POPIA FAQ Guide

frequently asked questions about POPIA

Table of Contents

Email: support@michalsons.co.za | Phone: 086 011 1245

Summary

This guide will answer your frequently asked questions (FAQ) about the impact the Protection of Personal Information Act (POPIA) is going to have on your organisation.

In future, everyone in South African has to try to protect the personal information they process. POPIA sets conditions that any person who processes personal information must comply with. POPIA aims to protect the personal information of people (like consumers and employees) so that they do not become victims of things like identity theft,[1] which can have very serious consequences. However, POPIA does not aim to stop the free flow of information. It recognises that there needs to be a balance.

Key points and possible actions

- Be responsible when processing personal information.
- Take practical effective steps to protect it whenever possible.
- You cannot protect all personal information, all the time. But you should try.
- It is very unlikely that anyone will go to jail for unlawfully processing personal information.

[1] http://www.michalsons.co.za/identity-theft-victim/12347

General

What is POPIA?

It is the Protection of Personal Information Act, a law passed by the South African parliament, which sets the conditions that you must follow to lawfully process the personal information about persons.

Why did POPIA come in to existence?

POPIA protects people (like you and me) from harm (both physical and loss of money) by requiring those who process our personal information to protect it. For this reason alone POPIA is important.

The protection of personal information is definitely needed now, more than ever. With the rise of computing power and devices like tablets and smart watches, personal information is at greater risk than ever before. POPIA will enable personal information to be transferred to South Africa, which will bring economic benefits for the country.

Key points and possible actions

- POPIA is not going to change.
- Your processing of personal information only needs to comply with POPIA by the end of the grace period.

What about the protection of state information?

The Protection of State Information Bill (POSI) requires people to protect state information. This is different to personal information. You almost certainly do not process any state information and therefore POSI is not applicable to you and you do not have to comply with POSI. Don't confuse POSI with POPIA – they are different laws.

Does POPIA apply to everybody?

Yes, virtually everybody. POPIA applies to everybody who processes personal information. It applies to all public (like Home Affairs and SARS) and private bodies (like financial institutions, healthcare providers and direct marketers).[2]

Key points and possible actions

- POPIA applies to Government.
- POPIA has a big impact on anybody in the financial services, healthcare or marketing sectors.

Who is exempt from complying with POPIA?

Very few people, but some are. For example, SAPS, Cabinet and journalists who process personal data for journalism.[3] Some processing of personal information is exempt. For example, if you personal information in the course of a purely personal or household activity.[4]

---

[2] POPIA, definition of responsible party.

[3] POPIA, Section 6 and 7.

[4] POPIA, section 6(1)(a).

Email: support@michalsons.co.za | Phone: 086 011 1245

Do you have to comply with POPIA?

Yes, you must comply with POPIA (and the consequences for non-compliance are quite severe), but you also want to do it efficiently and get business value out of those efforts.

Key points and possible actions

- POPIA almost certainly applies to you and you are not exempt. You must comply.
- You should do what is reasonably practicable to protect personal information.
- You cannot protect all personal information all the time.

What could happen if you do not comply?

In terms of section 92 of POPIA '*the Regulator may make public any information relating to the personal information management practices of a responsible party that has been the subject of an assessment under this section if the Regulator considers it in the public interest to do so*.' This could lead to significant reputational damage. Your records management practices may be aired in public.

On the evidentiary front, the non-retention of records that had to be retained by law may lead to negative inferences to be drawn by the courts in subsequent litigation should they not be available as evidence.

There are significant consequences for non-compliance, including:

- Suffer reputational damage.
- Lose customers and fail to attract new ones.
- Pay out millions in damages in a civil class action.[5]
- Be fined up to R10 million or face 10 years in jail for committing an offence.[6]

The reputational damage is probably the biggest risk. There are not many offences in POPIA (for example it is not an offence if you fail to comply with the conditions) and generally speaking you will know when you commit one. It is quite hard to commit an offence, but if you do, the Information Regulator can fine you if it merely alleges you have committed an offence.

What will happen to you, if you recklessly disclose a bank account number?

You could be fined R10 million or jailed for up to 10 years, if you:

- Fail to comply with the conditions when processing account numbers[7]
- Knowingly or recklessly obtain or disclose an account number[8]
- Sell (or offer to sell) an account number[9]

---

[5] POPIA, section 99.

[6] POPIA, section 109.

[7] POPIA, section 105(1).

[8] POPIA, section 106(1).

[9] POPIA, section 106(3) and (4).

Email: support@michalsons.co.za | Phone: 086 011 1245

Key points and possible actions

- Focus on account numbers. It is especially important to secure devices that have account numbers on them or records that have account numbers in them.
- It will be hard for you to commit an offence, but if you do, you will be in trouble.
- It is unlikely that anyone will go to jail.
- If you get fined, seriously consider paying the fine. If you don't, you could get a criminal record, suffer reputational damage, have to pay huge legal fees, risk a Magistrate making an adverse finding against you.

Who is the responsible party?

Whoever decides to process personal information in a certain way, is the responsible party. It is the person that, alone or in conjunction with others, determines the purpose of (why) and means for (how) processing personal information.[10] If you are processing personal information for somebody else, you are their operator and they are the responsible party.

Key points and possible actions

- It is the organisation (and not the employee or user) that is the responsible party.

Who is the operator?

If you are processing personal information for somebody else, you are their operator. If you do not determine the purpose and the means for processing the personal information you are the operator.

Key points and possible actions

- You are the operator, your clients determine the purpose and means for processing, therefore they are the responsible parties.

Does POPIA only relate to consumer data?

No, it relates to all personal information. Almost all consumer data is personal information, but personal information is much broader than just consumer data. For example, personal information includes the personal information of employees.

Does POPIA apply outside of South Africa?

Yes, POPIA does apply outside of South Africa. A responsible party does not need to be domiciled in South Africa for POPIA to apply. If the responsible party uses equipment in the country to process information then POPIA applies to that information.

What is personal information?

It includes information like race, gender, or age or relating to the education of a person. It includes the medical, financial, criminal or employment history of person. And contact details like an email address, telephone number or location information.

It is any information that relates to an identifiable, living, natural person. In other words it is information that identifies a human being. But in some circumstances it can also be information, which identifies an existing juristic person like a company, close corporations or trust.

[10] POPIA, definition of responsible party

POPIA also applies to public (not just private) personal information and the conditions for lawful processing apply.

Key points and possible actions

- Personal information includes a broad category of information.
- Personal information will be amongst all of your records and on all of your devices.
- Information that has been de-identified is not personal information.
- Information about a company can also be personal information.

Whose information must you protect?

It is any information that relates to an identifiable, living, natural person. In other words it is information that identifies a human being. However, in some circumstances it can also be information that identifies an existing juristic person like a company, close corporation or trust.

Key points and possible actions

- Information about a company can also be personal information.
- Companies can be the owners of properties in the vicinity.
- The responsible party must do what is reasonably practicable to protect personal information.

What must be done to protect personal information?

There are different ways to protect personal information. How you protect personal information will depend on what form the information is in and how the personal information is processed.

By protecting personal information you stop third parties from getting information and harming the person (potential buyers and sellers) to whom it relates.

Key points and possible actions

- Store electronic documents on systems that are encrypted.
- Save electronic documents to the cloud.
- Implement procedures within your company to address how the personal information of data subjects is used and who is allowed to use it.
- File physical documents (that contain personal information of your customers) in cabinets that have controlled access and are secure.

When will POPIA come into force? When must you comply by?

The President has signed POPIA in 2013, so it is here to stay. The regulations will not be significant so we know that material we have available is what we need to comply with. The Office of the Information Regulator has been created and consists of Adv Pansy Tlakula as the chair, Adv Cordelia Stroom (PAIA) and Mr Johannes Weapond (POPIA) as full-time members, and Prof Tana Pistorius and Mr Sizwe Snail as part-time members. The Regulator will draft Regulations and will announce a commencement date for

POPIA.[11] You will have a one year grace period after POPIA commences. The best course of action is for responsible parties, and operators if applicable, to take action steps now.

Key points and possible actions

- POPIA is not going to change.
- We recommend your processing of personal information should comply with the conditions in POPIA from the end of 2017.

When am I processing personal information?

You process information when you do anything with personal information. This includes processing using automatic means. For example, you are processing personal information:

- when you collect it,
- when you archive records that include personal information,

Does POPIA apply to paper-based forms or paper documents?

Yes. POPIA applies to all personal information, including information found in paper documents. Personal information in electronic form is also covered by POPIA.

Does POPIA require me to have accurate data?

Yes, the responsible party must take steps that are reasonably practicable to ensure that the information is accurate and complete.

Does POPIA require me to make disclosures?

Yes, you must be open about how you process personal information.[12] You must be able to provide people with a description of the subjects on which you hold records and the categories of records you hold on each subject.[13] You also need to notify the data subject of lots of things when you collect their personal information, including the nature or category of the information you collect from them.[14]

What is de-identified personal information?

Personal information is de-identified when you delete information about the specific data subject and you are then unable to link the information to the data subject. In other words, you cannot identify a specific person from the information you have. POPIA does not apply to de-identified information.[15]

---

[11] The Regulator announced at their media briefing that they hoped the commencement date would be before the end of 2017, but may only be in 2018. **https://www.michalsons.com/blog/progress-information-regulator-media-briefing/25208.**

[12] POPIA, condition 6.

[13] POPIA, section 17 and PAIA section 14 and 51.

[14] POPIA, Section 18(1)(h).

[15] POPIA, definition of “de-identify”.

Email: support@michalsons.co.za | Phone: 086 011 1245

When can I use records for historical, statistical or research purposes?

When the personal information is de-identified and meets the purpose the information was collected for or the law requires you to retain the record.

When is personal information no longer personal information?

De-identified personal information is not personal information.

Personal information of a deceased person is not personal information, as it does not relate to a living natural person.

Does the law now require information security?

Yes, it does. You had been securing the information that you have for a long time already because it made business sense to do so. POPIA now also places a legal obligation on you to secure the information you process. You must secure both the integrity and confidentiality of your personal information by taking appropriate, reasonable technical (like using encryption) and organisational (like policies) measures to prevent loss and unlawful access (a hack).[16]

What is appropriate and reasonable information security?

It depends. The question is what was appropriate and reasonable for you to do considering the type of person information that needs to be protected. What is appropriate and reasonable for some may not be appropriate and reasonable for others. But there are certain things that will be considered appropriate and reasonable measures for most people to take. One of those is to use encryption and policies to secure person information on mobile devices. Mobile devices contain lots of personal information, which is at higher risk considering that mobile devices by their nature move around a lot. You need to secure that information.

Key points and possible actions

- The law requires you to take both technical and organisational measures.
- If you encourage or allow users to use mobile devices, you must take measures to secure them.

Does cost play a role in determining what is reasonable?

Yes it does. To consider whether an organisation took reasonable measures the Information Regulator (or a court) would have to take into account how much money the organisation had available to it to protect its information.

Key points and possible actions

- You must do what is appropriate and reasonable for you.
- The challenge is to take practical effect of action to protect personal information at the lowest cost. And to get business value out of those efforts.

Must you encrypt your personal information?

Yes, because it is a key technical measure for securing data. Encryption is the first line of defence. Encryption is very important and is a key aspect of complying with POPIA.

[16] POPIA, section 19.

Email: support@michalsons.co.za | Phone: 086 011 1245

Can the cloud help me to comply with POPIA?

Yes, it can. If many copies of personal information exist in many different places it is exposed to a greater number of risks. If you can consolidate their personal information into one central location in the cloud and then control the security and access to their personal information, you will be protecting personal information.

Key points and possible actions

- POPIA does not mean you cannot use the cloud.
- Using the cloud can be an effective way of protecting personal information.

Who regulates POPIA? Will it have teeth?

The Information Regulator regulates POPIA (www.informationregulator.co.za). Parliament has gone to great lengths to give this regulator teeth. The Information Regulator can ask an organisation to produce a record to enable the Information Regulator to investigate a complaint (section 81 of POPIA). You need to be able to comply with such a request.

Key points and possible actions

- The Information Regulator has great power in terms of the law.
- We will have to wait to see if it exercises that power.

What laws are linked to POPIA?

There are various other laws that also protect personal information. The key ones are:

1. Consumer Protection Act (CPA)
2. National Credit Act (NCA)
3. Regulation of Interception of Communications Act (RICA)
4. Promotion of Access to Information Act (PAIA)

If there is a conflict between POPIA and another law, POPIA prevails. But if another law gives greater protection to personal information, the other law will prevail. For example, if POPIA says you do not need to get consent to market to someone and another law (like the NCA) says you do, the NCA will apply and you will have to get the persons consent.

There are various other laws, rules, codes or standards that relate to IT.[17]

Key points and possible actions

- Be aware of all laws, rules, codes or standards that relate to IT.

[17] **http://www.michalsons.co.za/it-laws-ict-laws-rules-codes-and-standards-list/3219**

Email: support@michalsons.co.za | Phone: 086 011 1245

About this guide

Copyright

Disclaimers

1. The content is provided for the jurisdiction of **South Africa** and is not suitable for other jurisdictions.

2. We give **no warranty** about it, and none may be implied. We are not responsible for **any mistake** in the information or any direct or indirect loss that may follow from it.

3. The guidance has been prepared by Michalsons and is based on their interpretation of the **principles of South African law at the time of publication**. The law may change due to future legislative enactments and court decisions.

4. It is a summary or opinion on general principles of law and is published for **general guidance purposes only**. The content does not constitute **specific** legal, tax, investment, accountancy or other professional advice.

5. Seek individual advice from a suitably qualified professional adviser before dealing with any specific situation.

Email: support@michalsons.co.za | Phone: 086 011 1245