



POPI Act: A layman's guide

Description

Summarizing the [POPI Act](#) is always going to be tough, but with the unenviable task of being a business consultant, I have to try. It's a very complex and broad law, and as such has different implications for different industries. Still, we are going to try and give you a brief guide with examples where possible.

Please note that is not meant to be a legal article, document, or legal advice. It is merely meant to be a guide to assist many information officers to get their organisations POPI Act compliant. Should you find yourself in breach, the services of a legal professional may be more helpful.

[What Is The POPI Act?](#)

[Who Is The POPI Act For?](#)

[What Is Personal Information?](#)

[Lawfully Processing Information Under POPI Act](#)

[The Rights Of Your Data Subjects](#)

[Exceptions From The POPI Act](#)

[The POPI Act, Your Marketing And Your Business](#)

[Marketing Under The POPI Act](#)

[The POPI Act And Automated Decisions](#)

[Consequences](#)

Conclusion

What Is The POPI Act?

The POPI Act is aimed at giving persons, natural or juristic, a legal avenue to protect the processing of their personal information. The term “processing” is broad but generally refers to the acquisition, storage, modification, and usage of that information at a later time. The POPI Act seeks to establish a legal basis for finding a balance between an individual’s right to privacy and the right to access information.

What this means is that the act establishes boundaries for those who wish to process personal information for any purpose. More importantly, it seeks to do this without completely impeding their ability to do so where this processing of information may be necessary.

Additionally, the Act gives legal remedy to owners of information where these boundaries are crossed. In so doing, the law looks to balance the rights of personal information holders and those who need to use this information.

Under this act, organisations need to establish an information officer responsible for the promotion and enforcement of the Act. This, in a nutshell, is the point of contact responsible for the information processor’s compliance with voluntary and compulsory measures outlined in the Act.

Who Is The POPI Act For?

The POPI Act applies to individuals or organisations in possession of personal information. This information may have been added to the holder’s database internally- for example by a cashier at a till.

Alternatively, the information may have been collected via an automated system during a transaction, for example, eCommerce store checkouts. This information needs to go on to form part of a record for the POPI Act to apply.

Should you process this information as a once-off occurrence, then the Act does not extend to you. Furthermore, for international parties, the law does not apply if information processed by an automated system went on to be a record outside the country.

For this reason, both local and international parties may be subject to the POPI Act. Perhaps more importantly, the Act is not meant to overhaul any other Acts set to govern the processing of personal information.

What Is Personal Information?

Personal information, or personally identifying information is any information that can be related to an individual. This means any non-aggregated data that could be used to identify one person from another.

Person in this instance refers to natural or juristic persons. It encompasses a number of things but includes:

- **Contact Information** – telephone number, email address etc.
- **Private Correspondence** – text chains, emails
- **Biometric Information** – blood group etc.
- **Demographic Information** – age, gender, race, date of birth, ethnicity etc.
- **History** – employment, financial information, medical history, criminal history as well as educational history

Lawfully Processing Information Under POPI Act

The POPI Act sets out some [important conditions](#) for the lawful processing of information. These include Accountability, Processing Limitation, Purpose Specification, Further Processing Limitation, Information Quality, Openness, Security Safeguards, and Data subject participation. What each of these entails is:

Accountability – The processing party has the responsibility of ensuring that the conditions for the lawful processing of information are observed during the processing of said information. Basically, adherence to the provisions of the Act is necessary for the lawful processing of information.

Processing Limitation – This refers mainly to the extent of processing and collection of personal information. On the former, personal information cannot be processed in a manner that infringes the right of the data owner. Additionally, said processing cannot go against any other laws that govern the processing of information.

On the latter, personal information needs to be volunteered by the information owner for lawful processing. The information can also be a public record that was volunteered by the information

owner to the public domain. Third-party information sources can also be used for collection if this would not infringe on the data owners' rights. Alternatively, the right to process this information could be given after the fact.

Purpose Specification Personal information must be used for the purpose it was collected for. It's also necessary to inform the data owner of the purposes for which personal information is being collected so they may consent to this use. Additionally, the law prohibits the storage of personal information beyond the period agreed upon by the data owner. This extends to periods beyond those stated when the data owner was being notified of the use case for the personal information.

Further Processing Limitation The POPI Act allows for the further processing of personal information to that in point 2. This is possible where further processing has an established relationship to the processing for which the information was collected. It's also permissible if the data owner gives permission or if the information was volunteered to the public domain.

Information Quality As a data processor, you have a responsibility in ensuring the accuracy of the information you collect. This is to ensure it meets the purposes of its collection. Furthermore, this ensures that the results of the purposes of collection do not cause harm, especially to the data owner. The POPI Act requires you to collect information that is complete, accurate, not misleading and up to date.

Openness Though seemingly obvious, this element gets overlooked by many data processors. You need to document your information processing protocols and be open about them where required. You need to make sure to communicate the information you are collecting and where you are collecting it from. This includes disclosing the purpose of the data collection, as well as your details as the data collector.

Security Safeguards Security breaches have become a daily threat in today's landscape, with dire consequences for data owners. The POPI Act sets out to establish a framework for the protection of personal information.

You need to make efforts to ensure the security and integrity of the data collected. This includes becoming aware of generally accepted security practices in your industry and applying them. In order to make this possible, a 4 step process may be applied:

1. Identify potential threats to personal information in your possession
2. Put in place measures to guard against these threats
3. Consistently ensure that you observe these safeguards

4. Adapt your security measures in line with newly identified threats or potential weaknesses in the system

Data Subject Participation – Owners of information should be given a channel and a right to confirm if you hold their information. Additionally, you should make available means for data owners to get this information destroyed, modified or deleted.

Even subject to the lawful processing of information, you may not process personal information with personally identifying traits that may prejudice a data subject such as religious or philosophical beliefs, race or ethnic origin, political persuasion, or health. Basically, it's safe to stay away from personal information that may lead to personal judgement being passed on a data subject and the consequences they would face.

The Rights Of Your Data Subjects

The POPI Act is mostly aimed at establishing and enforcing your data subjects' rights in addition to ensuring the proper use of personal information. To this end, staying compliant requires knowing these rights.

Over and above all, your data subjects have the right to have their data processed lawfully. Failure to lawfully process data according to established conditions is a breach of their rights. As stated in the previous paragraph, the POPI Act establishes a data subject's right to be informed that personal information is being collected.

Furthermore, this right extends to explicitly stating why this information is being collected. Data subjects can also enquire about what information is held about them and request access to this information. Because personal information belongs to the data holder, they can request to have their information corrected, destroyed or deleted.

Perhaps more importantly, data subjects can rescind their consent to have their personal information processed. They also have the right to institute civil proceedings where they deem their personal information violated.

Where you reasonably believe that a security/ data breach has occurred, you have to inform data subjects of this breach at the earliest possible opportunity.

This requirement takes into account the requirements of reaching the data subject. It also takes into account the time required for the prevention, detection or investigation of offences for the notice to not hamper their activities.

Further information should also be provided to data subjects in the event of a breach. This includes:

1. Perceived consequences of the breach
2. Steps being taken to deal with the breach
3. Advice to data subjects on minimizing the consequences of the breach
4. A point of contact for data subjects to reach out to for further assistance.

Exceptions From The POPI Act

The POPI Act generally does not extend to the activities of non-commercial entities. This means that the activities of individuals in a purely personal capacity are not included. Organisations like, say, NPOs, are still governed by the Act even though they are not strictly commercial.

Furthermore, personal information needs to be personally identifying to be covered by the POPI Act. Where information has been generalised to the point of not identifying individuals, it is not covered. Additional exemptions apply to [law enforcement and public sector entities](#). There are also additional exemptions for [journalistic, literary or artistic expression](#).

The POPI Act, Your Marketing And Your Business

Marketing is perhaps the area that will most interest businesses when it comes to the POPI Act. This takes into account direct marketing activities as they relate to the rights of data holders. These include marketing via calling machines, facsimile machines, SMSs or e-mail, as well as your data collection sources.

All in all, your entire [digital marketing stack](#) will be affected here. Everything from the data you collect for remarketing to the data that is the backbone of your [analytics](#) will need to be compliant.

Your approach to collecting, storing, retaining, and applying data will need to be audited. In some cases it may just be revising your privacy policy and reminding clients they opted into your marketing. In some, your system may need to be overhauled, but as of July 2021 not doing so will have consequences.

Marketing Under The POPI Act

The POPI Act makes compliance easy by making direct marketing by processing personal information illegal except under some exceptions. Most of these exceptions are covered here, most regarding the lawful processing of personal information. Basically, if you adhere to previous passages, you are in the right.

Specifically, your direct marketing activities are allowable if:

- The data owner has given you their consent to market to them via that specific medium, using the necessary personal information (e.g. phone number or email address) and you limit your marketing to what is consented to, and the period agreed upon.
- You are only reaching out to request consent to market to the data owner. You can, for example, send a potential client an email to ask for permission to send future marketing emails. This only applies if such permission was previously not denied.
- The data subject is a client of yours whose personal information was obtained during a transaction of a product or service. Such marketing communication must be for products or services related to the ones involved in the transaction. With each communication, your client must be given an opportunity to object to future communication.
- All your marketing communication explicitly states your details. This includes your identity, as well as your address and a means to request to opt out of marketing communications.

The POPI Act And Automated Decisions

The POPI Act makes a provision to protect individuals from automated decisions that may be derived from processing personal information. This specifically prohibits processing personal information to build a profile that may negatively impact this person, natural or juristic.

The resulting data may include work performance, creditworthiness, reliability, location, health, personal preferences or conduct. You may, for example, have failed to be compliant should you deny a candidate a job based on a location you gleaned from a LinkedIn profile using automated screening machines.

In all cases, your data subject should be afforded an opportunity to represent themselves about the decision made. This, of course, entails making the data subject privy to the underlying process that led to the decision.

Consequences

The POPI Act mentions a number of consequences for failure to comply including fines, penalties and imprisonment. These tend to vary with the severity of the breach, but with prison terms of up to 10 years and fines of up to R50 million in some instances, compliance is your safe bet.

Conclusion

The POPI Act is very broad and meant to establish legislation across many industries and instances of application. As such, it has different implications for different businesses in different industries. Additionally, it has exemptions and exclusions we may not have touched on here.

As a business consultant, with an affinity for small business, we dwelled mostly on factors affecting our primary market. Even then, as a business or small business, we may not have touched on everything you need to know. You are welcome to get in touch with us and let us help you figure out how you can be compliant with the POPI Act.

To re-iterate, this article does not constitute a legal breakdown of the POPI Act. It's just an analysis of some of the business implications from your friendly business consultants over at Mut-Con.

Category

1. Business Insights
2. Business Trends
3. Online Strategy and Presence

Mut-Con blog

Tags

1. Business Insights
2. Business Trends
3. Compliance
4. Data

Date Created

June 22, 2021

Author

mutconco