# POPIA Webinar Series – Nr 6

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


## 25 JANUARY 2021

***The Protection of Personal Information Act***

***Recap session***

# 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.

# About SAAA

## Creating opportunities to connect our partners to succeed

SAAA offers CPD training for accountants, auditors, bookkeepers and tax practitioners. We give you access to professional and technical content that ensures both your knowledge and skills are maintained so you remain professionally competent.

## The CPD policy is compliant with IFAC IES7

All training offered by SAAA is recognised for CPD hours by the relevant professional bodies.

# SAAA Rewards

**CPD Subscribers gain access to various rewards**

These can be accessed from your profile by logging in and navigating to your “My Rewards” > “Find out more” to see the reward partner benefits and claim it.

These rewards include discounts, reduced premiums and free stuff.

# Reward Partners

Acts Online provides legislation, including amendments and regulations, in an intuitive, online format.

Draftworx provides automated drafting and working paper financial software.

EdNVest offers an exciting and unique product that leverages Section 10(1)(q) of the Income Tax Act

InfoDocs Company Secretarial Software.

# Reward Partners *(continued)*

PRACTICE Ignition

Practice Ignition simplifies onboarding - from engagement letter creation to securing client signatures.

intuit quickbooks

QuickBooks Cloud Accounting Platform: The one place to grow and manage your entire practice.

the tax shop ACCOUNTANTS

Join the largest accounting and tax franchise in Southern Africa.

# Webinar Housekeeping

The **Webinar Material, Source Documents & Bonus Documents** will be uploaded to your SAAA profile after the webinar – it's usually a good idea to check the next day.

The **webinar recording** and **presentation** will also be available at the end of the webinar within your SAAA profile.

These can be accessed from your profile by logging in and navigating to your "My Dashboard" > "View Events" and then clicking on "Links & Resources" next to the webinar title.

The webinar is available under the "Recording(s)" tab and the **Webinar Material, Source Documents & Bonus Documents and Presentation** under the "Files" tab.

# Claiming CPD Hours

You can claim your CPD hours for this webinar at the end of the webinar within your SAAA profile.

This can be accessed from your profile by logging in and navigating to your “My Dashboard” > “View Events” and then clicking on “Links & Resources” next to the webinar title.

***Complete the Self-Assessment Questions to qualify for an additional 1 bonus hour of CPD***

The “Claim My CPD” option is available under the “CPD” tab. Once claimed you will be able to view and download your certificate.

# Ask 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 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.**

# Disclaimer

## Disclaimer

Whilst every effort has been made to ensure the accuracy of this presentation and handouts, the presenters / authors, the organisers do not accept any responsibility for any opinions expressed by the presenters / author, contributors or correspondents, nor for the accuracy of any information contained in the handouts.

## Copyright

# WHAT'S ON THE AGENDA?

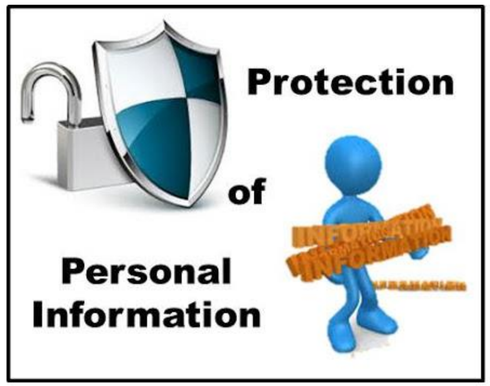
# Table of Contents

**Previously**: Where did we end with the previous webinar?

**Recap**: Focus on the most important requirements of POPIA:

- ❑ The basics of POPIA
- ❑ What is personal information?
- ❑ Processing of personal information
- ❑ Who are the Role Players?
- ❑ Your POPIA Compliance Checklist
- ❑ Protection & Recovery of data
- ❑ Specific industry considerations
- ❑ Source Documents available
- ❑ Bonus Documents available

**What's next?**




# Quotes

It's impossible to move, to live, to operate at any level without leaving traces, bits, seemingly meaningless fragments of personal information.

– William Gibson

We are like Hansel and Gretel, leaving bread crumbs of our personal information everywhere we travel through the digital woods.

– Gary Kovacs

# Recap

# Including the Basics of POPIA

# Where did we end last time?

Specific Industry requirements for personal info:

- ❑ COVID-19
- ❑ Financial sector (patented information)
- ❑ Education
- ❑ Health sector
- ❑ Residential / Gated communities
- ❑ Law firms

# Which other topics did we cover in 2020?

- Nr 1: POPIA in a Nutshell (7 Jul 2020)
- Nr 2: Completing your Compliance Checklist - Steps 1 & 2 (6 Aug 2020)
- Nr 3: Completing your Compliance Checklist - Steps 3 to 11 (3 Sep 2020)
- Nr 4: Data Protection & Recovery (5 Nov 2020)
- Nr 5: Specific industry considerations (10 Dec 2020)

# Today we revisit some of the most important POPIA requirements…

*aka Recap session*

# Recap on the Basics of POPIA

The basics have been summarized in detail in your previous Webinar Material:

1. Introduction
   - POPI vs POPIA
2. What are the Objectives of the Act?
3. Who does the Act apply to?
   - Private body
   - Public body
   - Exclusions
4. The Role Players
   - Data subject
   - Responsible party
   - Operator
   - Information officer
   - Information Regulator
5. What does it mean to “Process” information?
6. Which Type of Information is protected?
   - What is included in “Personal information”?
7. Interaction with GDPR
8. Penalties and Fines
9. Other consequences of Non-Compliance with POPIA to consider
   - Impact on organisation
   - Impact on employee
   - Considerations for the auditors & accountants (NOCLAR)
10. The Information Regulator
11. Links to relevant Legislation

***The Basics of POPIA has been saved in a separate Source Document – which is available to you***

# Which info about me is out there in the world?

# Introduction

As a business owner, your operational concerns include security and the protection of personal information. POPIA came into effect 1 July 2020 and a grace period of 12 months has been given to businesses to comply. Therefore, as of 1 July 2021, all businesses will have to be POPIA compliant.

You must be able to prove compliance as from 1 July 2021 – remember NOCLAR is a reportable matter!

**The POPI Act 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…What is Personal information?

"**personal information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

b) information relating to the education or the medical, financial, criminal or employment history of the person;

c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

# What is Personal information? *(continued)*

d) the biometric information of the person;

e) the personal opinions, views or preferences of the person;

f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

g) the views or opinions of another individual about the person; and

h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

# Remember…What does it mean to “process” info?

"**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;

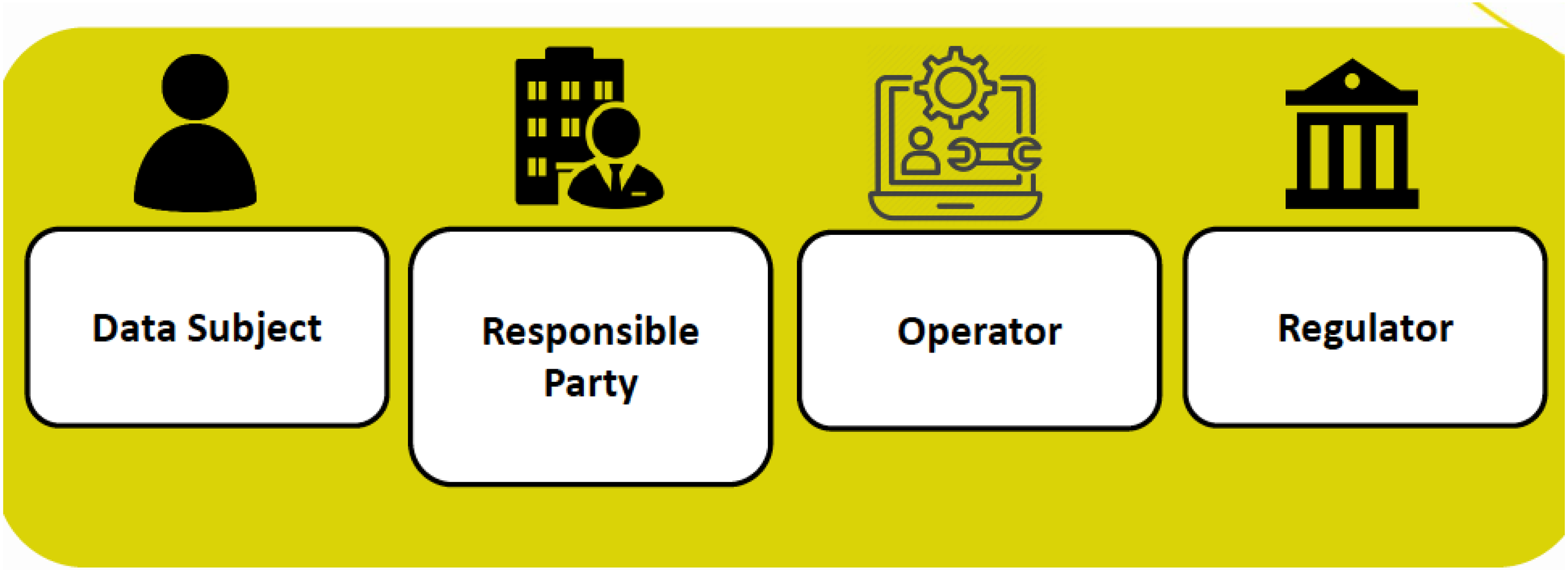
**How long should personal info be retained?**

= No longer than is necessary to achieve the purpose for which it was collected

# Employers process personal & special personal info for various purposes

- Legal obligations / Complying with the law
- Recruitment
- Training
- Promotion
- Discipline
- Security
- Monitoring/Assessing
- Performance
- Quality Control
- Customer Service
- Health and Safety in the
- Workplace
- Conclusion of Contracts

# Who are the Role Players?



# What are the 8 Conditions of POPIA?

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Accountability | Processing limitation | Purpose specification | Further processing limitation |

| 5 | 6 | 7 | 8 |
|---|---|---|---|
| Information quality | Openness | Security safeguards | Data subject participation |

# Your POPIA Compliance Checklist


Reg. No.: 2019 / 066104 / 07
Phone: +27 79 885 4543

**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)




Reg. No.: 2019 / 066104 / 07
Phone: +27 79 885 4543

- 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

Disaster recovery
Business continuity
Data Center consultancy
Artificial Intelligent (AI)
ICT Infrastructure Management
Business applications (ERPs)


Reg. No.: 2019 / 066104 / 07
Phone: +27 79 885 4543

**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.

Disaster recovery
Business continuity
Data Center consultancy
Artificial Intelligent (AI)
ICT Infrastructure Management
Business applications (ERPs)

***The POPIA Compliance Checklist is available to you as a Source Document***

# 11 Steps of the Compliance Checklist

1. Formalise your POPIA compliance project
2. Appoint an Information Officer
3. Perform a gap analysis versus the ACT (POPIA)
4. Analyse what and how Personal Information is processed (status quo)
5. Review / draft POPIA compliance policies based on findings
6. Review your websites & online platforms
7. Update / create your PAIA manual
8. Implement POPIA compliant PI management processes
9. Train internal stakeholders on their roles in POPIA compliance
10. Adopt POPIA compliance as “Business-As-Usual”
11. Information security Safeguards

***The POPIA Compliance Checklist is available to you as a Source Document***

# “Big Picture” Action Plan

**Responsible parties have to take various steps to comply.**

Here is one simplistic example:

1. Appoint an Information Officer.
2. Draft a Privacy Policy.
3. Raise awareness amongst all employees.
4. Amend contracts with operators.
5. Protect the information that you are privy to!
6. Report data breaches to the regulator and data subjects.
7. Check that they can lawfully transfer personal information to other countries.
8. Only share personal information when they are lawfully able to.

# Considerations for Responsible Parties

**Some considerations of the types of procedures that you would need to put in place as the Responsible party include:**

- How to inform the Information Regulator of any security breach?
- How to inform the Data Subject that their personal information has been compromised?
- Which procedures are followed when sharing personal information with an external operator?
- Which procedures are followed when sharing personal information with an external operator?
- How are safeguards continually updated?
- How are we alerted when personal information is accessed or modified without authorisation?

# Considerations for Responsible Parties *(continued)*

**Some considerations of the types of procedures that you would need to put in place as the Responsible party include:**

- How to determine which employees are permitted access personal information and what information they are permitted to access?
- How do we establish and maintain appropriate safeguards against the identified risks?
- How to prevent personal information from falling into unauthorised hands?
- How to identify any foreseeable internal and external risks to personal information?

***The remainder of our webinar series in 2021 focus on many of the above***

# Planning tips

**Remember the following NB tips during your action plan:**

- Keep a copy of both POPIA & PAIA handy as these 2 work hand in hand.
- Identify key players (Information officer, deputies, project officer in necessary).
- Outline roles and responsibilities & make official appointments for roles (incl. KPIs). Ensure that these are in line with both POPIA & PAIA.
- Break down the compliance planning over a few months using the checklist, but keeping in mind that the ACT is applicable in retrospect – so what you do before the deadline of 30 June 2021 matters too.
- Draft scope of work based on 8 conditions of compliance

# Safeguarding the information collected

- Consider the following when dealing with Protection of data:
  - How is data compromised?
  - How do criminals use your data?
  - What is the related risk of losing data?

  *Remember: Disaster strikes without warning, so you must be prepared!*

  - ➢ Now that we all work remotely, have you backed up all your laptops?
  - ➢ Do you know how you would recover your stolen / destroyed information?
  - ➢ Are you storing your information in local and secure environments?
  - ➢ How do you & your staff share large files? e.g. WeTransfer / Google docs.
  - ➢ Is your IT service provider well versed in POPIA compliance? Check!

**HOW DO I EFFECTIVELY PROTECT MY DATA???**

# Recovery of Data

- The need for recovery procedures
- Accessing if your business can be recreated after a disaster
- Identify potential backup and disaster recovery strategies

**HOW DO I ENSURE RECOVERY OF MY DATA???**

# Specific Industries – considerations

- What do specific industries require in terms of personal information?
- How does POPIA specifically affect each of the following industries?
  - COVID-19
  - Financial sector (patented information)
  - Education
  - Health sector
  - Residential / Gated communities
  - Law firms

**It's not just about how POPIA affects your organisation, but also how it affects the world in which you live, e.g. your office park, your transactions with hospitals, banks, etc.**

# Industry: COVID-19

➔ Let's have a look at what a pandemic did to this ubject matter data and how this fits into POPIA

- ❑ *Temperature, ID number, symptoms, etc.*
- ❑ *Current Coronavirus status*
- ❑ *The employer is obliged to maintain a safe and hazardous free working environment in terms of the OHSA, and can request specific info on the health status of an employee*

***Refer to the Source Documents for full detail:***

- *InfoRegSA-GuidanceNote-PPI-Covid19-20200403*

# Industry: COVID-19 *(continued)*

➔ **Guidance Note** issued by Information Regulator

- *Purpose = to guide public and private bodies and their operators on the reasonable limitation of the right to privacy when they process personal information of data subjects for the purpose of managing the spread of COVID 19*
- *It outlines the conditions for the lawful processing of personal information which public and private bodies must comply with when they process personal information of data subjects.*
- *These conditions include the following **obligations**: to ensure that personal information is collected for a specific purpose only, namely to manage the spread of COVID 19, to put adequate security measures in place to ensure the integrity and confidentiality of personal information of data subjects and to destroy or delete the information when no longer authorized to retain it.*

# Industry: Financial sector

➔ Is all your personal / confidential data protected?

➔ *LOTS of info is kept by financial industry:*

- ❑ *Name, ID number, Address, telephone numbers, email address*
- ❑ *Account information, Credit score, passwords, etc.*
- ❑ *Insurers – policy info, e.g. smoker*
- ❑ *Financial advisers – Financial history, personal information of beneficiaries, medical health info*
- ❑ *Audit, Tax & Accounting services – Contact info, financial info, tax info, etc.*

***Refer to the Source Document for full detail:***

- *INFO on Financial Services Sector*

# Industry: Education

➔ How does POPIA affect education? Where is data kept?

➔ What may and may not happen from a creche to universities?

- ❑ *Standard processes and documents like indemnity forms, deployment reports and educator details are all protected.*
- ❑ *Even processes such as submitting reports to the department is affected by the Act*

***Refer to the Source Documents for full detail:***

- *INFO on Education Sector*

# Industry: Health sector

➔ How does POPIA affect the health industry, from the department to a pharmacy?

- ❑ *Health records must be protected!*
- ❑ *A patient's information is confidential and a person may only disclose it in certain circumstances*
- ❑ *The time-honoured sharing of information between colleagues cannot continue given the new legislation*
- ❑ *Special personal info = health info (present)*
- ❑ *Personal info = Medical history (past)*

***Refer to the Source Document for full detail:***

- *INFO on Healthcare industry*

# Industry: Residential / Gated communities

➔ Does the local HOA have any idea what is coming their way?

- ❑ *Significant implications for owners, tenants and executives in community housing schemes like sectional title complexes, apartment blocks, residential estates and retirement villages*
- ❑ *Trustees must now be able to respond when owners want to know what they are doing with their personal information*
- ❑ *When you enter an office park – which information do you provide whilst completing the visitor's register?*

***Refer to the Source Document for full detail:***

- *INFO on Gated communities and Sectional title property*

# Industry: Law firms

A lot of law firms are advertising as being “privacy and data protection law specialists”

- ➔ Document management, is there a system in place to protect all the printed files?
- ➔ What happens if all the physical documents are gone?
- ➔ Are all your conversations private via telephone?
  - ❑ *How secure is “Legal privilege”?*

# 10 Source Documents available to you

- ❑ Basics of POPIA
- ❑ POPIA Compliance Checklist
- ❑ InfoRegSA-GuidanceNote-PPI-Covid19-20200403
- ❑ INFO on Direct Marketing
- ❑ INFO on Education Sector
- ❑ INFO on Financial Services Sector
- ❑ INFO on Gated communities and Sectional title property
- ❑ INFO on Healthcare industry
- ❑ Policy formulation example
- ❑ POPIA Regulations and Templates - Forms

# 3 Bonus Documents available to you

- **Detailed POPIA Compliance Checklist_STEP 1**
  - *Formalise your POPIA Compliance project*
- **Detailed POPIA Compliance Checklist_STEP 2**
  - *Appoint an Information Officer*

***Refer to Module 3 of your webinar material for more detail on these 2 items***

- **POPIA Compliance Checklist (in a MS-Word format)**

# In closing…

- ✓ Remember, you and other businesses in SA must be able to prove compliance as from 1 July 2021.
- ✓ Ultimately, the requirements of POPIA should not be seen as onerous within specific industries, they should be seen as good business practice for day-to-day operations.
- ✓ Communicate with those industry entities that you deal with, and ensure that your personal information is protected.
- ✓ Don’t forget to worry about the information that you hold in respect of clients and other data subjects!

**The remainder of our webinar series in 2021 will focus on how to secure your data and meet regulatory requirements**

# Contact our POPIA Experts


**Elmar Schorndorfer**
CEO

+27 83 652 3242
elmarsc@montanadc.com

**Karabo Letlhaku**
Account Executive

+27 84 550 9798
karabol@montanadc.com

# What's Next???


Dates for the 2021 instalments of the POPIA Compliance Series:

- **4 February 2020: 8 Conditions of POPIA (Part 1)**
- **25 February 2020: 8 Conditions of POPIA (Part 2)**
- **8 April 2020: Focus on safeguards & latest industry updates**
- *6 May 2020: Space left open for "emergency" topic*
- **3 June 2020: How to solve POPIA challenges facing Financial practices**
- **24 June 2020: POPIA Readiness check**

*Watch your e-mail inbox to book in advance for the rest of the webinar series and receive a discount!*

# QUESTIONS

# Formal Q&A Session

We will now take a **quick comfort break** before we discuss some questions received during the webinar.

- Please use the chat sidebar to the right of the video / presentation on the screen to ask your questions.

*Remember: A Q&A summary will also be uploaded to your profile, where applicable*

**If you would like to e-mail a question please use:**

**technicalquestions@accountingacademy.co.za**

**E-mail general comments to info@accountingacademy.co.za**


# for your participation!