POPIA: Advising Clients

Presenter: **Lettie Janse van Vuuren** CA(SA)

11 May 2022

The Protection of Personal Information Act (POPIA)

Webinar: Advising your clients on their POPIA compliance

Presenter

Lettie Janse van Vuuren CA(SA)

- Lettie joined SA Accounting Academy in November 2017 as Head of Technical. She is a Chartered Accountant, Qualified Auditor, Assessor and Moderator.
- She is a **professional trainer and webinar host**, and with her relaxed and humorous presentation style, she is able to hold the attention of an audience. She has a unique ability to communicate with delegates at their respective levels of knowledge and experience. Over the last 20 years, she has trained thousands of partners, managers, trainee accountants and other professionals.
- She is responsible for our MCLU (Monthly Compliance and Legislation Updates).
- She was the Professional Development Manager at SAICA for 4 years and in charge of accrediting new training offices and monitoring existing ones (including the moderation of training offices and trainee assessments).
- Lettie is passionate about improving the efficiency and standardisation at practices. She has extensive experience on a variety of technical and practical topics which she consults on, including: SAICA re-accreditation assistance and preparation, IRBA inspection assistance and preparation, audit file reviews (post-issuance monitoring and EQCR), Quality control implementation, other office-specific manuals, and FASSET skills development facilitation.

WHAT'S ON THE AGENDA?

CONTENTS

- Introduction: Recap on the basics and most NB aspects of the Act
  - Lawful processing of information
  - Information Officer (appointment & responsibilities)
  - Latest updates (from the Information Regulator)
- Consequences of non-compliance
- How you can assist your clients with their POPIA compliance
- How to use our FREE POPIA Compliance checklist
- Guest presentation – Smart Assessment

Abbreviations used

- **PAIA** = the Promotion of Access to Information Act of 2000
- **InfoReg / IR** = the Information Regulator of South Africa
- **POPIA** = the Protection of Personal Information Act of 2013

INTRODUCTION

JUST TO CONFIRM SOME NB PRINCIPLES

What is Personal Information?

What is ”processing data”?

“processing” means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

- POPIA requires me to change my entire business processes
- I found this personal information on a public domain, so I can process it freely
- POPIA only applies to information processed from 1 July 2021
- I will become 100% POPIA compliant
- There is a certification for being POPIA compliant

The Basics of POPIA

Assumed knowledge = definitions, who the role players are, basic POPIA requirements, etc.

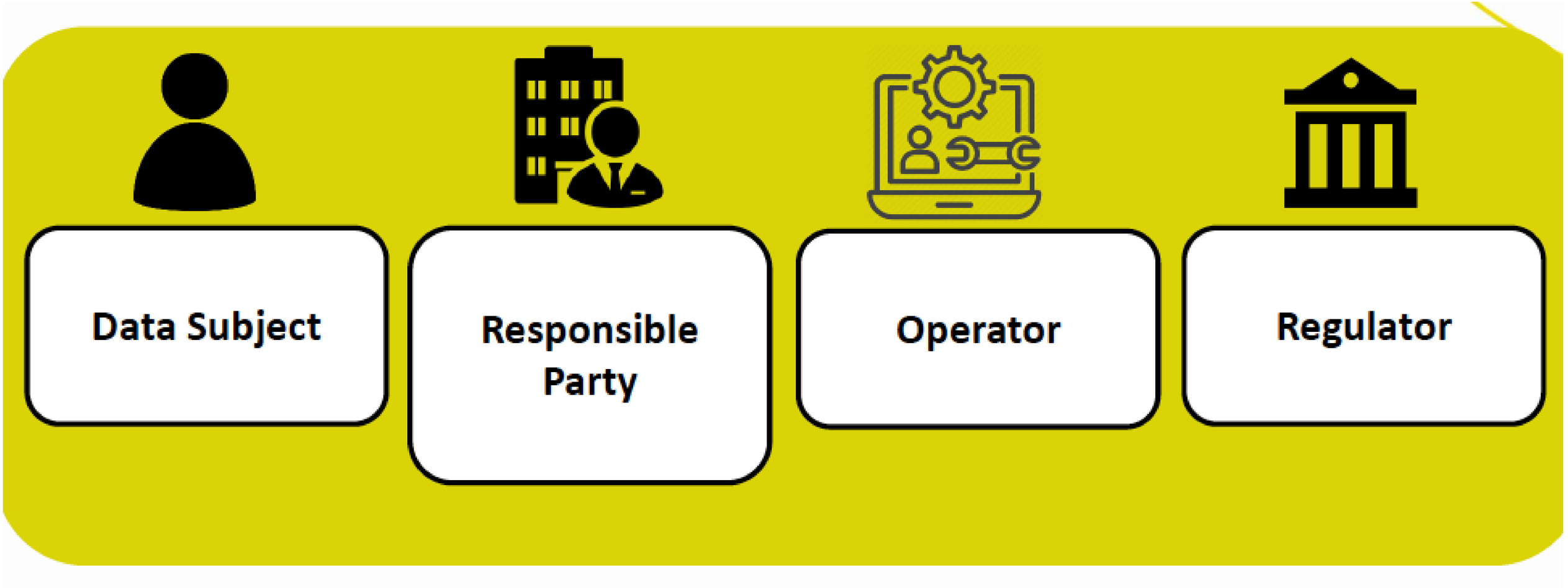
*Refer to **The Basics of POPIA** (Bonus document which is available to you)*

- POPIA requires **all businesses** (including employers) that process personal information, to ensure that the necessary measures are in place to implement, prove and monitor compliance (refer to Exemptions)
- POPIA (Protection of Personal Information Act of 2013), commenced on 1 July 2020
  - Responsible parties were granted a grace period of 12 months, to ensure compliance with POPIA by 30 June 2021
- You must be able to prove compliance from 1 July 2021
  - *Even though this is still not monitored just yet…*

Introduction *(continued)*

- POPIA protects data subjects from theft and discrimination and when breached will impact the responsible parties with heavy fines, imprisonment or both.
- The unlawful and unauthorised use of personal information of individuals is reported to be rising at an alarming rate within the country.
- Cybercrime and identity theft are serious crimes that pose massive threats to individuals who part with their personal information when dealing with various institutions
- *Remember that **NOCLAR** is a reportable matter!*
- POPIA is overseen by the Information Regulator of SA

Who are the key role players?



The Information Officer (IO)

- **Who** is the IO? *Default = highest ranking officer, e.g. Director, CEO*
  - ✓ Must be an employee of the organization (as per new Guidance Note)
  - ✓ Must be **formally appointed** (Appointment process must include training of appointee & should be included in performance management process – should it not be the CEO who is appointed as Information officer)
  - ✓ Must be **in writing**
  - ✓ **Must register with the Information Regulator**
- What are the **responsibilities** of the IO? *Consider POPIA & PAIA*
  - ✓ All parties are required to sign a **written** document of the delegation which includes responsibilities and **penalties for non-compliance** as well as how the role will be **performance managed**

Latest updates from InfoReg SA

- **Information Officer registrations:**
  - The Information Regulator has confirmed that there will be no deadline for registration of Information officers (IO) and Deputy Information Officers (DIO)
  - No responsible party will be held liable for not registering by 30 June 2021. This is due to technical issues faced by the Regulator's registration portal
- **Registration of IO for multiple entities:**
  - The registration of a Chief Executive Officer (CEO) as an Information Officer for multiple legal entities has been taken into consideration and it will be permissible.
  - The registration portal is currently being configured to accommodate these changes.
  - Will be announced when the registration portal = updated

INFORMATION REGULATOR (SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

Compilation of PAIA Manuals

- **All private bodies** WERE **exempted** from **compiling** a Sec 51 manual until **31 December 2021**
- **From 1 January 2022, all Public & Private Bodies must have compiled a PAIA Manual**
  - You do not need to submit the manual to the Information Regulator yet, but you must have one!
  - The manual should be provided to any person who asks for it, including the Information Regulator when required
  - Make it available on your website, if you can
  - Ensure it's accessible at the principal place of business for inspection during normal business hours.

"Private Body" is defined in the PAIA
"company" is defined in the Companies Act

INFORMATION REGULATOR (SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

Some NB detail about PAIA

The Act applies to persons, companies or other types of juristic entities that carry on a trade, business, or profession, including a political party; inclusive of a person providing services from their home or a small business in the form of a sole proprietor, company, close corporation or trust. Therefore, any person carrying on a business as a sole proprietor or in a juristic entity must prepare a PAIA manual. The manual provides guidelines on the processes to be taken when a request for information is made, the associated costs thereof, the type of information that is available, and contact details of the relevant information officers, amongst others.

Additionally, the PAIA manual should integrate the Protection of Personal Information Act by outlining; the purpose for the processing of information; a description of the categories of data subjects and of the information or categories of information relating thereto; the recipients or categories of recipients to whom the personal information may be supplied; planned transborder flows of personal information; and, a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed

Issued by the InfoReg

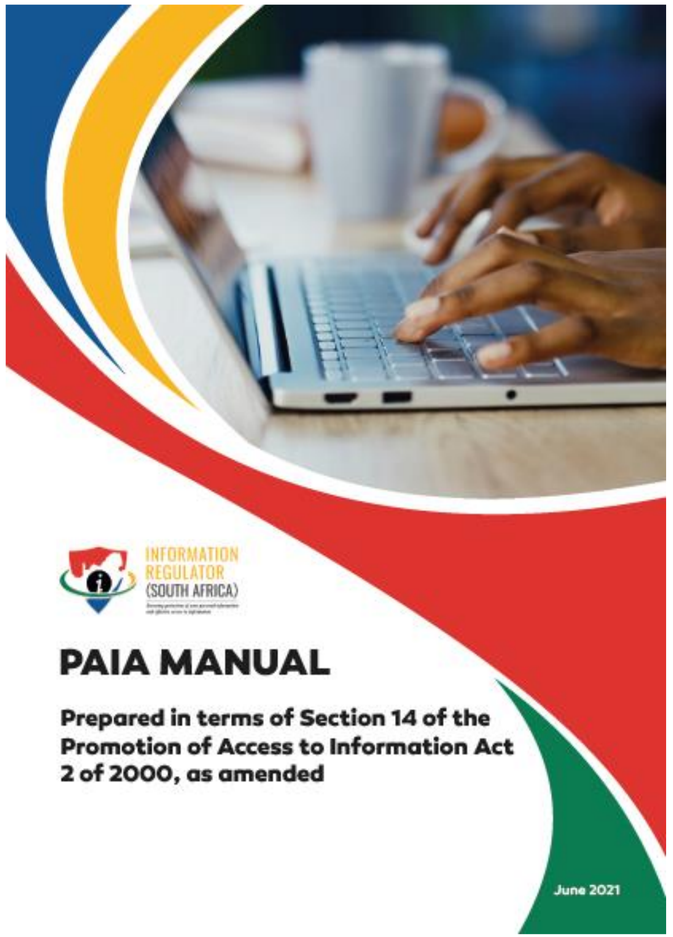
The following was issued by the InfoReg:

- **PAIA Manual**
  - This is the that relates to the InfoReg
- **PAIA Guide**
  - Created for the public to provide guidance on how to get access to information
- **PAIA Manual Templates**
  - Created by the InfoReg for anyone's use

Let's look at each one of these in a little bit more detail…

InfoReg's PAIA Manual

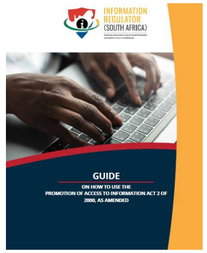
- One of the basic values and principles governing public administration is transparency.
- InfoReg = a Public Body
- This PAIA Manual prepared in terms of Section 14 of the Promotion of Access to Information Act 2 of 2000, as amended
  - *Issued in June 2021*
  - *75 pages*
- The manual is available in English, Sesotho and Afrikaans



Link to download the PAIA Manual in English:

- https://www.justice.gov.za/inforeg/docs/InfoRegSA-PAIA-Manual-2021-Eng.pdf

PAIA Manual: Contents



PAIA Guide

- Published by the InfoReg in *October 2021* in 11 official languages (59 pages)
- The InfoReg's PAIA Manual must be read in conjunction with the Guide on how to use PAIA (to facilitate the public's access to information held by the Regulator)

Purpose

- To provide information that is needed by any person who wishes to exercise any right contemplated in PAIA and POPIA.
- This Guide will specifically assist a person, also called a data subject, on how to access his/her personal information in terms of section 23 of POPIA.
  - https://www.justice.gov.za/inforeg/docs/misc/PAIA-Guide-English_20210905.pdf
  - Access the guide in the other 10 official languages (including, Afrikaans, isiNdebele, isiXhosa, isiZulu, Sepedi, Sesotho, Setswana, Siswati, Tshivenda and Xitsong) on https://www.justice.gov.za/inforeg/docs.html

PAIA Templates available

2 Templates created & available in Word-format:

- **Public Body (Sec14)**
  - https://www.justice.gov.za/inforeg/docs/forms/PAIA-Manual-Template-Public-Body.docx

- **Private Body (Sec51)**
  - https://www.justice.gov.za/inforeg/docs/forms/PAIA-Manual-Template-Private-Body.docx

Remember that the InfoReg confirmed that submissions of PAIA manuals will not have a deadline until further notice

Lawful processing of info

1 Accountability

2 Processing limitation

3 Purpose specification

4 Further processing limitation

5 Information quality

6 Openness

7 Security safeguards

8 Data subject participation

Comply with 8 Conditions

1. **Accountability**: Employers need to ensure that the conditions are complied with at the time of determination of the purpose and meaning of processing and processing itself. Employers can do this by appointing a compliance officer.
2. **Processing limitation**: The processing of personal information must be limited to lawful processing in a reasonable manner that does not infringe the privacy of the employee.
3. **Purpose specification**: When collecting information, it must be for a specific, defined and lawful purpose, related to the function of the employer in the employment context. The employer must inform the applicant or the employee of the purpose of the required documents.
4. **Further processing limitation**: Employers require the consent of the employees to put personal information to further use, e.g. passing on information to a Medical Aid or retirement fund.

8 Conditions in POPIA *(continued)*

5. **Information quality**: An employer must take steps to ensure that the information collected from the employee is complete, accurate and continually updated where necessary.
6. **Openness**: An employer requesting information must ensure that the employee is aware of the information collected, the source of the information, name and address of the responsible party, the purpose for which the information is requested, etc.
7. **Security Safeguards**: An employer must take reasonable steps to ensure that the personal information in its possession remains secure. The employer can do this through considering virus programs, back-ups and off-site storage
8. **Employee participation**: An employee has the right to know what information the employer has pertaining to him/her and may request the records or description of the information the employer holds.

Adequate safeguards

- In terms of section 19 of POPIA
  - Employers are required to guard against reasonably foreseeable risks in respect of non-compliance with POPIA taking measures to ensure that compliance is developed and implemented effectively
- Physical safeguards
- Electronic safeguards:
  - ✓ Understand how data is compromised, how criminals use your data, etc.
  - ✓ Back-ups
  - ✓ Storage of info (local & secure environments)
  - ✓ Electronic data protection tools
  - ✓ Recovery of stolen/destroyed information
- **Breaches:** Should there be reasonable grounds to believe that an employee's information has been accessed, the employer must notify the Information Regulator and the affected employee.

Consequences of Non-Compliance

Consequences of non-compliance

- **Reputational damage**
- **Criminal – Fines & Penalties**
  - Penalties range from R1 million and/or 1 year imprisonment to R10 million and/or 10 years imprisonment – depending on the severity of the offense.
  - Administrative fines of up to R10 million may be imposed by the Regulator on the responsible party – as set out in an infringement notice
- **Civil – paying out damages claims to data subjects**
  - In terms of section 99 of POPIA, a data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of POPIA
- **Effect on Auditor's/Independent Reviewer's Report**
  - The Non-compliance must be reported accordingly by the auditor/independent reviewer!

Possible defenses raised by employer

- ***Section 99(2)*** of the POPI Act sets out the **limited defences** which an employer may raise in response to a claim in terms of section 99(1)
- The defences include vis major, consent of the plaintiff, fault on the part of the plaintiff, **compliance was not reasonably practicable** in the circumstances of the particular case or the Regulator has granted an exemption in terms of section 37.
- Employers must be concerned that the defences do not include circumstances in which the employer is able to show that it did all that was reasonably practicable to ensure that the employee did not breach the POPIA

ADVISING YOUR CLIENTS…

In a nutshell…

What are the 3 main things employers need to do to ensure compliance with POPIA?

1. Employers must appoint an **Information Officer**
2. Employers need to ensure that they **lawfully process information**
3. Employers are required to implement **safeguards** (both technical and organizational, i.e. physical) to secure the integrity and confidentiality of any personal information in their possession or control

Refer to your BASICS OF POPIA Bonus Document for a little bit more detail…

How to advise your clients

- As a small business/practitioner, it is critical to find opportunities – like this – to grow your own practice and provide yet another service to your clients – your biggest asset
- *Your clients need to do Exactly what you need to do i.t.o. POPIA Compliance!!!*
- Give them **checklists** OR complete the checklists for them?
- Consider if you are allowed to provide this service
  - Section 90(2) of the Companies Act
  - Code of Conduct (identify threats to your fundamental principles & implement safeguards)
- It is recommended that you keep this as a separate engagement
  - AUP (agreed-upon procedures) engagement
  - Follow ISRS 4400 (Revised) – effective for engagements from 1 January 2022
  - Separate engagement letter

POPIA Compliance Checklist

POPIA Compliance Checklist

Your LOGO

Detailed POPIA Compliance Checklist

	Procedure	Yes	No	N/A	Done by	Date	Comments
Step 1 - Formalise your POPIA compliance project							
(a)	**Did you identify your relevant stakeholders (clients, suppliers, individuals etc.)?**						
	• *Go through your client contracts & appointment letters, invoices, ID documents etc. Do not forget that this includes both natural and juristic persons. Go as far back as possible (use the financial services regulation requirements on how long you should keep data).* • *Save all these / file them where they can easily be found should you need to provide evidence of them.* • *Create a spreadsheet where you can list to have a quick reference of how old the data is, who has access to it and where it is stored.*						

This Detailed POPIA Compliance Checklist_MASTER is available to you as a Bonus Document

Other steps to take towards compliance

- Analyse what and how Personal Information is processed
- Decide how long you need to retain information
- Review your websites & online platforms
- Update/review your PAIA Manual – *use the free template available by IR*
- Communicate the identity of the IO to everyone in the organisation
- Training of all staff (to maintain awareness)
- Review recruitment processes, HR policies and employment contracts, and include provisions on processing of personal information where necessary
- Acquire consent to process personal info and special personal info
- Amend contracts with operators
- Report data breaches to the Information Regulator and data subjects

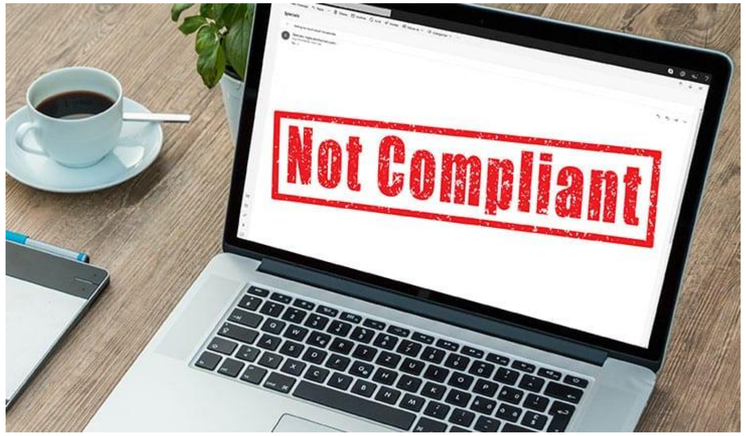
You should use a To-Do list to help you to keep track

COMPLIANCE TO DO LIST	DONE	NOT DONE
1. **Register** as Information Officer with the Regulator	X	
2. Have **awareness sessions** for staff on POPIA		X
3. Update engagement letters to include **POPIA consent** requirements	X	
4. Contact all service providers to get updated **written** agreements	X	
5. Update my **website** with cookies and privacy policy	X	
6. Run an **impact assessment** to find potential internal & external risks (incl. Safeguards)	X	
7. Check what **type of personal information** we process. Classify/categorize it		X
8. Have a plan for steps to follow should there be a **breach** (documented)	X	
9. Decide on **retention periods** for information stored (documented)	X	
10. Develop a **Compliance Framework** (your "how we plan to stay compliant process" document / file)		X
11. Develop / update PAIA Manual		X
12. Include **"opt-out" notices** in all mailers to clients e.g. newsletters	X	
13. Delete / shred personal information no longer needed		X
14. Have an **access control** register / means to monitor who has access to what information (remember paper-based information too).	X	

GUEST PRESENTATION

Enjoy today's detailed presentation

by **Pieter Fourie**



Guest Presenter

Pieter Fourie LLB, LLM (Law of Evidence)(Cum Laude)

- Pieter is a Senior Associate at SST Attorneys
- Practice areas: Civil Litigation, Labour Law, Commercial law
- He is a Specialist Commercial Attorney
- Pieter enjoys solving problems within the framework of the law to contribute to the orderly functioning of human society.
- He is inspired by the words of Voltaire – “No problem can withstand the assault of sustained thinking”

Complimentary
Self-help Smart Assessment

- **Is your business POPIA compliant?**
- https://sstlaw.co.za/tech-enabled-law/
- Benefits:
  - Enables you to determine how a certain aspect of law applies to your personal circumstances;
  - Visually displays your legal risks;
  - Save time and money;
  - Provides you with a written report containing legal guidance;
  - Your choice if a legal adviser should contact you.

Demonstration by Pieter…

Contact our Legal Commercial Specialist

SST ATTORNEYS
COMMERCIAL | CORPORATE | PROPERTY

Website: www.sstlaw.co.za
Telephone: +27 12 361 9823
Address: Menlyn Central Office Park | 7th Floor | 125 Dallas Avenue
Menlyn Maine | 0181

Pieter Fourie
Corporate & Commercial

+27 72 598 0423
pieter@sstlaw.co.za

TO OUR GUEST PRESENTER!

In closing…

- Compliance isn't expensive…it's priceless!!!!
- Stay up-to-date on POPIA developments!
- **Are you/your clients on track to ensure compliance by 1 July 2021?**
  - Have you appointed an Information Officer?
  - Do you fulfil the 8 conditions of POPIA?
  - Are you storing, transferring, sharing and deleting your data safely?
- **Remember that you must be able to PROVE your compliance…**essentially as from 1 July 2021
  - **NB** to document everything!

POPIA is definitely NOT going away, and monitoring will soon be on the way!

Bonus Documents

The following 3 Documents are available to you:

- ❑ The Basics of POPIA
- ❑ **Detailed POPIA Compliance Checklist_MASTER** *(MS-Word format)*
- ❑ PAIA-Manual-Template-Private-Body.doc
- ❑ PAIA-Manual-Template-Public-Body

Do you still need More Detail?

POPIA Compliance webinar series

1. POPIA in a Nutshell (7 July 2020)
2. Completing your Compliance Checklist - Steps 1 & 2 (6 August 2020)
3. Completing your Compliance Checklist - Steps 3 to 11 (3 September 2020)
4. Data Protection & Recovery (5 November 2020)
5. Specific industry considerations (10 December 2020)
6. Recap Session (25 January 2021)
7. 8 Conditions of POPIA (Part 1) (4 February 2021)
8. 8 Conditions of POPIA (Part 2) (25 February 2021)
9. Focus on safeguards & latest industry updates (14 April 2021)
10. Latest guidance for Information Officers (6 May 2021)
11. How to solve POPIA challenges in Financial Practices (3 June 2021)
12. Final POPIA readiness check (2 July 2021)

You can access these as Webinars-On-Demand *– Refer to the SAAA website*

Knowledge = Power!

- **Technical Alerts published daily**
  - **Follow SA Accounting Academy on LinkedIN**
- **Technical Summary Videos**
  - **Short summaries that you access when you want to**
- **Webinars-on-Demand**
  - **Wide variety of topics – not always a “live” event…**
  - All our webinars are available as individual recordings – which you can listen to at your leisure
  - Please refer to the SAAA website
- **MCLU subscription**
  - Stay up-to-date on all the latest developments in our field by attending the **Monthly Compliance & Legislation Update**
  - Please refer to the SAAA website for subscription options

QUESTIONS

for your participation!