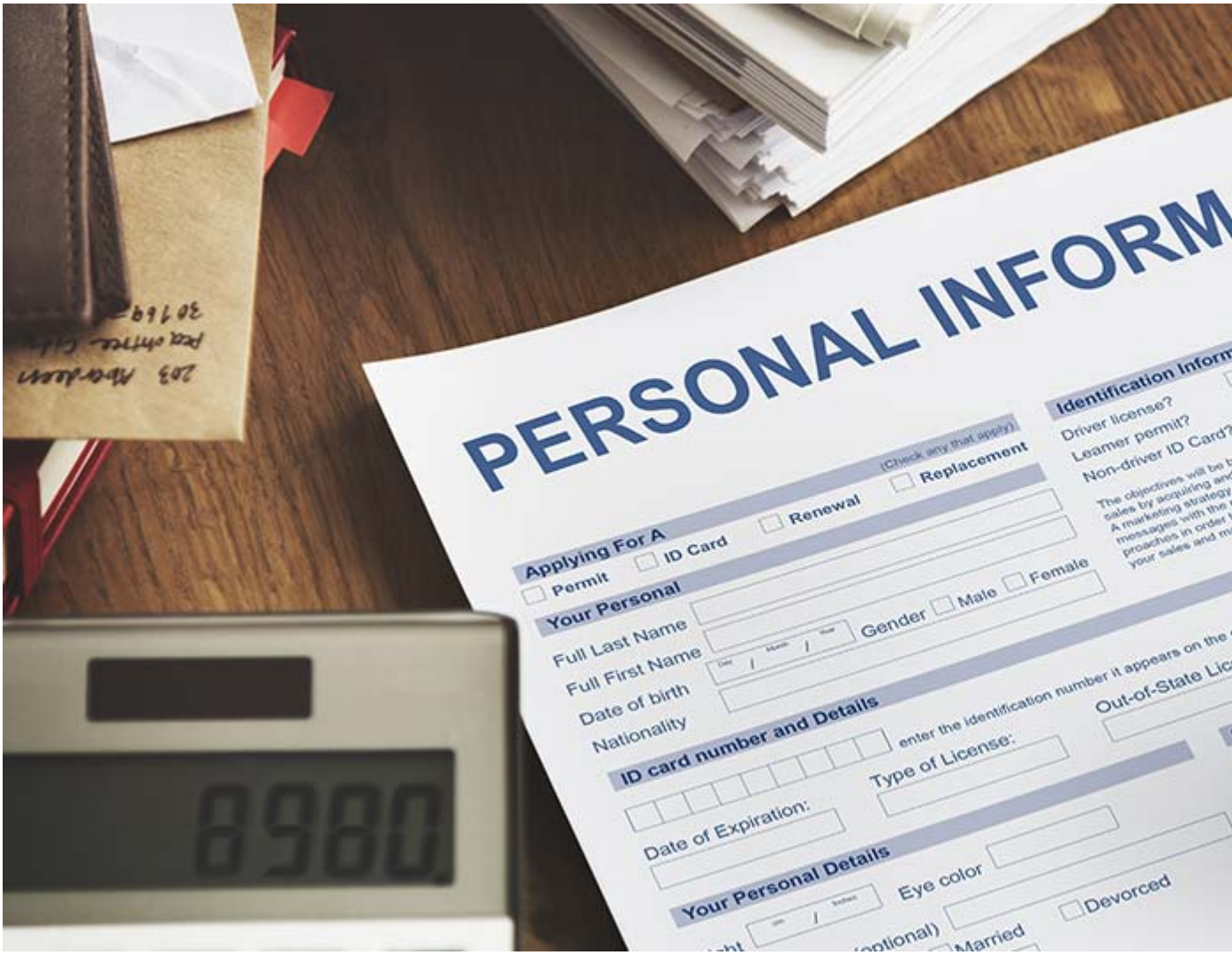
SIMPLE GUIDE TO POPI COMPLIANCE



The Protection of Personal Information – or POPI – Act regulates how organisations handle personal information, whether it's for individuals or other businesses. This includes how the information is stored, processed and shared.

The Protection of Personal Information Act 4 of 2013 (POPI or POPIA) is not a consent driven law. The default position is that you do not need to get someone's consent to process their personal information. But there are some instances when you do need to get the data subject's consent. For example, if you do direct electronic marketing to a prospect or if you are processing the personal information of a child and POPI does not authorise you in another way to process their personal information.

What are the legal requirements for this consent? What form must it take? What is prescribed in the POPIA Regulations?

Consent is closely related to two other important issues – disclosure and signature. The three are often so closely related that you can't actually deal with one without the others. Often consent is obtained electronically and in this context electronic consents, disclosures and signatures become a very important issue.

The legal definition of consent-

POPI defines consent to be
"*any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information*".

This is the measure or test that you must meet, if you need to get consent. The words specific and informed are of particular relevance. They are however open to some interpretation.

Some key points regarding consent and POPI

- A person must have a choice whether to consent or not (it must be voluntary).
- It must relate to a specific purpose (for example, to contact me about insurance products). You must specify your purpose.
- You must notify the data subject of various things as set out in section 18 of POPI.
- You must inform the person sufficiently to enable them to make a decision.
- There must be an expression of will. For example, tick a tick box, or click on a link. This is open to interpretation. Can a box be ticked by default for example. Is deemed or inferred consent OK?
- Another important point is that POPI does not require you to get the consent of the data subject in all instances. There are many other justifications in section 11 that you can rely on to process lawfully. It can be very useful, but it is not the only justification.

Who has to comply with the POPI Act?

Any organisation that obtains, processes, stores or shares personal information is required to comply with the POPI Act.
For example, if your business keeps information about employees and/or customers, it has to comply. In practice, this means very few South African companies are exempt.

What is personal information?

Personal information is any information that may reasonably be used to identify a particular individual.

Some examples of personal information are ID numbers, email addresses, phone numbers and addresses, ages and dates of birth, medical records, criminal records, financial information and employment history.

Photos or video recordings that show individuals – whether in business or social settings – also constitute personal information.

Information that's about individuals but that can't possibly be used to identify them doesn't qualify as personal information. Examples are anonymous survey results and demographic statistics.

Complying with the POPI Act

In line with international privacy legislation, the POPI Act requires that organisations:

- obtain unambiguous consent from individuals before obtaining, storing, processing or sharing their personal information
- collect only personal information that they need for legitimate business purposes
- use personal information only for the purpose for which it was originally collected
- keep personal information only for as long as it's legitimately required
- take reasonable measures to protect the security of individuals' personal information
- provide access to and update or correct individuals' personal information if requested to do so.

If personal information is to be shared with other companies or individuals, whether they are third parties or other legal entities within the same group of companies, these parties must have the same level of security for the protection of this information.

When does POPI come into effect?

Many people want to know what the POPI commencement date (or POPI effective date) will be. It is important because the grace period of one year starts running from the commencement date – the clock starts ticking. You must comply with POPI and the Information Regulator will start enforcing POPI one year after the commencement date.

Which sections have already commenced and what does this mean? When will the rest commence? What should you be doing when?

We are constantly on the lookout for indications of (or the proclamation of) the POPI commencement date (or effective date).

What has already commenced?

Certain sections of the Protection of Personal Information Act (POPIA) have already commenced (under proclamation No. R. 25, 2014), but it is only a few limited sections.

The majority of POPI (especially the sections that create compliance requirements) will only commence on a later date to be proclaimed by the President.

The sections that have commenced are not of great significance. The wheels have started to turn, but not much has changed. This development does not mean that you should go any faster or slower than you are already going. So which sections have already commenced.

- The definitions in section 1 – This section does not create any laws itself, but is necessary for other sections.
- The Information Regulator (Part A of Chapter 5) – Part A deals with the establishment, staffing, powers and meetings of the Information Regulator.

- Regulations (Section 112) – The Minister and the Information Regulator may now make POPIA Regulations.
- Procedure for making regulations (Section 113) – The procedure for making regulations is now in place and POPI Regulations have been finalised.

When is the POPI commencement date or POPI effective date for the rest?
We don't know for sure. Nobody does.
We are waiting for the President to proclaim the date. It will not be before the Information Regulator is operational, which might be in early 2019. Bear in mind that there is a one-year grace period that runs from the commencement date and you only have to comply with POPI at the end of the grace period. So, the POPIA deadline might only be early in 2020. The Information Regulator has published the final POPI Regulations 2018 and the deadline for applications for various executive positions has passed. This all points towards the commencement date being in the first half of 2019. The Information Regulator is an independent body that monitors and enforces the POPI Act, as well as the Promotion of Access to Information Act of 2000.

It will probably commence on a date in the first six months of 2019 and you'll have a 12 month grace period. It will be regulated by a new Information Regulator and your Information Officer is the key person who must ensure compliance.

How does POPI affect your business?

To comply with the Act, businesses must implement proper systems for getting individuals' consent and for deleting or destroying personal information once it's no longer required.

They should add disclaimers to physical and digital forms where applicable, and update their terms and conditions to communicate what information they possess and how it will be used, stored and, if applicable, shared.

Businesses must also ensure that any personal information they collect is adequately protected from data breaches and theft. This may involve updating systems used to collect and store personal information, and implementing new security products and protocols. Ideally, it should also involve training all staff on data protection and privacy requirements.

Non-compliance with POPI can result in a hefty fine and/or imprisonment for up to 12 months.

What does POPI mean when it comes to direct marketing?

This is dealt with in section 69. No direct marketing may be conducted electronically unless the data subject has consented thereto. The marketer may approach the subject only once to obtain consent. Anyone uses electronic direct marketing must disclose the identity of the advertiser and provide the consumer with an opt-out route. The rules of personal information collection apply here as well – any person whose information is sought must be offered the opportunity to consent thereto.
If the data subject feels that his/her rights in terms of the POPI Act have been infringed upon, he/she may approach the IR, who facilitates the implementation of the act.

What if there's a data breach?

If a data breach occurs or personal information is compromised in some way, the responsible organisation is required to inform the affected parties, including the Information Regulator, immediately.

The nature of the breach and steps being taken to rectify the situation must be explained, if possible. A subsequent investigation will determine if all reasonable measures were taken by the business to protect the information.