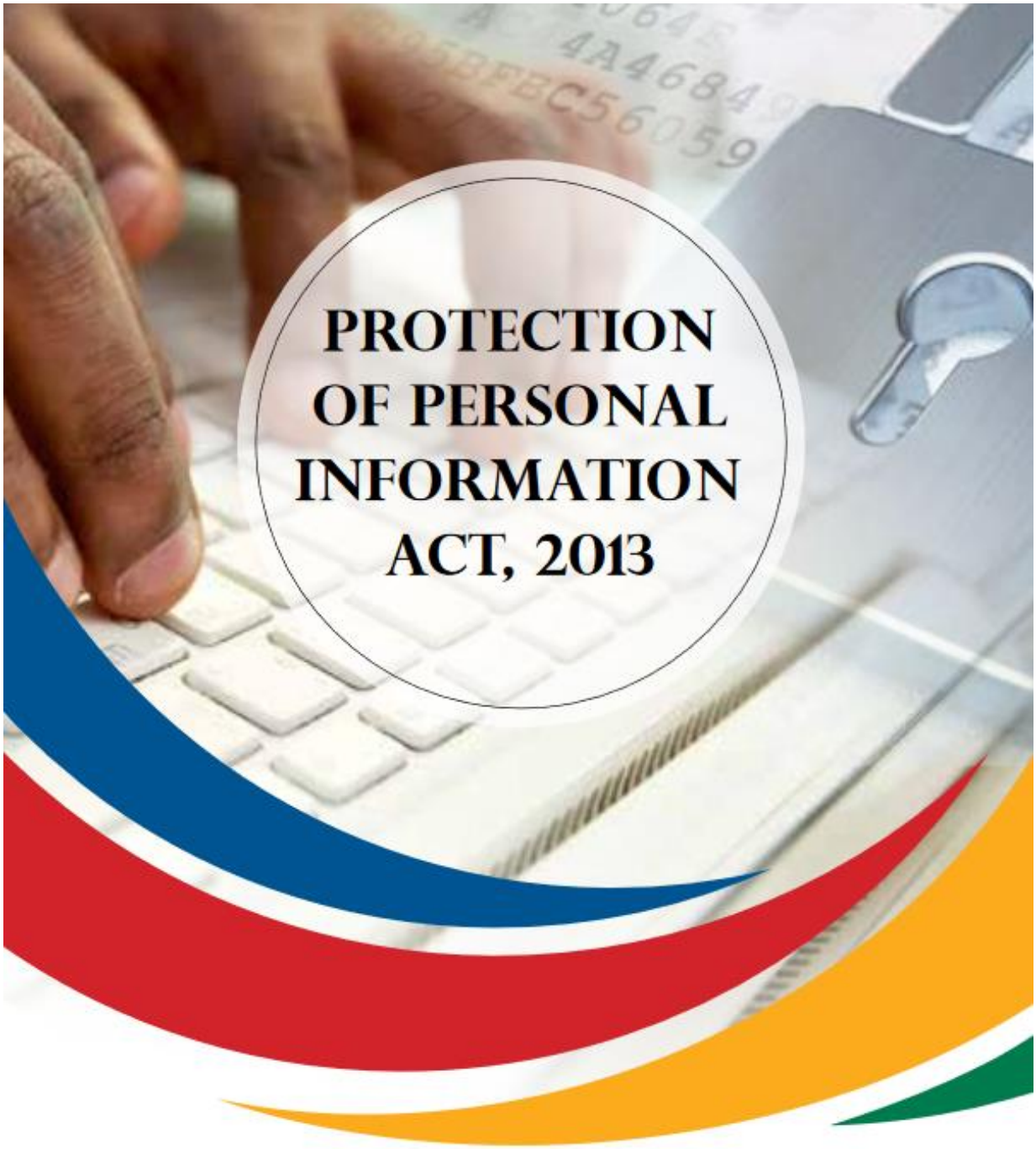

PROTECTION OF PERSONAL INFORMATION ACT, 2013

INFORMATION REGULATOR (SOUTH AFRICA)

POPI

By **Jean-Pierre Murray-Kline for websitedesign.co.za**

- Do you have permission by every person on all your databases to have their data?
- Do you have an understanding of the legal obligations imposed upon a business by POPI?
- Are you planning a personal data information audit anytime soon?
- Have you appointed an Information Officer within your business?
- Have you started preparations to facilitate Data Subject Rights?
- Have you set up digital information security measures?
- Are you preparing to tweak your direct marketing practices?
- Have you created a Privacy Policy?

If you answered '**no**' to even one of these questions then this article will be of value and hopefully help you avoid getting into trouble.

Introduction.

'POPI' stands for South Africa's *Protection of Personal Information Act* and it is a comprehensive bit of legislation that focuses on data protection and overseeing the way we process people's data. This law is a work in progress.

World-wide, legislation is being rolled out to ensure information in the digital universe is better managed. In South Africa we have the Constitutional right to privacy and the POPI Act is the vehicle to deliver this right. Each of us are meant to benefit from this Act which offers us some control over those who use our information.

Even though POPI is law, it still has its training wheels on, therefore we can expect teething pains as we come to grips with what is required of us. Big businesses are going to have to improve many of their systems and call on the experts in the fields of privacy, legal, data and even cyber security to ensure compliance.

Married with the POPI Act is a Code of Conduct, issued and managed by the 'Regulator'. It is an equally important document. Here is a helpful link to see the draft document, I am yet to find a final published version.

https://www.justice.gov.za/inforeg/docs/InfoRegSA-CodesOfConduct-Draft-20191021.pdf

I can assist with digital audits, planning and implementation of POPI. If I feel there is substantial risk for a client I can call on my extended legal network to offer extra scrutiny.

POPI explained.

Our personal data on file and in context of POPI is called a ***Data Subject***. If a business has information about you, they hold a Data Subject. Any local or foreign organisation doing business in South Africa and in possession of a Data Subject, are subject to regulations of POPI. Everyone has until July 2021 to make sure they have their T's crossed and I's dotted.

If you are familiar with the *General Data Protection Regulation* (international standard) you will come to terms with POPI far quicker.

POPI will be regulated by the Information Regulator of South Africa (https://www.justice.gov.za/inforeg/about.html), who will also be the authority dealing with complaints, resolution process, enforcements and other nasty things like warrants. When dealing with personal information from this point onwards we need to think in three 'time periods' of data lifespan:

1. Information / data **collection**,
2. Information / data **use**,
3. Information / data **discarding / deletion**.

Each phase name gives us a very good idea already on what logical processes are at play. Let's unpack some practical concepts of this new 'mind-set' we need to adopt, and please bear in mind, I have written this article through *the looking glass of a business*, and therefore if you run a public office, or some other type of entity, this document will be void of special points for you. Of course, you are always welcome to contact me for information specific to your type of organization.

'Personal Information' can be any identifiable information linked to a person (natural or juristic) or entity (sole proprietor, PTY, CC, NPO, NGO, etc) that includes data information such as, but not limited to:

- E-mail addresses,
- Phone numbers,
- Physical or postal addresses, geo locations,
- Information on a person's physical details, such as disability,
- Someone's employment history,
- A personal opinion or view, (therefore no gossiping!)
- Information on age or language,
- A persons date of birth,
- An ID or passport number,
- A persons history, (general, employment, etc)
- Financial information and history,
- Information on a person's education,
- Social media information,

There is a second category of information treated differently, and certainly requires more care with many other processing conditions. This data is called ***Special Personal Information***, covering, but not limited to:

- Religious & philosophical beliefs,
- Race or ethnic details,
- Trade union membership,
- Political persuasion,
- Health or sex life details,
- Biometric information,
- Criminal history.

I believe a person's image, voice, or video could be protected as an identifying data point.

Any of these nuggets of info can form part of a Data Subject and any abuse can perhaps one day lead to Administrative fines of up to 10 million rand or a prison sentence up to 10 years, or both!

Remember a Minors rights need to include participation from a legal guardian.

A **'Privacy Policy'** is something that should be accessible on all digital communications and platforms. It is imperative you are able to prove this access was offered should something go wrong. Take steps now to create an easy to read and understandable + public-facing document that tells your customers (or anyone else) how you process personal information. The Privacy Policy requirements under the POPI Act are extensive, but here are some examples of information I feel are important for you to include:

- The benefits of providing information and usage within your organization,
- The name and contact details of your organization,
- The sources you use to obtain information,
- The nature of the information you collect, and how (voluntary or mandatory)
- The use / purpose of information,
- What will happen if people don't participate in providing information,
- If the information will be shared with third parties or not, and if so, with whom and for what purpose,
- Information on Data Subject Rights**:** ability to access / correct information and how to opt out.

Our leaders (Government) should set an example, but I can't find a Privacy Policy on their site specific to this Act. I have found a good *Terms and Conditions* page which I suppose they could argue includes their Privacy Policy as well as terms of use. They also had an Opt out of Google Analytics link which when I clicked on it didn't appear to do anything. Take a look at this link and attempt to match information or better it: https://www.justice.gov.za/inforeg/terms.html

Click here to opt-out of Google Analytics

You need to have both a **Usage Policy** and a **Privacy Policy** in place. If you require help in policy creation, I can assist.

The POPI Act mentions three **Data Subject Rights**:

- **Access,**
- **Correction**,
- **Deletion**.

These rights are afforded under certain circumstances. It is very important that your team do not infringe on these rights and if a person requests access to their personal information, and are able to provide proof of their identity, you will have to attend to their request. You must, for free, confirm if you have a Data Subject file on the person.

You can in certain circumstances charge for preparing a report and information pack to hand over to the Data Subject if they make a request. When attending to this sort of matter, you will need to ensure you respond in a reasonable period of time and manner. You may quote for this administrative task to be done and ask for a deposit.

A person can after reviewing the information you provided, request for information to be amended if it is found that the data is:

- Obtained unlawfully,
- Irrelevant,
- Inaccurate,
- Out of date,
- Excessive,
- Incomplete,
- Misleading.

In some circumstances, refusal to make changes can be made, but then a number of other processes need to be followed. Offer written confirmation once an amendment has been completed.

What **'Activities'** constitute processing of data?

Today, there are many automated systems in place which gather information without any human participation. For example, cookies on a web browser or Google analytics. Information is gathered and digitally sent all over the place without most business owners having the foggiest idea on the technical processes at play. You will need to learn how your organization gathers information because you cannot plead ignorance as a form of defence should something go wrong.

Take a look at your web forms, storefront purchasing systems, and benefit systems at tills, chatbots and Facebook Messenger. The way we obtain information is just one of the activities a Data Subject is involved with, let me elaborate:

- Point of **arrival**. EG: Arriving on your website. Attention is required even at the start.
- Point of information **gathering**. EG: a company WhatsApp asking for an email address. You need to get across your usage and privacy policy before you can save information.
- Point of **storage**. EG: An excel document. Is it protected?
- Point of **sharing**. EG: forwarding an excel document. Does the recipient have limited **access** and do they support your policy?
- Point of **reuse**. EG: taking email address from excel document and adding it to an remailer for a newsletter. Does this 3rd party protect your data? Did your Data Subject know about this 3rd party and consent?
- Point of **disposal**. EG: person asking to be unsubscribed and then making sure it's removed from database.

Be '**proactive**' and insist that internal policies are created and shared with staff and suppliers. No defence will be considered if you have not taken all reasonable measures. There are two sides to the *proactive coin*: one is **precautionary** / preparatory steps, and the other is **responsive** / reactive **steps**.

Regular training of staff and ensuring policy is in their employment contracts is a very good idea. Failure to do this could be argued as negligence.

'Actual compliance'. Each business is different, and that is why a 2nd opinion such as a digital audit helps put minds at ease. Here are some absolute essential actions you should take as well as some additional tips of my own.

All entities, public or private, need to designate an **Information Officer**. This portfolio should be added to their contract and duties should include:

- Learning the POPI Act,
- Enforcing and overseeing compliance of POPI,
- Learning the most current Code of Conduct from the Regulator, and mimic points in the company policy,

- Communicating with your team on policy and procedures,
- Attending to client, supplier and own staff Data Subject Rights,
- Working with the Information Regulator when required,
- Preparing a Preparatory Plan (precautions) and a Response Plan (disaster).
- Keeping a record of assessments, workshops, plans and actions taken. Keep records for at least 3 years.

The Information Officer should adopt an ethos which could include:

***Accountability*.** Information is privileged. Show respect for a person's data and you will almost certainly be compliant with the POPI Act.

Be ***unambiguous***. In decisions and actions. Obtaining excessive information is not legally justifiable and the same goes if you use it for reasons other than stated, for example: if you did not ask permission to share with third parties, don't. Do what you say you are going to do, nothing more, and nothing less.

Stick to ***limits***. This goes for collecting of information and also for storing data for excessive periods of time, or after the purpose for collection has been concluded.

Strive for ***quality***. Pride and cherish the data you have on file. It is of extreme value to your company and also the person you have obtained it from. Look at it as someone has asked you to take care of their pet for a period of time. If you do, your data will be accurate and of a high quality.

Ensure ***transparency***. The way you conduct your data activities must be *glass window clear*. Always have a door open to a person so they can engage with you with any aspect of their Data Subject.

Future '**Marketing**'. The POPI Act expands on existing marketing legislation such as the Consumer Protection Act for privacy law. We need to focus on Chapter 8 of the POPI Act which has pertinent points that can help us ensure our marketing activities are permissible. In short, if a person:

- gives consent**,** or
- are already an existing customer,

- + they are offered the option to opt out of future marketing communications.

… you are on the right path.

It is important to understand 'consent' in context of POPI Act. It is defined as a "*voluntary, specific and informed expression of will*" and this needs a bit of elaboration:

> Voluntary means someone must "opt-in" to future communication. They cannot be assumed to have given consent. This prevents the use of pre-checked boxes with statements like "*yes, subscribe me*."
>
> It is safer that direct marketing consent be made separately to other forms of requests.

You don't need consent to send direct marketing to an existing client if you can prove:

- You received their contact details, direct from that person, in context of making a sale. In other words that person made contact because they were interested in a service and therefore you are responding to their request in which they provided their contact information.
- Or you are offering something relevant or similar to a service they've already bought or requested in the past.

An extra nugget: You may not automatically be allowed to use Data Subject information to request a donation.

'Lawful' A business, you can no longer just cut and paste Data Subject information from a website, save it and use it. The excuse of "I got your information off a website, so I added you to my subscribed mail run" is not lawful.

You need to do a self-assessment of absolutely all your data and go back to each person and get their permission.

There are some grey areas. Examples:

- POPI does not apply to certain situations related to journalistic, literary or artistic functions, but this needs to be assessed on merit and you need to consider factors like public interest, the right of privacy and expression.
- Information in certain situations can be collected without consent for historical, statistical or research purposes as long as the Data Subject cannot be identified.
- Sending Data Subject information to an international entity is prohibited, unless certain steps are taken and rules followed.
- Some organizations can obtain and process Data Subject information without express permission being granted, such as a Public Office, Courts and Police.
- In some scenario's, if information is taken from certain public records, or deliberately made public by a person, consent for usage might not be required, but it would depend on factors and the nature of use.
- One section I found very interesting related to 'automatic decision making', for example: a credit rating system, or AI deciding if we get a VISA. I believe we have to consent to this explicit use and we would have the right to demand the criteria used in the decision process.

'Digital security', 19.2 (a) of the POPI Act requires us to identify all reasonable and foreseeable internal and external risks to personal information in our possession or control. Larger organizations should really do a digital security audit and smaller businesses run a workshop. Each organization needs to work through phases of:

- Risk assessment,
- Technical measures,
- Breach processes.

Make sure you have firewalls, passwords, two step authentication, virus software and threat notification systems or processes. One of the greatest risks in digital security is staff or people. The more data staff have access to, the greater the risk. A good check list to work through when dealing with human risks are these questions:

- Do we really need to collect this information?
- Who needs to have access to this information?
- How long should we keep this data?
- How might someone lawfully or illegally access this data?

Less people + less data + less transfer = **less risk.**

Revisit your information flow and look at it through the eyes of a criminal, seek out the loopholes**.** Check hard drives, web servers, cookies and e-mail. Also take a look at information shared outside of your business, like data sent to a marketing company or data provider.

Next, think about the actual data and what can be done to it to further reduce risk.

- Scrambling the entire contents of a set of information known as Encryption
- Scrubbing personal information of all identifiers, referred to as de-identification.
- Swapping out identifying details in a set of personal information called Pseudonymization.

Data breach. The first thing you are meant to do is implement your reactive / disaster plan. Your entire team needs to be ready for this. Every company will suffer a digital attack at some point, be prepared and also remember that digital crime is still crime, and should be reported to SAPS.

Once your reactive / disaster plan is in motion, it is time to inform the Information Regulator of the data breach. If you feel it is necessary, or you are demanded to by the Information Regulator, you can notify the individuals who have been affected by the breach via post, email and phone. You might not need to take this step if it could hamper a criminal investigation. You may need to make a public announcement on your own platforms if the Information Regulator makes such a request.

Digital crime is ever evolving. No data is 100% protected, and that is why I made a point that your business must keep records of assessments, workshops, plans and actions taken. It is essential for your defence. Learn from the breach.

I hope this article was of value, and if you would like to tackle the Act yourself I have added the link below. Otherwise, I would love to hear from you if you are interested in support for POPI compliance or a keynote talk / workshop on the subject.

https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf

www.websitedesign.co.za