

POPIA IS HERE TO STAY!



Presented by:

Lettie Janse van Vuuren
CA(SA)



Free webinar

Protection of Personal Information Act of 2013

Asking Questions

To ask questions and interact during the webinar please use the chat sidebar to the right of the video / presentation on the screen.

→ ***NB = Please include the topic that your question is about for easy identification purposes***

Feel free to ask your questions during the webinar in the chat

- Some of these will be addressed by the presenter during the presentation
- And the rest in the short Q & A session at the end of the presentation.

CONTENTS

- Introduction: Recap on the basics and most NB aspects of the Act
 - Latest updates (from the Information Regulator)
- How to use our FREE POPIA Compliance checklist
- Lawful processing of information
- Information Officer (appointment & responsibilities)
- Adequate safeguards
- Digital signatures
- Consequences of non-compliance





Introduction

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
- 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 won't be 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



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

PAIA updates from IR *(continued)*

- **Extension alert:**

- SMME's in certain industries have been exempted from having PAIA Manuals. The exemption expires 30 December 2021.

(refer to next 2 slides for details)

- **PAIA Regulations:**

- Regulations for PAIA have been drafted and are currently under review. These changes will affect roles of information officers as well as PAIA Manuals

Compilation of PAIA Manuals

<https://justice.gov.za/inforeg/legal/20210629-gg-PAIA-Exemption.pdf>

- **All private bodies are exempted from compiling a Sec 51 manual until **31 December 2021**, except:**
 - a) is not a private company as defined in section 1 of the Companies Act, 2008 (Act No. 71 of 2008); and
 - b) is a private company as defined in section 1 of the Companies Act, 2008 (Act No. 71 of 2008) which operates within any of the sectors mentioned in Column one of the Schedule **and**
 - i. has 50 or more employees in their employment; **or**
 - ii. has a total annual turnover that is equal to or more than the applicable amount mentioned in Column 2

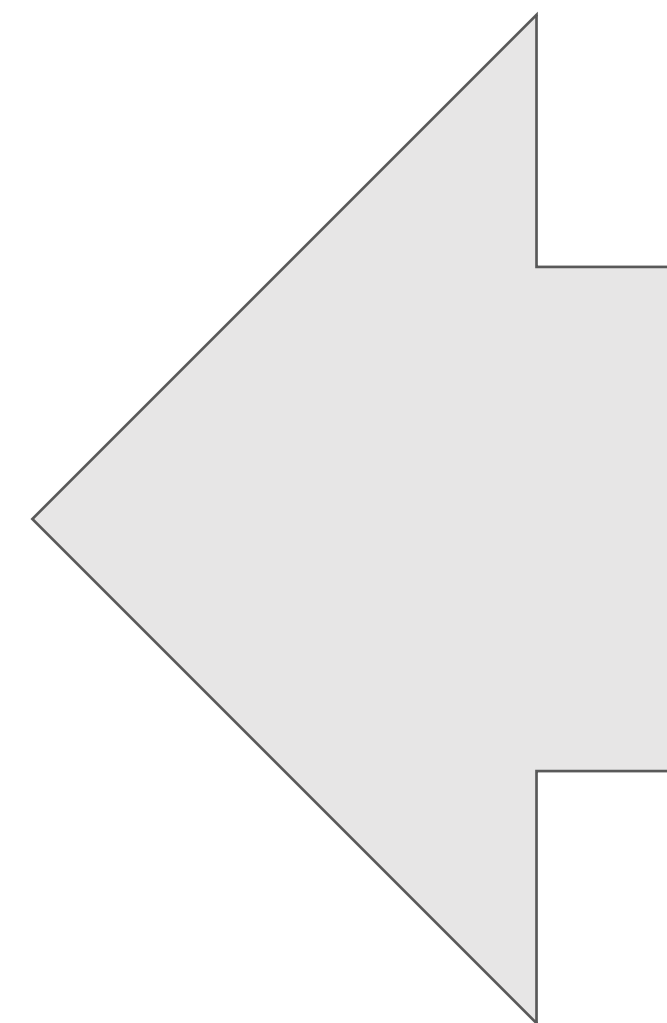
“Private Body” is defined in the PAIA

“company” is defined in the Companies Act

SECTOR	EMPLOYEES	ANNUAL TURNOVER in millions ZAR
Agriculture	50 or more	02
Mining and Quarrying	50 or more	07
Manufacturing	50 or more	10
Electricity, Gas, Water	50 or more	10
Construction	50 or more	05
Retail, Motor Trade and Repair Services	50 or more	15
Wholesale Trade, Commercial Agents, and Allied Services	50 or more	25
Catering, Accommodation and other Trade	50 or more	05
Transport, Storage and Communications	50 or more	10
Financial and Business Services	50 or more	10
Community, Special and Personal Services	50 or more	05

How to read the schedule:

Step 1	Step 2	Step 3	Step 4
Is the private body a company in terms of the Companies Act?	Does the company operate within any of the sectors listed under column 1 of the schedule?	Does the company have 50 or more employees OR	Does the company have an annual turnover equal or more than the amount listed under column 2 of the schedule?



NB

All private bodies are exempt except:

- Those NOT registered as private companies according to Companies Act
- Any private company which operates within the listed sectors and has 50 or more employees and the turnover listed alongside the sector in this table.

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.)?						
	<ul style="list-style-type: none">• 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

XS POPIA Checklist



POPIA COMPLIANCE CHECKLIST (HIGH LEVEL)

1. Formalise your POPIA compliance project

- Identify your relevant stakeholders (clients, suppliers, individuals etc.)
- Identify your project sponsor
- Identify your project manager
- Set high level scope, timescale, budget
- Identify security safeguards applicable to your industry / business

2. Appoint an Information Officer (Legal requirement – Default is highest ranking officer)

- Ensure alignment between your Promotion of Access to Information Act (PAIA) and POPIA Information Officer (IO)
- Decide whether the CEO can fulfil the IO function or needs a Deputy/Deputies (DIO)
- Agree IO/DIO roles and responsibilities
- Complete the formal appointment process

3. Perform a gap analysis versus the ACT (POPIA)

- Set interim and final targets for compliance – Compliance within reasonable practicality.
- Engage with stakeholders in the assessment
- Use an evidence-based approach
- Use the assessments for ongoing compliance monitoring

4. Analyse what and how Personal Information is processed (status quo)

- Use a broad definition of record types as per the POPIA (e.g. CCTV, biometric)
- Identify Special Information (e.g. Biometric data, Gender Information etc.)
- Look at various aspects as required by the POPIA (including consent, purpose, source, sharing, destruction)

Business critical Business continuity	Data Center compliance GDPR/Hedge (1)	IT Infrastructure Management Business applications (POPIA)
150 Lyntonville Park Centurion 0157 0157	150 Lyntonville Park Centurion 0157 0157	150 Lyntonville Park Centurion 0157 0157

- Consider user rights and their management
- Think broadly in terms of the types of devices where data is stored – and represents a security compromise risk

5. Review / draft POPIA compliance policies based on findings

- Review existing relevant policies
- Ensure your policies are reasonable and appropriate
- Make sure your policies are enforceable

6. Review your websites & online platforms

- PAIA Manual availability
- Data security notices
- Implement "best practice" such as Cookie notifications
- Develop and implement your remediation plan

7. Update / create your PAIA manual

- Confirm your organisation needs a Promotion of Access to Information Act (PAIA) manual
- Confirm whether you are a Public or Private Body as per the PAIA
- Review the proposed contents of your manual
- Ensure your PAIA manual follows the prescribed layout and includes the necessary details

8. Implement POPIA compliant PI management processes

- Look at the Personal Information lifecycle: including acquisition, processing, retention, and destruction practices
- Develop reasonable and appropriate measures to ensure ongoing compliance (e.g. Procedure document, self-assessments, health-checks, formal audits)
- Develop your dashboard for monitoring

Business critical Business continuity	Data Center compliance GDPR/Hedge (1)	IT Infrastructure Management Business applications (POPIA)
150 Lyntonville Park Centurion 0157 0157	150 Lyntonville Park Centurion 0157 0157	150 Lyntonville Park Centurion 0157 0157

9. Train internal stakeholders on their roles in POPIA compliance

- Design on-going training according to their needs
- Look to special needs such as the IO/DIO roles

10. Adopt POPIA compliance as "Business-As-Usual"

- Recognise that POPIA compliance will be the "new normal" and work that way
- Build compliance into your products, services and processes – adopt "Privacy By Design"

11. Information security Safeguards

- Consider generally accepted information security practices and procedures for both local and international data flows
- Consider electronic data protection tools i.e. Cybersecurity against Ransomware
- Consider means for secure data transfer, storage & recovery
- Revise processes for non-electronic data storage / filing
- Agree on safety practices for both operators and processors of data and manage these through contractual agreement where necessary.

Business critical Business continuity	Data Center compliance GDPR/Hedge (1)	IT Infrastructure Management Business applications (POPIA)
150 Lyntonville Park Centurion 0157 0157	150 Lyntonville Park Centurion 0157 0157	150 Lyntonville Park Centurion 0157 0157

This Checklist was provided as part of our POPIA Compliance webinar series and is available to you as a Bonus Document



In a nutshell...

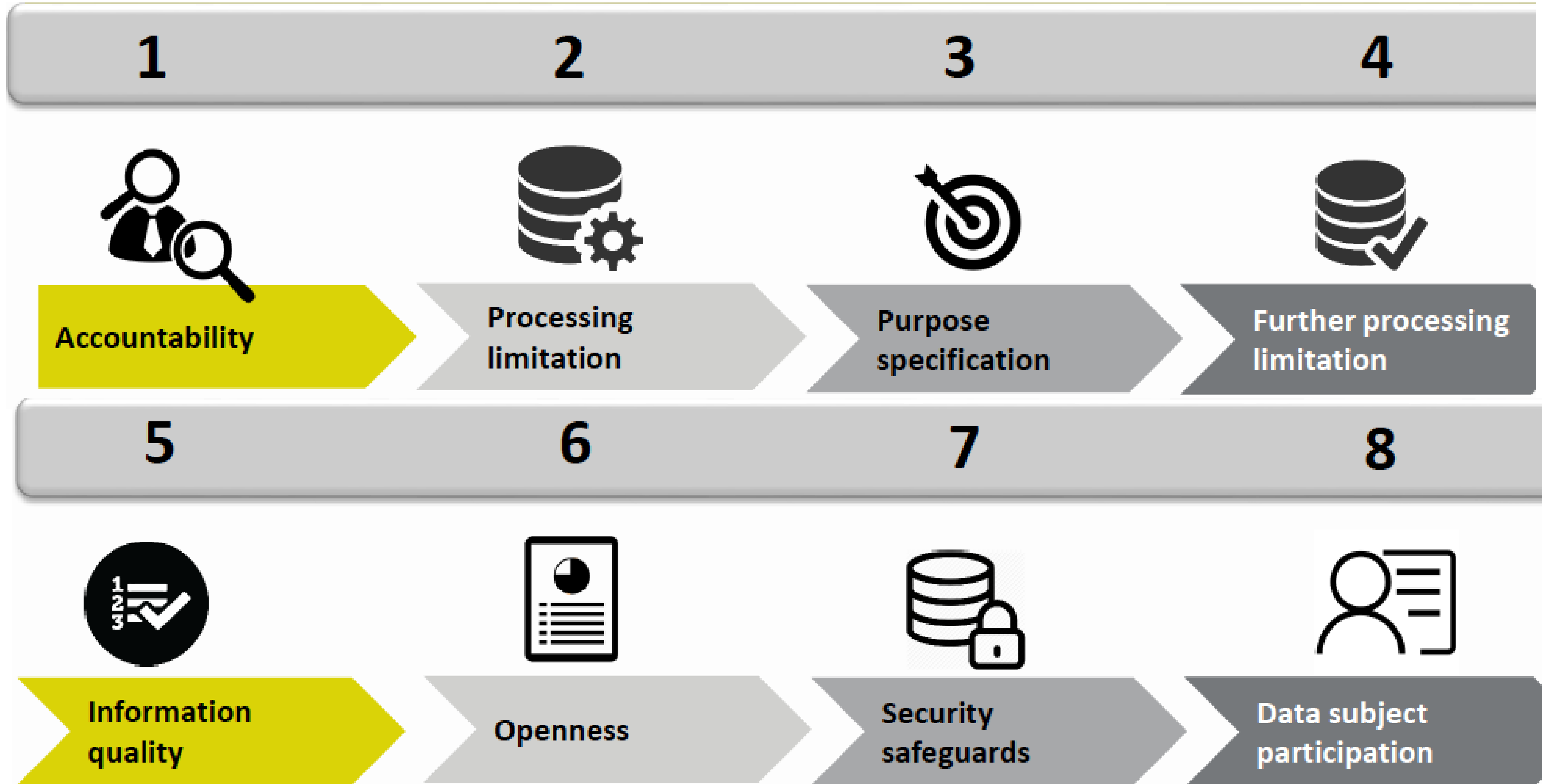
What are the **3 main things** employers need to do to ensure compliance with POPIA?

1. Employers need to ensure that they **lawfully process information**
2. Employers must appoint an **Information Officer**
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

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



Lawful processing of info



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.

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**

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.

Which Signature to use?

- It is best to use a **Digital Signature**:
 - If you need an audit trail
 - If you need a digital certificate to encrypt the final document
 - If you need to prove that the signature is authentic
 - If the document needs to be secure

Alternatively, an **Electronic Signature** may suffice

5 tips to secure digital Signatures

- ✓ Find **signature technology** that all of your main signatories will have access to and be able to use for all documents.
- ✓ Ensure that the signature created using this system has both a **“user identity” stamp** and a **“date and time” stamp** created automatically by the secure signature system with each signature made.
- ✓ Make sure documents to be stamped can **only be signed by designated signatories**.
- ✓ A signing system that keeps a **record of document version control** is vital, and your software must note a version for every person who has edited a document.
- ✓ Have the necessary **security protocols** in place, *such as:*
 - *Secure login credentials with an email notification to the user for every login, One-Time-Pins (OTPs) sent via SMS or Email of the appropriate signatory; or an Authenticator App for each login, encryption of all documents for signing, Secure audit logs of who signed which document, on which days and at what time, and the ability to lock the file once signed*

<https://www.bizcommunity.com/Article/196/662/215629.html>



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
- 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	

Consequences of non-compliance

○ Criminal

- POPIA imposes various criminal offences for non-compliance
- Non-compliance with POPIA can result in **imprisonment up to 10 years** and/or **fines of up to R10 million**

○ Civil

- 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

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 Act

MYTHS



- ❖ **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**



In closing...

- Stay up-to-date on POPIA developments!
- **Are you on track to ensure compliance by 1 July 2021?**
 - Do you fulfil the 8 conditions of POPIA?
 - Have you appointed an Information Officer?
 - Are you storing, transferring, sharing and deleting your data safely?
- **Remember that you must be able to PROVE your compliance...**
 - **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)*
- XS_POPIA_Checklist



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

What's Next?

- ❑ **Next webinar = Beginning of August 2021**
 - ✓ **FAQ session**

- ❑ **Monthly POPIA Update Series of webinars:**
 - ✓ **To function as regular contact sessions and**
 - ✓ **Communication of latest POPIA news and updates**

We will communicate the dates and contents of upcoming webinars to you...watch your inbox!



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





for your participation!