

POPIA: How can SMME's in SA become POPI compliant?

Issued by [Company Partners](#)

25 Aug 2021

Compliance with [POPIA \(Protection of Personal Information Act\)](#) has had everyone in a flat spin, causing a lot of confusion since the POPI Act came into effect in July 2021.



Kindly note: This article does not constitute legal advice, and it should not be interpreted as such. This is the opinion of Company Partners based on its experience and should be accepted as such. It is recommended that you approach a suitably qualified legal practitioner and/or POPI specialist for assistance with your compliance.

Over the past month, a lot of SME's in South Africa have been in a panic, trying to figure out exactly what is needed to ensure they comply with POPI. This is mostly due to lack of practical guidance provided by government on how a Small Businesses (who cannot afford an expensive POPI Compliance Specialist) should go about getting their compliance in place.

We interviewed Matthew Schoonraad from Company Partners' POPI Division to get some "How-to" tips on POPI Compliance.

What is your background, Matthew?

Mostly commercial and labour law. My colleagues and I have recently shifted our focus to [POPI Compliance](#) – up to date we have assisted over 200 businesses of all sizes to get fully POPI Compliant.

How can I be sure that POPI Compliance is even required for my business?

In the case of most laws, you will rarely find a straight "yes" or "no" answer. In the case of POPI – if your answer is "yes" to the questions below, you need to become POPI Compliant.



1. Do you have a trading business within the borders of South Africa?

2. Does your business have any Personal Information of clients?

Example: Mr Smith is a plumber and sends a quotation to Ms Jones (which contains her cell number; address; email address). He captured Ms Jones personal details in his diary. He entered the information onto an invoice generator to prepare the quote, which he saves on his phone.

So that basically includes 99% of all trading business in South Africa. In legal terms you are seen as a “Responsible Party” - a body who determines the purpose and means of how personal information is processed.

As with any compliance laws, I think most readers are thinking “What is worst that could happen if I do not comply. I have heard some of the ‘consequences’ listed by the Information Regulator to those who do not comply. Can they really make a big deal of it if my business does not comply with POPI?”

Once again, this is one of those “yes/no” answers. I will try and keep it simple and straightforward so that it makes sense.

Simply put, yes, they the [Information Regulator](#) has a lot of powers. Let me list some of the important ones relating to your business: assessing your business in terms of POPI compliance; investigate any complaints it receives in terms of your business and resolving any disputes failing which they can enforce compliance. The Information Regulator can also make rules (i.e., Code of Conduct) for a particular industry. The Information Regulator can even sue you for damages in Civil Court.

Other than the normal powers and functions which most government bodies have, and which sets POPI apart, are fines and imprisonment they can enforce for breaching POPI (in some instances). The Maximum fine they can issue is R10m and/or a 10-year prison sentence. Remember, they are empowered to enforce “either or” which means you can end up receiving the thick part of the stick and sit in jail for 10 years with a R10m fine.

These first few years of the Information Regulators coming to life, will be the most telling. As there should be a large number of complaints made by individuals and companies alike.

Small businesses are warned to avoid so called “POPI specialists” who provide copy and paste POPI Compliance services. If I have a small business with limited budget, what are my options then?

Yes, there are certainly charlatans out there portraying themselves as “Specialists” when it comes to POPI – so businesses must be careful and only get the assistance from the appropriate qualified legal practitioners (amongst others).

Unfortunately, there is no reliant way of becoming POPI Compliant without using your lawyer or a ‘real’ specialist to some degree.

[Click HERE if you’d like an expert, like Matthew, to assist you with your POPI Compliance Now.](#)

POPI Compliance is so expensive though. How will the start-up or general SMME be able to afford the fees of lawyers?

There has been a small amount of qualified legal practitioners, such as me, who have adjusted our normal extensive and expensive POPI Compliance process into a “let’s cover the basics for cheap” process. That would be the best route for start-ups and SMME’s to take, or rather to get you as compliant as reasonably possible.

The alternative is to navigate through the [POPI Act](#) yourself. Then you can fix what you think needs fixing in your company yourself using the free resources out there; and then ask your lawyer to just do a ‘double-check’ and signoff as a third party that you have all your ducks in a row. That should also not break the bank.

Let's assume an SMME takes one of these cheaper routes, it is still an admin-heavy process. How can it be simplified?

As [POPIA Compliance](#) is such a 'new compliance requirement' for business, even some lawyers out there are still misinformed, and this creates a lot of confusion for most business owners. So effectively the process is overcomplicated by many.

We, amongst others who have simplified the service, are focussing on the pure 'basics' which the POPI Act requires you to have in place. To simplify the admin, we divide the service into 3 steps:

1. POPI Audit

We guide you through a small 'POPI Audit' of your Company.

2. Audit Report

Working with the information you have provided; we advise you on the right Policies and Procedures to 'fix'. These POPI Compliance Docs are also offered in different packages ranging from simple to comprehensive, to fit every budget and business.

3. Compliance

Once you have the proof in place you receive a "Certificate of POPI Compliance" which is basically a confirmation from a registered lawyer that you have taken reasonable steps to become POPI Compliant or bringing your company as reasonably close as possible to compliance. Clients must always remember that compliance is an ongoing process.



We package these steps into a package which costs under R4000 to assist you to get POPI compliant. [Click here for more info on our POPI Compliance Certificate service.](#)

Can you give me a breakdown of how each of these steps will practically work?

Sure. As mentioned, if you are a business trading in South Africa who deals with ANY Personal Information, you need POPI. So, this is the approach we take:

Step 1 – POPI Audit. What areas of your business should you get 'under the POPI Act'?

As with many things in life, before you can see what your missing, you need to know what you have. This is where we jump in and conduct what we call a "[POPI Gap Audit](#)" of our clients to determine what they have in place to meet the requirements of POPI and then highlight the shortcomings. We then guide them on closing these shortcomings.

Here are a few basics in most small businesses:

1. What tech do you use? (laptops / cell phones / tablets / desktop TV / PABX etc)
2. Who is the owner of the Tech that you use? (Is it company property / is the staff's own tech etc.)
3. What security measures are in place for the tech? (Anti-virus; passwords; pin codes; calls are recorded etc.)
4. Do you have a website? (Does it have an SSL certificate / the server is managed by a reputable source; secure passwords to access the system etc.)
5. Do you have a business premises? (Is there an alarm; is your office separate; does client information lay around or is

it stored / does the filing cabinet have a lock etc.)

6. Do you employ any staff? (Do they have contracts that mentions privacy and confidential information which must be protected / does the company have a written policy that speaks about POPI / does each staff have access to all the same client information etc.)
7. Do you have subcontracts / suppliers that perform work for you? (Do you have an accountant that accesses client information for the books / do you have a contract with them that covers confidential information etc.)

Step 2 – Audit Report. Now that you know what you have in place, let's break down what are you missing.

You have taken stock of your business and its measures to comply with POPI (even if you didn't know it was applicable). So now you get fix whatever needs fixing. The next question we get a lot is what else do you actually need to be fully compliant? In simple terms it depends on the structure / nature of your business.

However, in general terms you will have to look at putting the following in place (not a closed list) to finalise the POPI Compliance process:

1. Register with the Information Regulator as the Information Officer (i.e. the head of the business) - <https://www.justice.gov.za/inforeg/portal.html>
2. Update all employment contracts with contract provisions relating to POPI (e.g. You hereby consent that we may process your personal information during the course and scope of employment for XYZ reason...).
3. Emails – Put a proper email footer in place which informs the receiver of their obligation.
4. Website – Put a privacy policy on your website that is easy to access which sets out the client's rights and obligations / what you will do with their personal information etc.
5. Website – Make sure you have updated Terms of Use / Terms and Conditions accessible on your website which stipulates how the services will be completed/ how does refunds take place/ who is the Information officer etc.
6. PAIA Manual – Prepare a PAIA manual for your company, which is basically a roadmap of which data you store / how can a third-party access that data etc. (check first if you're exempt of compiling one / if the deadline for implementation has been extended again).
7. Information and Communication Technology – make sure all your ICT has security protocols in place like anti-virus / passwords / limited access by staff etc.
8. Contractors / suppliers – put contracts in place with Third Parties which deal with the sharing of data with third parties / who is responsible for what / what safeguards will they put in place etc.
9. Clients – ensure all clients consent to you processing their personal information / they are aware of their rights relating to their information / they know for what purpose you need the information etc.

Step 3 – Compliance. I'm done now, right?

Basically... Your [POPI compliance](#) has now been setup and you can sleep easy tonight. Unfortunately, it is not a once-off process. You will have to create reminders for yourself to frequently review your compliance and implement some practical steps to safeguard your infrastructure / client personal information. Such as:

1. Updating all computer / cell phone / Wi-Fi routers / email account etc passwords once every 3 months.
2. Make sure passwords are complex (Contains uppercase letters, lowercase letters, numbers, and special characters. It also has no connection to you or your business such as your birthday etc. e.g., "Cartoon-Duck-14-Coffee-Glvs").
3. You purchase and renew effective Anti-Virus software.
4. You look at how you market your services to clients (if your strategy changes your POPI compliance will most likely change);
5. If new staff were employed – is their access limited to information based on their role / do staff have access to information they shouldn't.
6. Is your staff being trained on the basic / refresher training?

Thank you, Matthew, that has been very helpful. Any closing statements?

We hope this was of value and pointed you in a more concrete direction to get your compliance sorted. Remember, POPI compliance is not a “copy-and-paste” job. Each business is different and as such the compliance will differ.

Reach out should you require assistance with your POPI Compliance; our details can be found at <https://ptycompanyregistration.co.za/contact-us/>.

For more, visit: <https://www.bizcommunity.com>