POPIA Webinar Series – Nr 12

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

2 JULY 2021

The Protection of Personal Information Act (POPIA)
Final POPIA readiness check (& latest news snippets)

Presenter

Lettie Janse van Vuuren CA(SA), RA, CBA(SA)

- Lettie joined SA Accounting Academy in November 2017 as Head of Technical. She is a Chartered Accountant, Registered Auditor and Certified Business Accountant.
- 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.

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, these will be addressed live in the formal Q & A at the end of the presentation.

Where appropriate, a Q & A Summary will be uploaded to your profile as soon as all answers have been documented.

WHAT'S ON THE AGENDA?

Contents

Recap: Where did we end with the previous webinar?

Module 1: Latest updates (from the Information Regulator

Module 2: Checklist : Key points to remember

Module 3: Tip of the day : Signature security

Module 4: Busting some POPIA myths

Module 5: Managing electronic information

Where did we end last time?

Focus was on How to solve POPIA challenges facing Financial Practices:

- Consent
- Data Classification
- Best Practices
- Common challenges with storage

Today we look at the latest updates & revisit some vial points to check your POPIA readiness

" Mr. Deadline, would you mind coming back when we're all perfectly ready? "

GUEST PRESENTATION

Enjoy today's detailed presentation by

Karabo Letlhaku

&

Stephane Geldenhuys

Guest Presenter

Karabo Letlhaku

Karabo’s interest in data protection was ignited in 2013 when the POPI Act was first introduced.

As the lead in the Policies and Procedures management project at Eskom Pension and Provident Fund at the time, Karabo was in charge of ensuring that all policies and procedures of the Fund were updated and compliant with the various regulatory requirements affecting financial services and Pension funds.

She joins Montana Data Company as an Account Executive specialising in assisting clients to find simplified yet effective ways of managing data and complying with data related regulation.

She is currently a candidate in the Masters in ICT Policy & Regulation programme with Wits and holds a Communication Science and a Media Ethics degree from UNISA.

MONTANA
DATA COMPANY

Guest Presenter

Stephane Geldenhuys

Stephane' motto in life is simple, "BE the CHANGE you want to see in the world - it starts with YOU as the individual."

She is a highly accomplished and committed Management Professional that has a vast knowledge in designing and deploying sales and marketing strategies and programmes. She has a passion for customer centricity and believes that at the heart of any successful business is a satisfied customer.

Steph has 21+ years ICT and Telecommunications experience with a strong technical and solution selling understanding from Network/ Last Mile Connectivity, Voice, Mobile, Data Centre Solutions, Call Recording and Data Management. She joined the Montana Data Centre team as Sales Executive and with her knowledge and experience from the ICT environment has the main responsibility of customer engagement in the Data Management side of business.

MONTANA
DATA COMPANY

Module 1

Latest updates from the Information Regulator

INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

Updates from the Regulator

- **EXTENTION ALERT**: SMME's in certain industries have been exempted from having PAIA Manuals. The exemption **expires 30 December 2021.** ***(refer to next slide)***

- **EXTENTION ALERT**: All private & public bodies that were required to apply for PRE-AUTHORISATION to process **Special personal information** now have until **1 February 2022**.

- **Information Officer registrations**: No responsible party will be held liable for not registering by 30 June 2021. This is due to technical issues faced by the Regulators registration portal.

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

See Source documents – Draft regulations, exemption notes for all the above

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 withing the listed sectors and has 50 or mores employees and the turnover listed alongside the sector in this table.

Special Personal Information
(Prohibited with exception)

As per **Section 26** of POPIA :-

- ***Religious*** *information*
- ***Philosophical beliefs***
- ***Race*** *or* ***ethnic origin***
- ***Trade union membership*** *&* ***political persuasion****,*
- ***Health or sex life***
- ***Biometric*** *information*
- ***Criminal behaviour*** *of a data subject to the extent that such information relates to –*
  - *(i) the alleged commission by a data subject of any offence; or*
  - *(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.”*

NB*: There is prohibition to processing* ***CHILDREN’S*** *information too!*

Module 2

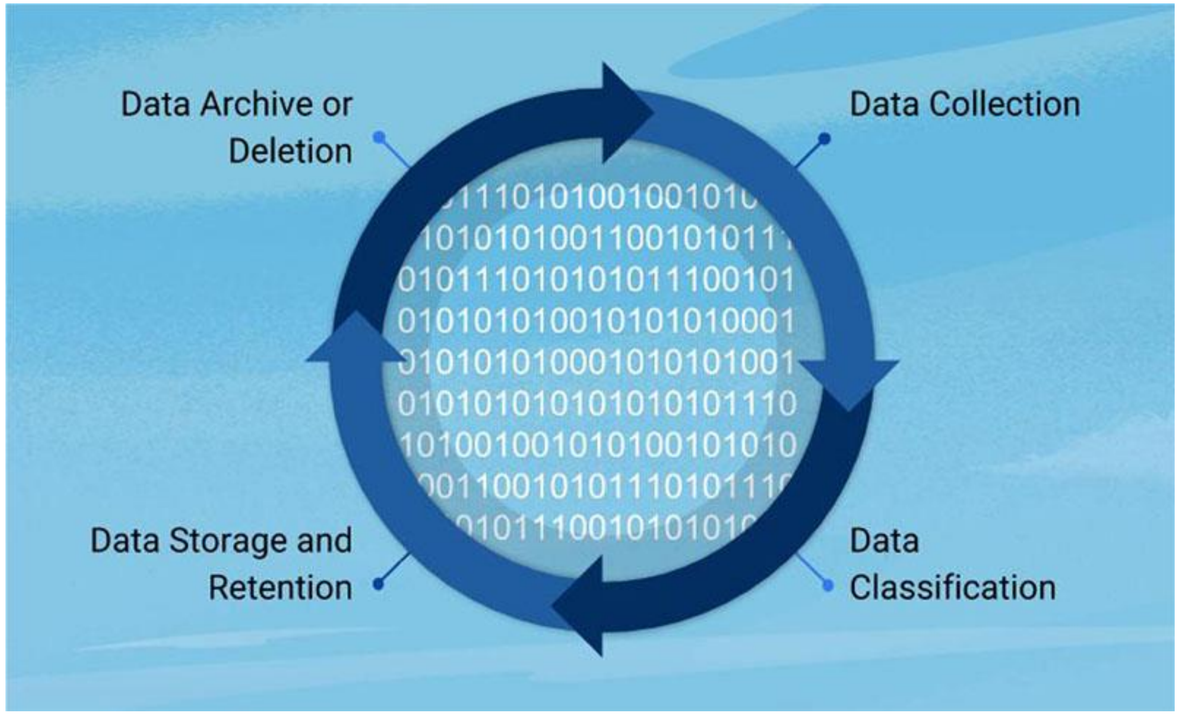
Checklist: Key points to remember

COMPLIANCE CHECKLIST

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	

Data Retention

- *HOW LONG IS TOO LONG?*



Section 14 of POPIA specifically states that records of personal information may not be retained any longer than necessary for achieving the purposes for which the information was collected or subsequently processed unless:-

- the retention of the records is required or authorised by laws; or
- the responsible party reasonably requires the record for lawful purposes related to its functions or activities; or
- the retention of the records is required by a contract between parties, or
- the data subject or a competent person where the data subject is a child has consented to the retention of the records.

OING FORWARD

STEP	DESCRIPTION
1. Define the purpose of the information gathering/ processing	• **Ensure that the personal information that you intend to collect is for a specific, explicitly defined, and lawful purpose that relates to a function or activity of your company.** • **Determine the duration for which the information will be retained in order to achieve this purpose.**

2. Notify the data subject	• **Take the necessary steps to notify the person whose information is being processed.**
	• **Inform them of:**
	  • what information is being processed;
	  • why their information is being processed;
	  • your company name and address;
	  • whether the provision of the information is voluntary or mandatory;
	  • the consequences of failure to provide the information;
	  • any particular law authorising or requiring the collection of information;
	  • whether the information will be transferred to a third party or foreign country; and
	  • if the information is not collected from them directly, the source from which it is collected.

STEP	DESCRIPTION

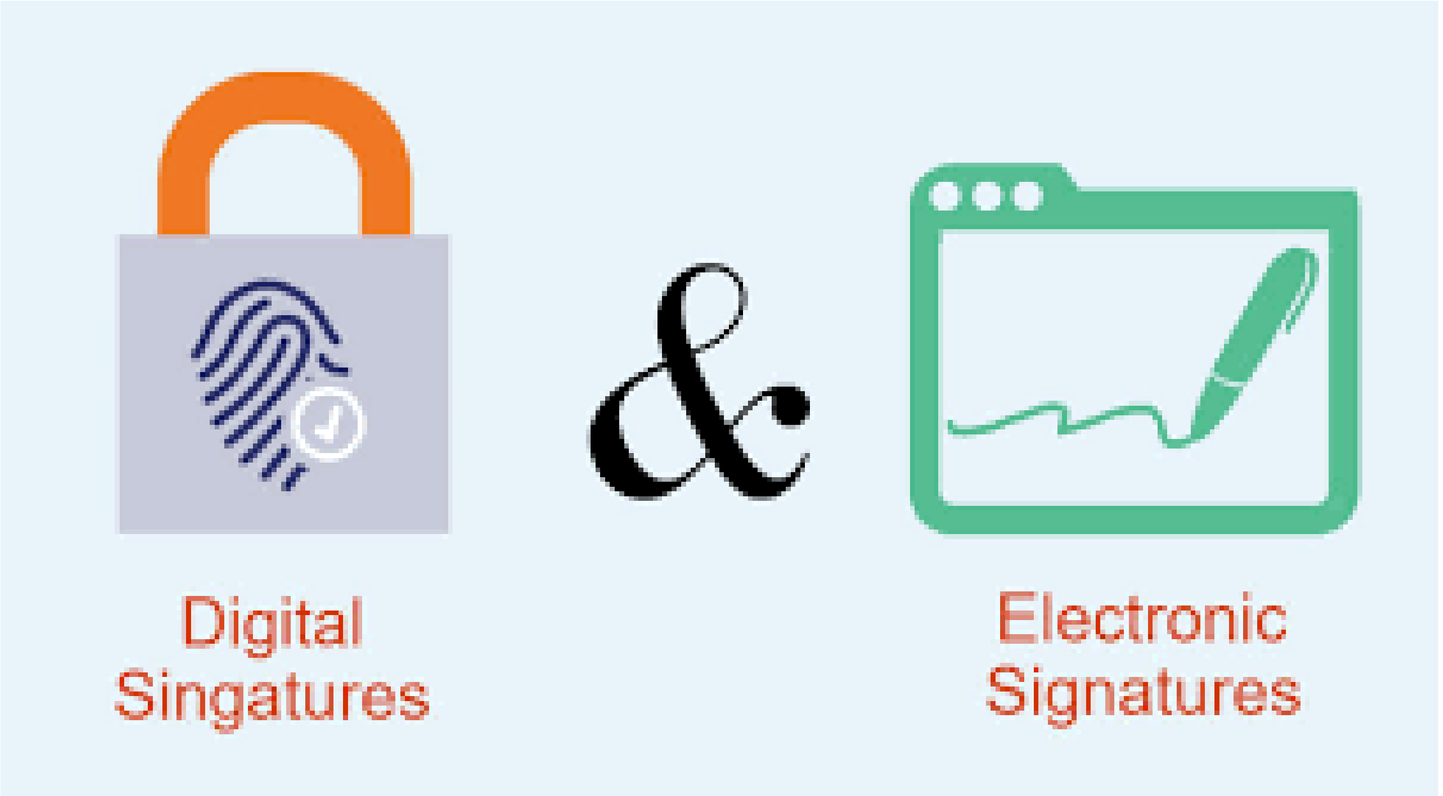
3. Determine the legal basis for processing of personal information	• **Assess and ensure that you have a legal basis (in terms of POPIA) for each processing activity which you undertake.**
	• **Ensure that you obtain the informed consent of the data subject (or in the case of a child, a competent person) in order to obtain and process their information, where this may be required.**
	• **The general legal bases provided under POPIA, apart from consent, include:**
	  • the processing of the personal information is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
	  • the processing complies with an obligation imposed on you by law;
	  • the processing protects a legitimate interest of the data subject; or
	  • the processing of the personal information is necessary for pursuing the legitimate interests of your company or of a third party to whom the information is supplied.
	• **Please note that there are specific requirements relating to the different types of special personal information.**

Source: Cliffe Dekker Hofmeyr April 2021 Newsletter

Module 3

Tip of the day: Signature security

KNOW THE DIFFERENCE



Which one to use?

	DIGITAL SIGNITURE	ELECTRONIC SIGNATURE
If you need an audit trail	Yes	No
If you need a digital certificate to encrypt the final document	Yes	No
If you need to prove that the signature is authentic	Yes	No
Does the document need to be secure?	Yes	No

Secure solutions for legal compliance

- ✓ Find signature technology that all of your main signatories will have access to and be able to use for all documents. This must be a single system, controlled centrally in your organisation or for your board of directors.
- ✓ 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.
- ✓ A truly secure system where individuals can sign documents legally has 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

Module 4

Busting some POPIA 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

MODULE 5

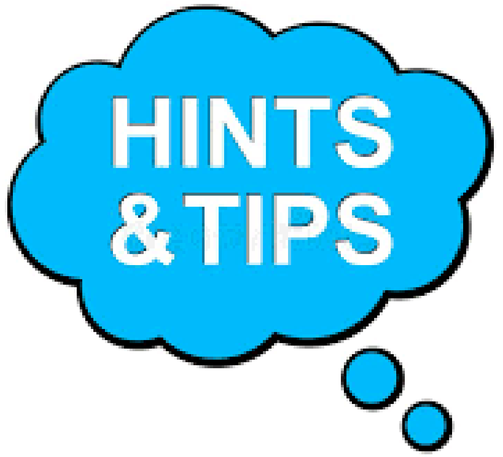
MANAGING ELECTRONIC INFORMATION


You lost a lot of files, but one Doc was recovered. Looks like your 2014 Resolutions. All it says is "Backup Data."

Some safeguard recommendations

- **Most Critical: Data Security, Storage and Recovery**
  - Store your information in a local and secure environment
  - Avoid using external hard drives and memory sticks – this can get stolen, be lost or go corrupt
- **Retention of Data**
  - Ensure you only keep data for the period it's required – this will also help save cloud storage cost
  - Archiving of historic data may be an affordable option, whilst ensuring the data is safe and secure
- **Backup in an environment you can quickly & efficiently restore**
  - Make sure the backup is minimum AES128 encrypted
    - End-to-end encryption as far as possible
  - Google Drive, OneDrive, Dropbox
    - These are File Sharing environments, NOT backup solutions
    - Vulnerable to Cyber Attack, Hacking and Ransomware

Some safeguard recommendations *(continued)*



- **Passwords**
  - PC / Laptop Password
  - File level Passwords
  - Router: apply a strong & secure password
  - Frequently change Passwords
  - Don’t use the same Password for multiple log-in’s
  - Store passwords in a safe environment – many secure password management tools
- **Anti Virus**
  - Google Result of Top 10 Anti Virus software packages, i.e. TotalAV, Norton, Kaspersky, Bitdefender, BullGuard (Gamers), McAfee
  - Is free anti-virus solutions safe to use?
    - They may protect against common, known computer viruses, but may leave you vulnerable to as yet-unknown threats

Some safeguard recommendations *(continued)*

- **Shared Environments – Google Drive, OneDrive, Dropbox**
  - Remember it's a replication and NOT a backup
  - Manage who has access
    - Change password once somebody has left your company
- **Phishing / Ransomware**
  - Surf the Internet safely
    - Careful of unsecure sites
    - Careful what you download and install
  - Think twice before opening links/documents that you're not 100% sure of
    - Recent ransomware links also have the secure lock embedded, so it looks legit

If hacking your environment result in the disclosure of email addresses, contact details, etc. you may be held accountable for breaching POPIA

TO OUR GUEST PRESENTERS!

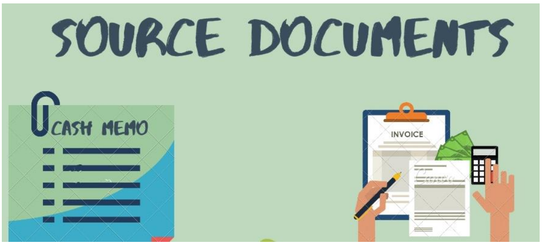
In closing…

- ✓ Remember, keep your to-do list updated
- ✓ Don’t wait until you are asked to prove compliance to start documenting…keep your Compliance Checklist updated
- ✓ Decide how long you need to retain data
- ✓ Use the appropriate signature security
- ✓ Safeguard your data
- ✓ **POPIA is definitely here to stay, so make sure that your processes are sustainable and practical to include POPIA on an ongoing basis!**
- ❑ **We will also keep you updated with new developments and announcements from the Information Regulator**

Source & Bonus Documents

The following 10 Documents are available to you:

- ❑ **Detailed POPIA Compliance Checklist_MASTER** *(MS-Word format)*
- ❑ Gazette on PAIA exemption list
- ❑ InfoReg_20210622_EnforcementPowers and registration of IOs
- ❑ InfoRegSA-GuidanceNote-PPI-Exemption for LawfulProcessing-202106
- ❑ InfoRegSA-GuidanceNote-Processing-PersonalInformation-Children-20210628
- ❑ InfoRegSA-GuidanceNote-Processing-SpecialPersonalInformation-20210628
- ❑ Know your signature security
- ❑ PAIA Extension of Exemption Update
- ❑ RecordRetentionSamplePolicy
- ❑ Article: 4 POPIA myths you need to know the truth about



Contact our POPIA Specialists

MONTANA
DATA COMPANY

Suite 51
377 Rivonia Boulevard
Rivonia
2128
South Africa.
http://www.montanadc.com

Karabo Letlhaku
Data Governance Account Executive

+27 84 550 9798
karabol@montanadc.com

Stephane Geldenhuys
Sales Executive

+27 76 411 5089
Stephaneg@montanadc.com

What’s Next?

- **Next webinar = End of July / Beginning of August 2021:** **FAQ session**

- **Monthly POPIA Update Series of webinars:** **To function as regular contact sessions and communication of latest news and updates on POPIA**

- **POPIA Compliance Series:** **Refer to next slide**

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

Completed webinars in this 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)

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!