POPIA Without the Panic

The UbuntuGuard Guide to POPIA

What is POPIA and Why Should You Care?

Protection of Personal Information Act, 2013 (POPIA) is a law in South Africa that protects personal data, including names, contact details, health records, and anything else that could identify a person. The law requires that businesses handling this kind of sensitive information do so in a responsible and secure manner. It is essential that any company that collects, stores, or uses the personal data of South African citizens comply with this law. Non-compliance could not only get you fined but also seriously damage your reputation.

Why POPIA Matters for Your Business

POPIA is vital for your business as it fosters customer trust, legal adherence, and superior data management practices. The law essentially states that any kind of personal information must be processed responsibly and in a way that grants the data subject the right to have some say in how their data is handled. In order to foster rather than stifle such rights, POPIA lays out some very clear paths that all of us can and should take.

Common Terms Explained

Here are a few terms you will come across when reading about POPIA. Let us break them down simply:

- Data Subject: This is the person whose information you are collecting. For example, your customer.
- Responsible Party: This is you, the business owner, or the organisation collecting and using the data.
- Operator: This is someone who processes the data on your behalf, like a third-party service provider.
- Personal Information: Any info that can identify a person – like their name, contact details, or even their social media posts.

How to Follow POPIA in Your Business

Here is what to do, step by step, to ensure POPIA compliance. The terminology explained above will help you understand as you read along.

1. Designate a Responsible Individual (Information Officer)

Picture the Information Officer as your enterprise's "privacy protector". This person ensures that all processes related to your data protection work and work well. If you are a smaller enterprise, you might serve as the Information Officer too.

Why it Matters: Let us face it – POPIA compliance is not something most people think or talk about very much. It is kind of like dental floss. You know it is good for you, and that if you do not do it, you are likely to run into trouble. But you do not get a lot of enjoyment out of doing it.

2. Understand What Data You are Collecting

Gather the details of the kind of personal data you collect. This can be names, emails, addresses, or even payment details. Once you know the makings of your data, you can make absolute certain under what presiding authority in pseudonymisation, encryption, or fireproof laws your data is kept.

Special Data: Some types of personal data need extra protection. For example, health details or information about someone's race or religion are considered “special” data under POPIA. You need permission to collect and use this kind of data.

3. Make Sure You Have a Good Reason for Using the Data

Under POPIA, you can only collect and use personal information for a clear and valid reason. This could be to provide a service, fulfil a contract, or get the customer’s consent to use their information for marketing.

Why it matters: Do not collect data you do not need. Only ask for what is necessary to do business.

4. Safeguard the information

You are collecting certain data – now you are ready to keep it under wraps. The main ways of doing it are:

- Keeping your data safe by using things like passwords, encryption (a way of protecting information with codes), and physical security (like locked filing cabinets).
- Only giving your staff access to the data that they need to do their job.

Why it matters: Secure your data, protecting data helps prevent unauthorised access, theft, and breaches. If a breach happens, you must act quickly.

5. Train your staff on How to Handle Personal Data

Make sure your team understands the basics of POPIA. It is not just about having an Information Officer – it is about making sure everyone knows how to handle personal data safely.

Training Tips: Hold regular training sessions for staff, especially for those who deal directly with customers' personal information. The training should cover:

- How to store data securely.
- What to do if there is a data breach.
- The importance of keeping data confidential.

Why it matters: Everyone in your company needs to be aware of how to keep data safe.

6. Have a Clear Plan for Deleting Data When You No Longer Need It

Once you no longer need a customer's information, it should be securely deleted or anonymised (turned into data that can no longer identify someone).

Why it matters: Keeping personal data longer than necessary increases the risk of misuse. Once the data has served its purpose, get rid of it securely.

7. Be Transparent with Your Customers

One of the main principles of POPIA is transparency. When you collect personal data from your customers, let them know exactly why you are collecting it and how you plan to use it. Here is what you need to tell customers:

- Why you need their personal information.
- How long you will keep it.
- How you will protect it.

Why it matters: If customers know their data is being used in a way that is aligned with POPIA, they are more likely to trust your business.

8. Make it Easy for Customers to Access or Correct Their Data

Under POPIA, customers have the right to see the information you have about them and ask you to correct it if it's wrong. Here is what you should do:

- Allow customers to easily request access to their data.
- If a customer requests changes to their information, make sure it is updated.

Why it matters: This is part of respecting your customers' rights. You should also make it easy for them to opt out of marketing communications if they wish.

Wrapping up

Complying with POPIA is achievable and by taking simple steps, you can ensure your business respects customer privacy, avoids fines, and remains compliant. Below are the key actions you can take to align your business with POPIA:

- Understand what POPIA requires. This is simple. You can read the law and its guidelines, or you can have someone who understands compliance read them and summarise them for you.
- Decide who is going to work on your compliance.
- Allocate a budget.
- Determine the key areas where your organisation fails to comply with the law as it currently is written.
- Devise a plan to fix these things and ensure compliance.
- Implement the plan.
- Monitor your compliance.

By following these steps, your business will be well-positioned to achieve POPIA compliance, ensuring data protection, legal adherence, and continued trust with your customers.