POPIA: Information Regulator update & FAQ session

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

8 NOVEMBER 2021

Documents & Guidance issued by the Information Regulator
Latest POPIA developments

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.

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

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

DRAFTWORX™
Financial Statements | Working Papers

Draftworx provides automated drafting and working paper financial software.

EdNVest

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

ID InfoDocs

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 **23 Source & 3 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 **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.

The "Claim My CPD" option is available under the "CPD" tab.

Once claimed you will be able to view and download your certificate.

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

Disclaimer

Disclaimer

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 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 on the basics and most important aspects of the Act;

- 2021 POPIA updates and documents published by the Information Regulator;

- The latest PAIA Manual templates issued by the Information Regulator;

- How to use our FREE POPIA Compliance checklist;

- Some of the most popular FAQs on POPIA and PAIA to date
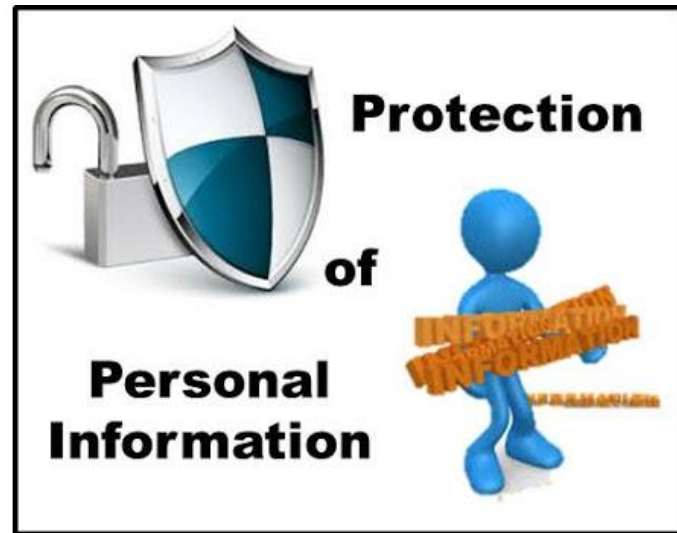
- In closing…

INTRODUCTION
RECAP ON THE POPIA BASICS

Abbreviations used

- **POPIA** = the Protection of Personal Information Act of 2013

- **PAIA** = the Promotion of Access to Information Act of 2000

- **InfoReg** = the Information Regulator of South Africa

- **FAQs** = Frequently Asked Questions

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)*

o 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

o 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

o You must be able to **prove compliance from 1 July 2021**

  ➢ *Even though this won't be monitored just yet…*

Introduction *(continued)*

- 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 & PAIA is overseen by the Information Regulator of SA

  - As of 30 June 2021 the Information Regulator took over the regulatory mandate functions relating to PAIA from the SAHRC

Introduction

Lawful processing of info

1	2	3	4

Accountability → Processing limitation → Purpose specification → Further processing limitation

5	6	7	8

Information quality → Openness → Security safeguards → Data subject participation
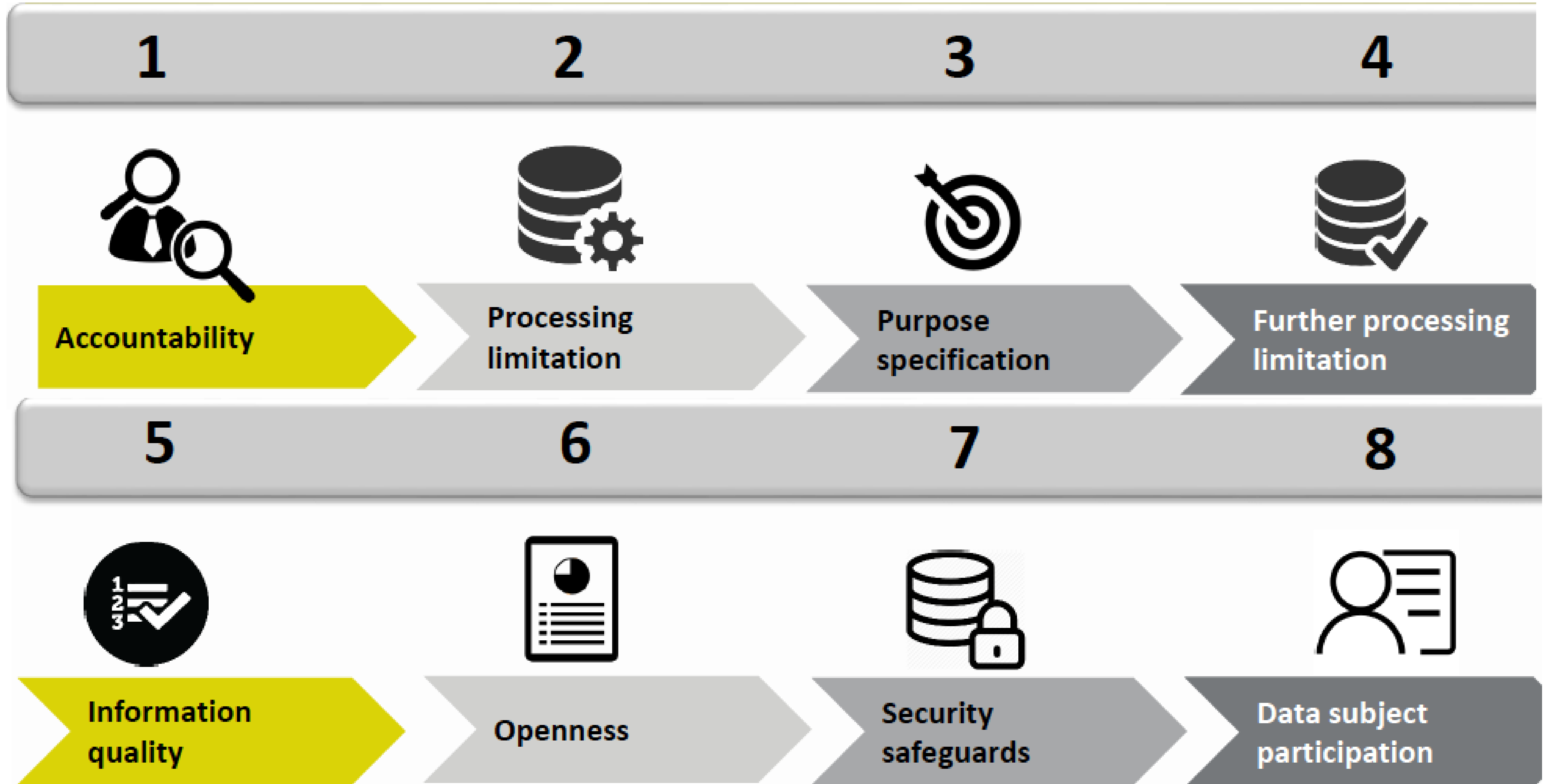
The Information Officer (IO)

❑ **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**

2021 POPIA Updates & Documents published by the Information Regulator

Previous updates from InfoReg SA

o **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 was due to technical issues faced by the Regulator's registration portal

o **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

PAIA updates from InfoReg

o **Extension alert:**

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

(refer to next 3 slides for details)

o **PAIA Regulations:**

➤ Refer to Source Document

- *Gazetted on 27 Aug 2021*

- to align the previous PAIA regulations with POPIA given that, as per section 114(4) of POPIA

- Some of the key changes introduced by the Regulations relate to the functions and procedures of the Information Regulator.

- In addition, the Regulations also contain further duties of Informa
  some of which are linked to the functions of the Information Regu

Latest extension of PAIA Manual exemption

➤ *Refer to Source Document*

o *PAIA = Promotion of Access to Information Act, 2000*

o The current exemption expired on 30 June 2021

o The Minister of Justice and Correctional Services, extended the current exemption by a further six (6) months

o effective from 1 July 2021 to 31 December 2021

o to afford private bodies that are currently exempted adequate time to compile their PAIA Manual

o ***On 1 January 2022, ALL public & private bodies MUST compile a manual!***

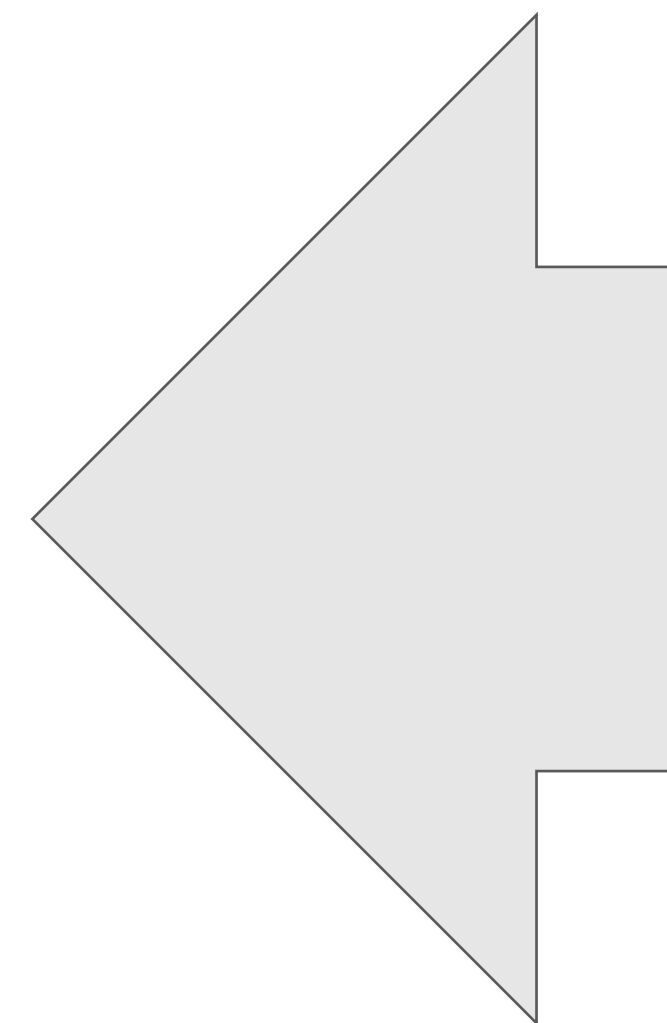o **The current exemption:** Applies to SMMEs in certain industries

As per Gazette…

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

LATEST POPIA UPDATES
& DOCUMENTS PUBLISHED
BY THE INFORMATION REGULATOR

Latest InfoReg Update

➤ *Refer to Source Documents available to each of these items*

1. **InfoReg acknowledges receipt of Codes of Conduct**
    - *BASA (deals with how personal information will be processed by member banks)*
    - *1. National Radiology Services Inc, 2. Regio Independent School, 3. Rockjumper Birding Tours CC, 4. Silk Route Gold (Pty) Ltd, 5. WILLCOM (Pty) Ltd, 6. Willow Acres Estate, and 7. Maktaba Stationery Trading As PNA*

2. **PAIA Manual templates** published (in Word-format) **– PUBLIC & PRIVATE BODY**

3. **PAIA forms 1, 2, 4, 5 and 13 published**

    o Form 01: Request for a Guide from the Regulator [Regulation 2]

    o Form 01: Request for a Copy of the Guide from an Information Officer [Regulation 3]

    o Form 02: Request for Access to Record [Regulation 7]

    o Form 04: Internal Appeal Form [Regulation 9]

    o Form 05: Complaint Form [Regulation 10]

    o Form 13: PAIA Request for Compliance Assessment Form [Regulation 14(1)]

InfoReg Update *(continued)*

4. **PAIA update from Information Regulator**
   - confirmed that **submissions of PAIA manuals will not have a deadline until further notice**

5. **Guidance note on exemptions from the conditions of POPIA**
   - This applies to Responsible Parties who:
     - Intend to apply for exemption (Sec37), or
     - Are exempt from processing personal information (sec38)

6. **InfoReg confirms commencement date of Section 58(2) of POPIA is 1 February 2022**
   - Private & Public bodies that were required to apply for Pre-Authorisation to process Special personal information, now have until 1 February 2022
   - Responsible Parties must obtain prior authorisation from the InfoReg prior to any processing of personal information in terms of Sec 57 of POPIA

InfoReg Update *(continued)*

6. **Guidance note on Processing of Special Personal Information**
   ○ Application form provided

7. **Guidance note on Processing of personal info of children**
   ○ Application form provided

8. **POPIA Security compromise notification**
   ○ The Information Regulator notifies potentially affected persons who are 'data subjects' of the Regulator about the security breach that they experienced. Malware has attacked the Information Technology systems of the Department of Justice and Constitutional Development – as was confirmed by the DoJ&CD in a public statement on 9 September 2021

   ➢ In terms of **section 22 of POPIA**, where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Information Regulator (Regulator) and the data subject, unless the identity of such data subject cannot be established.

InfoReg Update *(continued)*

9. **PAIA Guide**
   - o The Information Regulator published its Guide on how to use the Promotion of Access to Information Act 2 of 2000 ("PAIA Guide") in each of South Africa's 11 official languages.

   - o *The purpose of this Guide is 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.*

InfoReg Update *(continued)*

10. New email addresses for Information Regulator

- The Regulator's email system now operates under a new domain in order to ensure accessibility to the public and stakeholders.
- The new email addresses have been created to ensure accessibility for the public and stakeholders.
- Specific email addresses have been created for different purposes, including:
  - general enquiries;
  - the lodging of complaints, for example, when you feel that your personal information has been violated or that your request for access of information is unduly denied;
  - the manual registration of Information Officers; and
  - general compliance in relation to POPIA and PAIA

InfoReg Update *(continued)*

11. How to handle POPIA complaints

- The Information Regulator has published rules of procedure relating to the manner in which a complaint must be submitted and handled by the Information Regulator.

- The Rules of procedure contain the following sections:
  Arrangement of Rules
  Chapter 1 – Definitions
  Chapter 2 – Introduction
  Chapter 3 –Purpose of Rules
  Chapter 4 – Lodging a Complaint
  Chapter 5 – Processing of complaint lodged with the Information Regulator
  Chapter 6 – Action taken after receipt of a complaint
  Chapter 7 – Investigation of complaints
  Chapter 8 – General aspects in resolving complaints
  Chapter 9 – General Provisions
  Annexures

IRBA Staff Alert 6

Key Questions for the firm's leadership to consider when processing client data

1. Do engagement letters, terms and conditions and other contracting documents contain the relevant clauses regarding data protection and security?
2. Are the tools and technology used for the processing of data secure and compliant with the standards and legislation?
3. Can the processes and controls that are in place be demonstrated to regulators, authorities and clients?
4. Are there adequate policies and procedures in place to ensure the protection of data from the point of collection to destruction?
5. Are the processes, controls, and procedures frequently reviewed and tested?
6. Has training been provided to all employees regarding the protection and retention of client data?
7. Is there a response plan if a data breach were to occur?
8. Are third parties/service providers aware of and have sufficient data protection controls?
9. Are there adequate resources engaged by the firm to proactively monitor and maintain data security processes and controls?

CHECKLISTS

POPIA Compliance Checklist

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 justitic 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 assessment 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)

- 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

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.

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

Practical 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	

FREQUENTLY ASKED QUESTIONS

Bonus Documents

In addition to the Source Documents, the following 3 Bonus Documents are available to you:

❑ The Basics of POPIA

❑ **Detailed POPIA Compliance Checklist_MASTER** *(MS-Word format)*

❑ XS_POPIA_Checklist

✓ *Remember that these are uploaded to your profiles & should be available immediately after the webinar has ended*

➢ *Refer to other webinars presented by Lettie on POPIA and PAIA*

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

In closing…

- POPIA & PAIA are here to stay!
  - Ensure that your manuals are drafted & up-to-date
  - Remember that YOU need to prove compliance (when asked)

- Refer to the Compliance To-do-list for some practical issues that MUST be considered

For now…ensure that you & your clients have PAIA manuals on 1 January 2022!

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 **M**onthly **C**ompliance & **L**egislation **U**pdate
- ➢ Please refer to the SAAA website for subscription options

QUESTIONS

Formal Q&A Session

We will now take a **quick comfort break** before we go live to 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!