in how their Personal Information is used. In effect, it is the law that governs how people may and may not treat others' Personal Information in terms of processing, handling, sharing and storing this information.

### POPIA is effective from 1 July 2021

The Act was promulgated into law on 1 July 2020, but it allowed for a one-year grace period to allow companies to adapt their practices.

### POPIA applies to you

Every business must adapt to the new law. It is not possible for one party to 'sanitise' data so that the data is POPIA-compliant for anyone else who touches it. The compliant part applies to the company, not to the data. For example, if you receive data from a company that is POPIA-compliant it simply means that they have processed the data in line with POPIA while they've been handling it. You have an equal responsibility to process the data in line with POPIA while it's in your hands.

### What are your obligations?

POPIA covers two roles – the [Responsible Party](#) and the Operator. The Responsible Party is the party that chooses what data to source and what to do with it – they carry the most responsibility under POPIA. If you collect the contact details of prospective home buyers and sellers, you are the Responsible Party. An [Operator](#) is someone who is executing some instructions regarding the processing of the data, on behalf of the Responsible Party. If you supply your photographer with someone's contact details to set up an appointment to photograph their home, the photographer is your Operator and must not do anything else with those contact details other than what you hired them to do.

### Is there a summary of what I need to know?

There is no 'cheat sheet' for POPIA. You need to read at least [Chapter 3 and Section 69](#). Chapter 3 outlines your obligations for processing data according to the [Eight Conditions for Lawful Processing](#), while Section 69 governs what you may and may not do regarding Direct Marketing (also known as Canvassing to Estate Agents). Also important are [The Six Legal Grounds for Processing Personal Information](#). Each time you handle Personal Information as a Responsible Party you need to ensure that one of these grounds applies.

# POPIA Overview



My business is all about [Direct Marketing](#).

## What do I need to know?

POPIA is not the only law that governs Direct Marketing – the Consumer Protection Act (CPA) covers some elements of it too.

[POPIA's Section 69](#) speaks specifically to Direct Marketing via electronic communications. Electronic communications is defined in POPIA as 'any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient'. We believe this doesn't cover making human-to-human phone calls.

Most important here is how you contact current, previous and potential clients and then how you store their Personal Information.

Take a look at what we have covered under [Direct Marketing](#) and [The Client Contact Book](#) for some more detailed and useful information.

## Lightstone is here to support you

We know, there's a lot to know! Having done the hard yards ourselves we want to help our Estate Agent clients. In addition to this booklet we have prepared a [Podcast series](#) specifically for Estate Agents explaining some of the things that are most likely to impact you.

## Finally, what happens if I get it wrong?

If you've done something that is non-compliant or contravene's POPIA, the most likely way this would play out is that the Data Subject would complain to the Regulator's Office and they will decide whether to conduct an investigation or not. The Regulator can also choose to investigate on suspicion (not just by report) of non-compliance.

The investigation could result in what's called an Enforcement Notice, which is basically an instruction to stop doing something or to fix the way you're doing it. If you then change your practice in line with the Enforcement Notice, you're good. But if you disobey an Enforcement Notice, the penalty could be up to R10m in fines, or imprisonment of the Information Officer, which is typically the head of the business and the deputies. But more importantly, there will likely be a reputational impact too – nobody wants their name in the news associated with not respecting peoples' right to privacy.

[Read here](#)

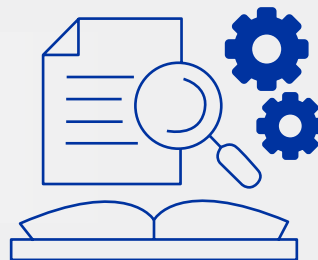
for more detail about the consequences of non-compliance.





# Contents

# Key Role Players



1



## Data Subject

**The person to whom the Personal Information relates to is known as the Data Subject.** An example of this would be a consumer, such as a person buying a house.

2



## Responsible Party

**The Responsible Party is the party that processes the Personal Information.** The Responsible Party determines the purpose for which the Personal Information is needed and whether to outsource a part of or all of the processing of the Personal Information to a third party, who is referred to as an Operator. This role involves a lot of responsibility around the collection, use and care of that data.

**A simple way of identifying the Responsible Party.** If you are the one who decided what data to collect and what to do with it, you are the Responsible Party. For example, you decided to collect contact information from a potential home buyer and to use it to help them find a home. This makes you the Responsible Party for that data.

3



## The Operator

**The Operator is any third party processing the Personal Information on behalf of the Responsible Party.**

When the Operator is contracted to do something on behalf of a Responsible Party, the Operator will only be allowed to execute on the terms of that arrangement, and will not be bound to some of the other conditions of POPIA, which apply to the Responsible Party. In short, the Operator:

- (a) may only process the Personal Information with the knowledge or authorisation of the Responsible Party, and
- (b) must keep that data safe. These are their only obligations.

POPIA requires a Responsible Party to enter into a written contract with the Operator, to ensure that the Operator establishes and maintains the necessary security measures when dealing with Personal Information.



# Key Terms

## Personal Information

This covers a very broad spectrum of information, such as a person's race, gender, age, medical history, employment history, address and various other classes of information. The definition also includes a person's biometric information (eg: fingerprints) as well as private correspondence and opinions of an individual.

Aggregated information or any Personal Information that has been anonymised (or de-identified without the chance of re-identifying it) does not constitute Personal Information under POPIA.

## Processing

Processing refers to the handling of data in any which way, including:

- collection
- storage
- usage
- deletion
- sharing
- changing

## Direct Marketing

When you approach a Data Subject, either in person, via email or another form of electronic communication, for the direct or indirect purpose of:

- a) promoting or offering to supply, in the ordinary course of business, any goods or services
- b) requesting the Data Subject to make a donation of any kind for any reason.

## Unsolicited Direct Marketing

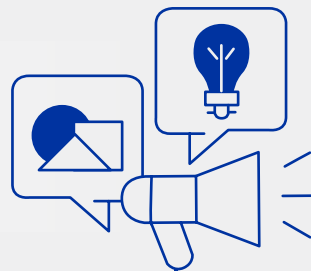
When you contact somebody without them seeking that contact, in order to sell them a product or service, ie marketing your services to that person, who has not asked for those services.

## Electronic Communication

POPIA specifically regulates Direct Marketing by means of electronic communication. This is any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

# Key References

## Eight Conditions for Lawful Processing



1

### Accountability

You must ensure that the other seven conditions are upheld by yourself throughout your entire journey with the data.

#### Ask yourself:



Is / are your Operator/s in a position to handle the data with that same due care?

### Processing Limitation

You must process the Personal Information in a manner that is adequate, relevant and not excessive for the purposes it is being processed.

#### Ask yourself:

Do I have one of the Six Legal Grounds for processing this Personal Information?



#### Safety Checks:

Collect the minimal amount needed for that purpose.  
Make sure any processing you do is in line with the reason you collected it.

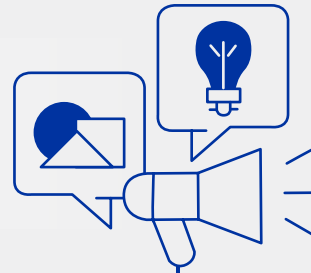


2



# Key References

## Eight Conditions for Lawful Processing



3

### Purpose Specification

You must have a specific and lawful purpose that is related to your function / activities.

#### Ask yourself:

Is the Data Subject aware of my purpose? Check for differences that may apply in the case of public-sourced data, where your Data Subject may not be aware of your purpose.

#### Safety Checks:

Do not retain Personal Information for longer than your purpose requires.

- ✓ Delete the records after your purpose has been completed. (\*read up on exceptions)

### Further Processing Limitation

Anything else done with the data must be compatible with the original purposes of collection.

#### Ask yourself:

Are my intended actions in line with why I originally collected the Personal Information?



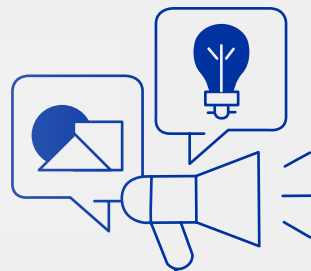
4





# Key References

## Eight Conditions for Lawful Processing



### Information Quality

Make sure the Personal Information you collect is correct.

#### Ask yourself:

**?** Is the Personal Information accurate, complete, not misleading and up-to-date, based on the purpose of collection?

### Openness

Be open and transparent about your processes.

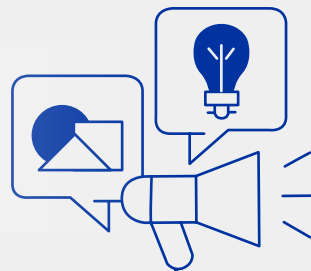
#### Safety Checks:

Keep documentation of all your processing operations.  
 Make these operations available to people through an accessible PAIA manual.  
 Make Data Subjects aware of your processes and purposes (ie the what, who, where, how and why you are collecting their Personal Information.)



# Key References

## Eight Conditions for Lawful Processing



### Security Safeguards

You need to safeguard the integrity and confidentiality of the Personal Information.

#### Ask yourself:



Is this data safe and confidential across the entire processing journey?  
Can anyone who isn't allowed to, see or use this data?

#### Safety Checks:

Proactively identify all the risks, internally and externally.



Put measures in place to protect Personal Information.

Ensure all your contracts with Operators uphold these safety measures.

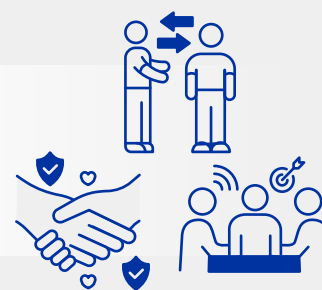
### Data Subject Participation

People have the right to know if you hold their Personal Information and how it is being used or shared.

#### People also have the right to:

Request changes to the Personal Information, if it is incorrect.

Request that the Responsible Party delete their Personal Information (\*read up on the conditions in 24 (1) (a)).



# Key References



What are the laws that govern Processing Limitation?

## The Six Legal Grounds for Processing Personal Information

A Responsible Party may only process Personal Information if:

(1)

The Data Subject consents to the processing.

(2)

Processing complies with an obligation imposed by law on the Responsible Party.

(3)

Processing protects a legitimate interest of the Data Subject.

(4)

Processing is necessary to carry out actions for the conclusion / performance of a contract to which the Data Subject is part (eg: marketing their home to sell).

(5)

Processing is necessary to pursue the legitimate interests of the Responsible Party or of a third party.

(6)

Processing is necessary for the proper performance of a public law duty by a public body.

# Key References



**What are the laws**  
that govern Processing Limitation?

## **In the case of using Lightstone's Valuation Reports, what if I don't have one of those legal grounds?**

**No problem, you can still get the reports, but we will de-identify the homeowner. You will get all the pages of rich content excluding the homeowner's name and ID number. And even though we have removed the Personal Information in the Transfer History section for all reports, you will still know the value and date of each property transaction.**

# Key Questions



## Who can be considered an **existing customer**?

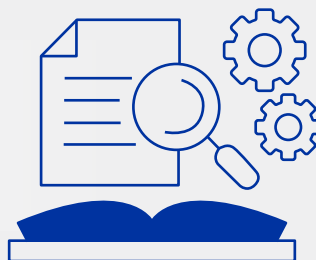
- This is not very clear in POPIA and you will need to seek legal guidance, and make an objective decision yourself on what defines a customer in the context of your business.
- Each company will have to evaluate the databases that it has collected over the years and determine how that company will decide who falls within the category of existing customers.

***Something to debate: If someone bought a house from you eight years ago, are they really still a customer? If you had a contract with them to sell their house but in the end another agency ended up selling it, are they still a customer of yours?***

## How do you get consent “in the prescribed manner and form”?

- [Form 4](#) offers an example of the type of form used to get written consent.
- Make sure the customer understands what they are consenting to by ensuring:
  - ✓ The consent obtained from the customer must be voluntary, specific and informed.
  - ✓ The direct marketing subjects must be specified.
  - ✓ The details of the marketer should be recorded so it's clear who the Data Subject is giving their permission to for purposes of the direct marketing.
  - ✓ The Data Subject should have the right to choose which methods of communication they're happy with and which they don't want.

# The Client Contact Book



## Importance:

Contains private information about current, previous or potential clients, some of whom you have never met or had direct dealings with.

## Types of contacts:

- ✓ People you sold to in the past.
- ✓ People you're engaging with currently around selling or buying a property.
- ✓ Potential home buyers or sellers where no deal was ever finalised.
- ✓ Contact details bought of home owners to contact.

## Impact:

Processing and Direct Marketing

## Key references for this section:

- ✓ Eight Conditions for Lawful Processing
- ✓ Including the Six Legal Grounds for Processing Personal Information

## Who can I contact and when?

### CATEGORY 1:

#### Current or past clients

Clients whom you have engaged with, in the context of a request to find or sell their home. (Even if the deal was not concluded.)

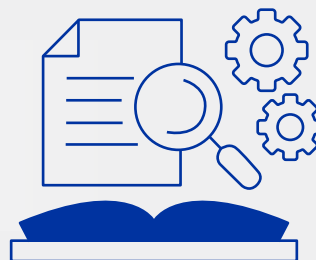
#### You are permitted under POPIA to:

- Contact these clients **about the same thing** you got their details for originally (eg buying or selling a home).
- You are allowed to market that category of services to them indefinitely, but on each electronic communication you must allow them the option to opt-out of the communications, and you must respect their wishes if they opt-out.

POPIA permits these activities for customers but is not prescriptive about the definition of a customer. It is up to each company to take a position on what a customer is, in a way that's objectively rational.

See [KEY QUESTIONS](#) for more on who can be considered an **existing customer**.

# The Client Contact Book



## CATEGORY 2:

### Contact details gained for a specific purpose such as a Show Day

You have their contact details now, but are you allowed to use them?

**In short:** When you collect Personal Information from people, you need to make it clear what the purpose is (what you're going to use the information for) and, in general, get their consent for each purpose you'd like to use the data for. Explain at the top of the register what you require the information for, and then only use it for that purpose. If you'd like to use it for other purposes (eg to phone them in order to try to help them find an appropriate house), you must ask their permission for that purpose on the form. A simple tick box asking consent to contact them for that purpose, will do.

- ✓ Only use the data for the permitted purpose
- ✓ Delete it when that purpose is complete
- ✓ Keep it secure\*

\*Keeping it secure also means not leaving peoples' Personal Information exposed for others to see. So the old-style Show Day registers, with one sheet containing everyone's information, will need to be revised, unless you can ensure you're not exposing Personal Information to other people when they complete the register.

- ✓ **Check in with:** Six Legal Grounds for Processing Personal Information
- ✓ **Follow up:** Eight Conditions for Lawful Processing

## CATEGORY 3:

### Contact details bought or given indirectly

Details obtained from any other source, other than directly from the Data Subject. Most of the time, Estate Agents want to use these contact details to solicit potential listings or to find potential customers.

### Remember, these subjects have NOT given their consent for you to Direct Market to them.

- ✓ You MUST get their consent.
- ✓ You have **ONE opportunity to contact them** (by means of electronic communications) and request **consent for specified direct marketing purposes.**
- ✓ The consent doesn't have to be in a particular format but should contain the substance of [Form 4](#).
- ✓ Some interpretations of POPIA exclude phone calls from falling under electronic communication. In this case, you may still be able to contact them using a phone call.

### BUT ONLY...

- in the prescribed manner and form (refer to Form 4 and Section 69 of POPIA),
- if they have not previously withheld consent.

# Consent



## Consent under POPIA is when:

the Data Subject has given you permission to use their data for the purposes you have outlined to them.

## Importance:

Consent needs to be **voluntary, specific** and **informed**.

## Impact:

Processing and Direct Marketing. When you are processing Personal Information at all, you need to have one of the Six Legal Grounds – consent is **one of** those options. You should select the most appropriate legal grounds for the processing you're doing. In addition – if you wish to Direct Market (using electronic communications) to people who are not your customers, you **must have consent** for that purpose.

## Key terms for this section:

- ✓ Responsible Party
- ✓ Operator

## Key references for this section:

- ✓ Six Legal Grounds for Processing Personal Information
- ✓ Eight Conditions for Lawful Processing
- ✓ Direct Marketing and electronic communication

## Breaking down consent

### Consent must be:

- ✓ **Voluntary**  
The consent must be the **result of a genuine choice**. It can't have been coerced or forced in any way.  
(**No go:** Allowing access to a service only after they give consent to their details being used for purposes outside of that service.)

- ✓ **Specific**  
Consent cannot be general and far-reaching. Consent must be:
  - focused and particular;
  - processed and used in a determined manner.

**In practice:** If someone signs up to receive newsletters from you, and consents to the use of their email address for that **particular purpose**, you cannot use that information to send them information about listings or anything other than the newsletter (unless you also have consent for that purpose).

- ✓ **Informed**  
You must make the Data Subject aware of **how, why and when** you will use their Personal Information. And they must consent to the information being **used in this manner**.

### You also need to inform them:

- of the name and address of the Responsible Party (ie Estate Agent);
- whether you need to share their information with another party;
- that they have a right to access and rectify any Personal Information you hold on them.

Complexity Alert: Please refer to [Section 18](#) of POPIA



# Consent



## When you need consent:

**If someone is already a customer**, you are free to keep using their Personal Information if the purpose is similar to the service you now want to deal with them on, ie based on your existing relationship.

**If someone is not a customer**, you need to get consent to Direct Market to them.

**Top tip:** Consent must always be opt-in and must be clear as to how and when the information will be used for direct marketing purposes.

## How to get consent:

- **Direct Marketing:** See an example of a consent form in [Form 4](#). You don't have to specifically use that form but the information should be similar in essence. What is important is that you have a record of the consent, in case of a dispute later on.
- **Bought contacts pre-POPIA:** You are allowed to contact (electronically) each person on that list only once to establish if they're happy to be contacted in the future or not. If they don't respond or specifically give consent, you may not (electronically) contact them again.

**Top tip:** Make sure you gather consent upfront for all the purposes **you will need** to contact that person for.

### When in doubt, get consent for anything and everything?

## No!

As the Responsible Party some of the other legal grounds could be more appropriate for some of the types of processing. For example, a sole mandate (contract) covers certain uses of Personal Information. But other aspects of POPIA apply, eg you may not collect more Personal Information than you need for your (lawful) purpose in the anticipation that you may want to use it someday.

# Consent



Consent is only one of the **Six Legal Grounds** for processing Personal Information.

See our [Key Reference](#) for all six.

## The two other grounds most applicable to Estate Agents are:

- If you have a contract with them and you need to process their data to fulfil that contract.
- If the handling of their data protects a legitimate interest of the Data Subject, eg if you're trying to secure a refund for them for some reason.

**In practice: is canvassing home owners to see if they want me to sell considered a legitimate interest?** No. Even though some people may want the service, the Data Subject's right to have a say in the use of their data is the most important thing here.

## What about homeowner details obtained from

### Stay on the right side of the law:

1. **Ask yourself:** "Does my action require the use of Personal Information and, if so, am I ensuring that the Data Subject has a say in the use of their own data?"
2. **Make sure you always comply** with the Eight Conditions for Lawful Processing of that Personal Information.
3. **Make sure you have one of the Six Legal Grounds** to process the Personal Information of the Data Subject.

## Lightstone reports?

Lightstone has done extensive work preparing for POPIA. A fair amount of the data we use in our reports comes from public sources – the Deeds Office, CIPC, municipalities, etc. This does not give us (or anyone) the right to use it however we want, but there are some aspects of POPIA that apply differently to publicly-sourced data. We are confident that when we're processing the Personal Information, we're doing it within the law. But when we pass Personal Information on to you, then you become the Responsible Party, and you need to process it within the law too. That means having legal grounds to receive and handle Personal Information.

# Direct Marketing



## Key terms for this section:

- ✓ Direct Marketing
- ✓ Unsolicited Direct Marketing

## Which laws will continue to govern Direct Marketing? Both the **Consumer Protection Act 2008 (CPA)** AND **POPIA** will apply to Direct Marketing:

- ✓ CPA (Consumer Protection Act 2008) applies to **all Direct Marketing**.
- ✓ **POPIA only applies to electronic forms\*** of Direct Marketing.
- ✓ **If mutually inconsistent**, the Act that provides the most protection to the consumer will apply.
- ✓ **The ECTA of 2002 which also governed some aspects of Direct Marketing, falls away** when POPIA comes into effect.

## \*POPIA defines electronic communications as:

- ✓ all text, voice, sound or image messages
- ✓ sent over an electronic communications network
- ✓ either stored in the network or in the recipient's terminal equipment
- ✓ until it is collected by the recipient.

# Direct Marketing



## In practice: can I do unsolicited direct marketing of my own products or services?

Yes, provided you follow the prescribed criteria of POPIA and CPA:

- If they're a customer of yours you can market similar products and services, but you must give them reasonable opportunity to object (free of charge, and without too much formality) to the use of their details (eg provide an opt-out button on all emails).
- If they're not a customer you can electronically contact them once – it would be wise to use that one chance to seek opt-in consent as without that you cannot electronically contact them again.
- Making human-to-human phone calls doesn't appear to be prohibited in POPIA – but CPA still applies, so check whether they're on opt-out lists before calling them; give them reasonable opportunity to object; only contact them during the prescribed hours, and if they ask not to be contacted then respect that.

The prescribed hours are 08:00-20:00 Monday to Friday and 09:00-13:00 on Saturdays

## As a rule:

- ✓ **All processing of Personal Information** by means of **unsolicited electronic communications** for the purposes of Direct Marketing **must comply with POPIA.**
- ✓ **The manner in which you undertake** the Direct Marketing (in any form) must **still comply with all CPA requirements.**

## In practice: Can I still buy Personal Information from companies for Direct Marketing purposes?

Companies selling Personal Information for Direct Marketing purposes must also be compliant with POPIA from 1 July 2021. One of the requirements is that they have legal grounds to sell the information for Direct Marketing purposes. If you're purchasing contact details from a company, first ask what their legal grounds are for processing the information.

# Direct Marketing



Under POPIA, engaging in unsolicited electronic communications is prohibited **unless:**

**The Data Subject is an existing customer of yours, and:**

1. You got their details in the context of a previous sale.
2. The marketing is related to your own (and not another company's) similar products or services to the one you got their details for originally.
3. You gave the Data Subject a reasonable opportunity to object to the use of their details for marketing when you collected the details.
4. Each time you contact them you give them fair opportunity to tell you they don't want to be contacted.

**You get consent from someone who is currently not a customer, but remember:**

- You are only allowed to (electronically) approach each Data Subject **once**.
- And only if they have not previously withheld consent.
- And you must **gain their consent** 'in the prescribed manner and form'.
- You may contact them human-to-human via phone but must still first check that they're not on an opt-out list, and must respect any wishes to not call them again.

**What about a verbal consent?**

POPIA does not say you can't get verbal consent, but if the Data Subject later complains, you will need to prove that they gave consent, ie be able to evidence opt-in consent.

**Get the answers to the following  
KEY QUESTIONS [HERE](#):**

- ✓ Who can be considered an "existing customer"?
- ✓ How do I get consent 'in the prescribed manner and form'?

# What Happens

if you don't get POPIA right?



## Scenario

1

Prohibited Conduct

**Cause: you do something that goes against some aspect of POPIA**

### This would most likely happen because:

**A complaint is made to the Regulator**, eg someone sees a report with their name on it and they complain that they didn't have a say in that. This includes disgruntled employees reporting that some aspect of the business is not compliant.

Or someone has asked the Regulator to make an assessment of whether an instance of processing complies with POPIA.

**In addition** the Regulator can take action on **suspicion of non-compliant (illegal) processing**.

### The Regulator could take the following steps:

- If the Office of the Regulator thinks it warrants attention, they could initiate an investigation.

- They can tell you to suspend an activity while they investigate.
- This could mean a loss of revenue and impact on clients.
- The Regulator can, under certain circumstances do a “dawn raid” in which they have “unfettered” access to your systems, which can be a huge disruption to business.

### Results of the investigation or assessment could lead to an Enforcement Notice, if a change is required:

- You can object, but this becomes a legal process with associated fees and time in court.
- The impact on your brand could be harmful.

A civil action can be instituted against you for damages

# What Happens if you don't get POPIA right?



## Scenario

2

Data gets out or  
could've gotten out

**Cause: someone gets hold of the data who shouldn't have it.**

### This would most likely happen because:

1. Someone gains unauthorised access to your system/products (eg hacker)
2. You send the data out inappropriately, as a result of, for example:
  - Phishing
  - Malice (including disgruntled employees) or self-interest (eg employee selling your data)
  - Accidentally
3. An Operator has an event (as above) and the data is stolen from them. The Responsible Party is still liable because it is their data.

**The Responsible Party** needs to report it to the Regulator and affected parties (Data Subjects).

### Potential repercussions include:

- The Regulator / client investigates, which could be extremely invasive and disruptive to the business.

- With any breach, whether guilty, negligent or simply accidental could result in any one of, or combination of the following consequences:
  - You could receive an investigation and enforcement notice.
  - You could be fined (up to R10m in fines).
  - Someone could go to jail (usually the Information Officer, which is typically the head of the business and the deputies).
  - People may decide your business can't be trusted with their data and avoid engaging you.
  - The brand name may be harmed and securing new business is hard and expensive.
  - Data Subjects could implement civil action and you have to pay damages and costs.
  - You end up spending money on corrective actions.

# Seven Ways to get compliant



1



## Appoint an Information Officer to ensure compliance with POPIA

- Who:** We suggest this person must have an in-depth knowledge of the Act and also hold a senior position in the business.
- Why:** The Information Officer is ultimately responsible and accountable for the company's ongoing compliance, and is personally liable if the company contravenes an instruction from the Regulator.
- When:** According to the Information Regulator, registration of Information Officers started on 1 May 2021, and it will be an ongoing process where you can update details from time to time. Due to technical issues on the registration site, the Regulator has issued guidance that those who have not registered Information Offices by 1 July will not be penalized.

2



## Carry out an audit of how your business handles Personal Information

- Why:** To determine the vulnerabilities and changes you need to make to be compliant.
- What:** Consider the current sources like storage, protection and the destruction of information that you hold. Also consider the type of information you hold and the purpose of holding the information. Do you outsource any functions in your business? If so, do service providers hold any of your clients' information? You will also need to have POPIA compliance agreements with service providers.

3



## Do an IT stress test

- What:** Make sure your IT systems have the necessary protective measures in place to avoid access to your information by outsiders.
- How:** Ensure all your devices are password protected and where possible implement two-factor authentication. We suggest that you check with an IT specialist to confirm that the measures you have in place are reasonable.
- Why:** POPIA requires that you put *reasonably practicable measures* in place. Provided your solution is reasonable in the circumstances and you are not reckless with the Personal Information you hold, you should be compliant.



# Seven Ways to get compliant



4



## Prepare your customer databases

**What:** Split your databases into two: one for customers and one for non customers.

**Why:** Because you need to treat them differently from a contact and marketing perspective.

5



## Ensure your marketing practices are POPIA compliant

**What:** As a Responsible Party you cannot hold more information than is required for the function you are undertaking.

**Example:** To conclude a sale you do not require information about the client's hobbies, although it might be important information for future marketing purposes. In this case, we recommend you obtain the client's consent to request additional information for marketing purposes. Your client will need to explicitly agree for you to hold the information and for you to contact them in the future.

**Why:** Consent is an important aspect of managing your POPIA compliance. You are not allowed a blanket consent clause at the bottom of your mandate or bond application covering all marketing aspects. The consent must be specific, eg: 'you can contact me every year on my birthday or add me to your database for your newsletter'. You must also bring the client's attention to the clause by asking them to initial it.

6



## Be careful when dealing with special Personal Information

**What:** Bank account details, medical history, and political affiliations.

**Why:** There are serious sanctions in the Act for not being extra careful with such information.

7



## Engage with a specialist to assist you with POPIA compliance

**Why:** Getting help to update your policies and practices would be a step in the right direction to avoid any legal action being taken against you.



For any further information please contact:

Linda Reid: [lindar@lightstone.co.za](mailto:lindar@lightstone.co.za)

Esteani Marx: [esteanim@lightstone.co.za](mailto:esteanim@lightstone.co.za)

Lightstone Support:

[support@lightstone.co.za](mailto:support@lightstone.co.za)

## Disclaimer

**Please note:** This content has been created to help you unpack POPIA and its practical implications, but may not in any way be construed as legal advice from Lightstone (Pty) Ltd or its directors, employees, agents or other representatives (“Lightstone”). The views set out herein are simply Lightstone’s interpretation of a number of topics related to POPIA and Lightstone does not warrant the correctness, completeness or accuracy of the information set out herein. Please do not rely on this information and seek formal, professional legal advice in relation to POPIA. Lightstone shall not have any liability for any reliance on this information by you or any other third party.