SA | ACCOUNTING ACADEMY

Connect. Partner. Succeed.

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

POPIA Webinar Series – STEP 2

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

3 SEPTEMBER 2020

The Protection of Personal Information Act

*Completing the POPIA Compliance Checklist – **Steps 3 to 11***

Presenter

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

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 SAAA's 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

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

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

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 **Source 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 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.

Disclaimer

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

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

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.

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.

SA | ACCOUNTING ACADEMY

What's on the Agenda?

Table of Contents

Module 1: Gap Analysis: The Act vs your status quo **(Step 3)**

Module 2: How else do you process information? **(Step 4)**

Module 3: Revise / draft policies & procedures **(Step 5)**

Module 4: PAIA - Revise / draft & upload your manual **(Steps 6 & 7)**

Module 5: Compliance maintenance **(Steps 8, 9 & 10)**

Module 6: Security safeguards **(Step 11)**

Today's Quote

"Safety isn't expensive, its priceless"

author unknown

"We like to greet our Regulatory Compliance hires with one word."

Introduction

Recap on the Basics of POPIA

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

If you are not in possession of this webinar material, please contact SAAA to obtain a copy

Where are we now?

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

Xtreme Systems
Where customers are partners.

Reg. No.: 2019 / 086104 / 07
Phone: +27 79 885 4543

POPIA COMPLIANCE CHECKLIST (HIGH LEVEL)

We are still in the Consultative phase and we are PLANNING!

- *In our previous webinar, we discussed* ***Steps 1 & 2*** *of the POPIA Compliance Checklist*
- Today = **Steps 3 to 11 of the POPIA Compliance Checklist**

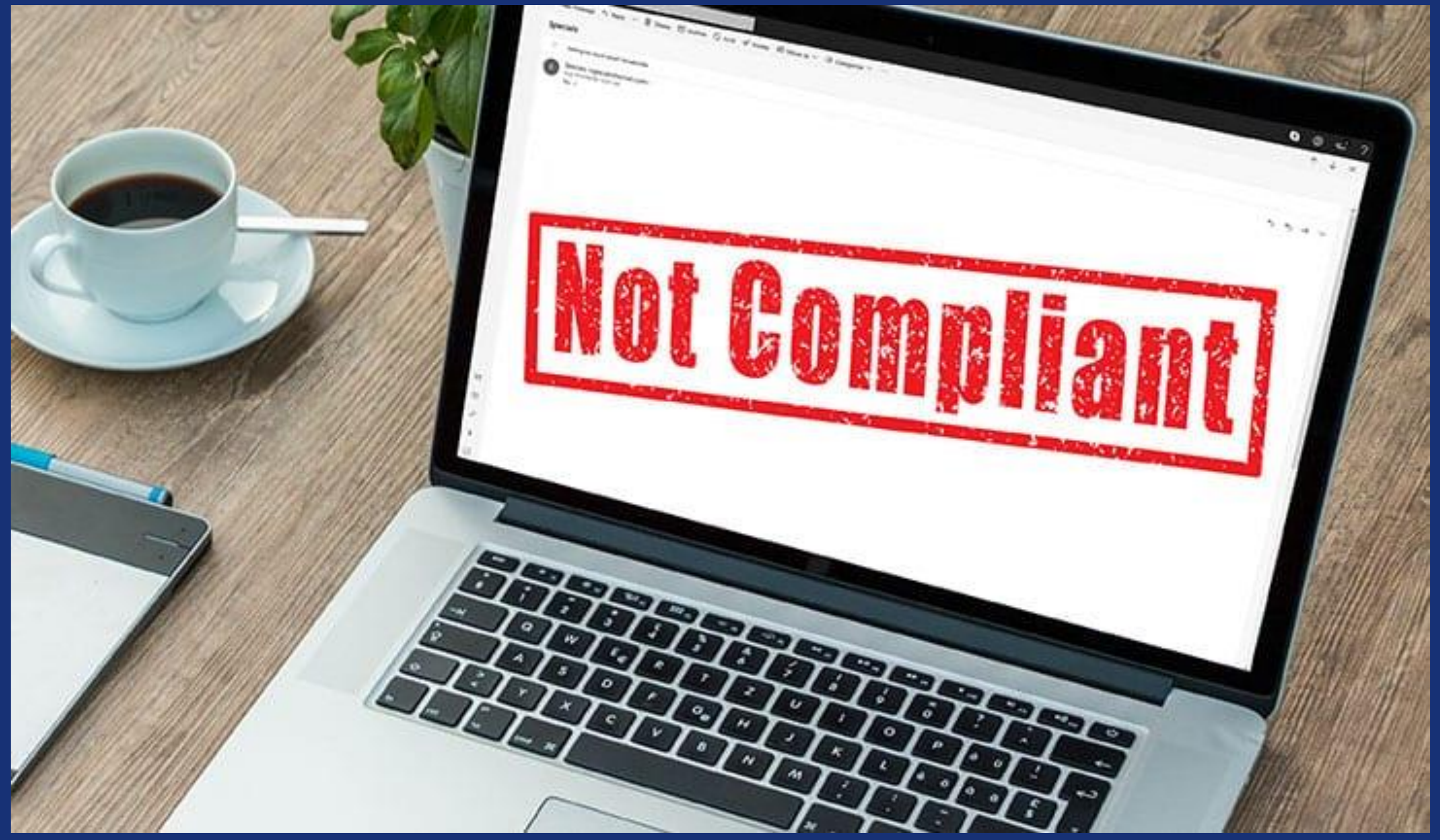
This POPIA Compliance Checklist (High Level) is once again available to you as a Source Document

SA | ACCOUNTING ACADEMY

Guest Presentation

Enjoy today's detailed presentation

by **Karabo Letlhaku**



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.

Let’s recap and emphasize some **VERY IMPORTANT** aspects…

Planning

➔ 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 next 11 months using checklist, but keeping in mind that the ACT is applicable in retrospect – so what you do this year matters too.

➔ Draft scope of work based on 8 conditions of compliance.

POPIA: Protection of Personal Information Act
PAIA: Promotion of Access to Information Act

SA | ACCOUNTING ACADEMY

MODULE 1

STEP 3

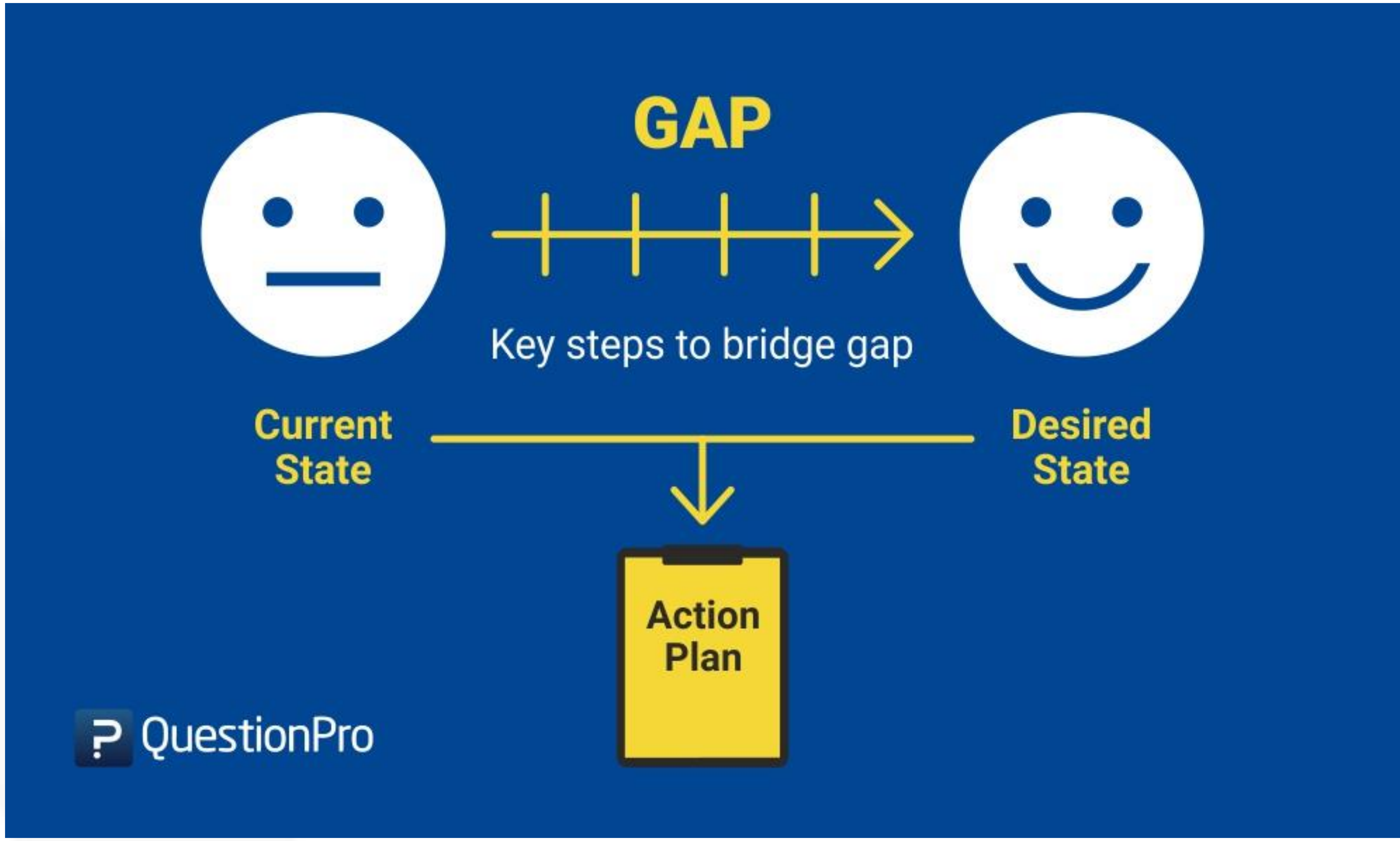
GAP ANALYSIS: THE ACT VS YOUR STATUS QUO

The Gap Analysis

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

The following items are dealt with here:

1. *Contents of this step on the Checklist*
2. Where are you now?
3. The 8 conditions of compliance are key



Checklist – Step 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

Where are you now?

- Are your employees trained & can you prove it?
- Do your contracts include non-disclosure clauses?
- Are your internal documents compliance ready e.g. policies, delegation of authority, employment contracts
- Do you have the appropriate IT systems in place? e.g DR, Back up, are you sharing documents in secure environments?
- Are your business processes helping you stay compliant? Is your physical filing system secure?

The 8 POPIA Conditions of Compliance

1

Accountability

Responsible parties must comply with these eight conditions

2

Processing Limitation

Personal information should only be obtained by limited and lawful processing that does not unnecessarily infringe privacy

3

Purpose Specification

The purpose for which personal information is collected must be specific, explicitly defined and lawful

4

Further Processing Limitation

Further processing must be compatible with the purpose for which personal information is collected

5

Information Quality

Reasonably practicable steps to ensure personal information is complete, accurate, not misleading and updated

6

Openness

Advise the data subject of certain mandatory information in respect of collection

7

Security Safeguards

The integrity and confidentiality of the personal information must be secured

8

Data Subject Participation

The data subject has certain access rights, including a right to request its deletion

MODULE 2

STEP 4

HOW ELSE DO YOU PROCESS INFORMATION?

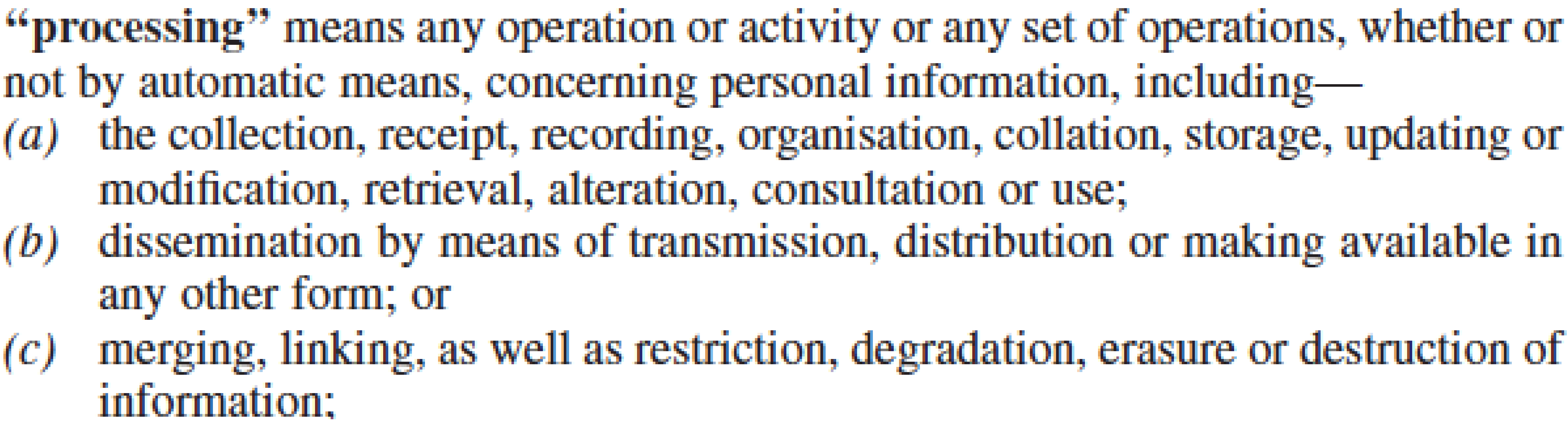
Step 4 – How else do you process information?

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

The following items are dealt with here:

1. *Contents of this step on the Checklist*
2. What is Processing?
3. Think about your data, activities, equipment and processes…

”Processing” defined



“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;

Checklist – Step 4

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

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

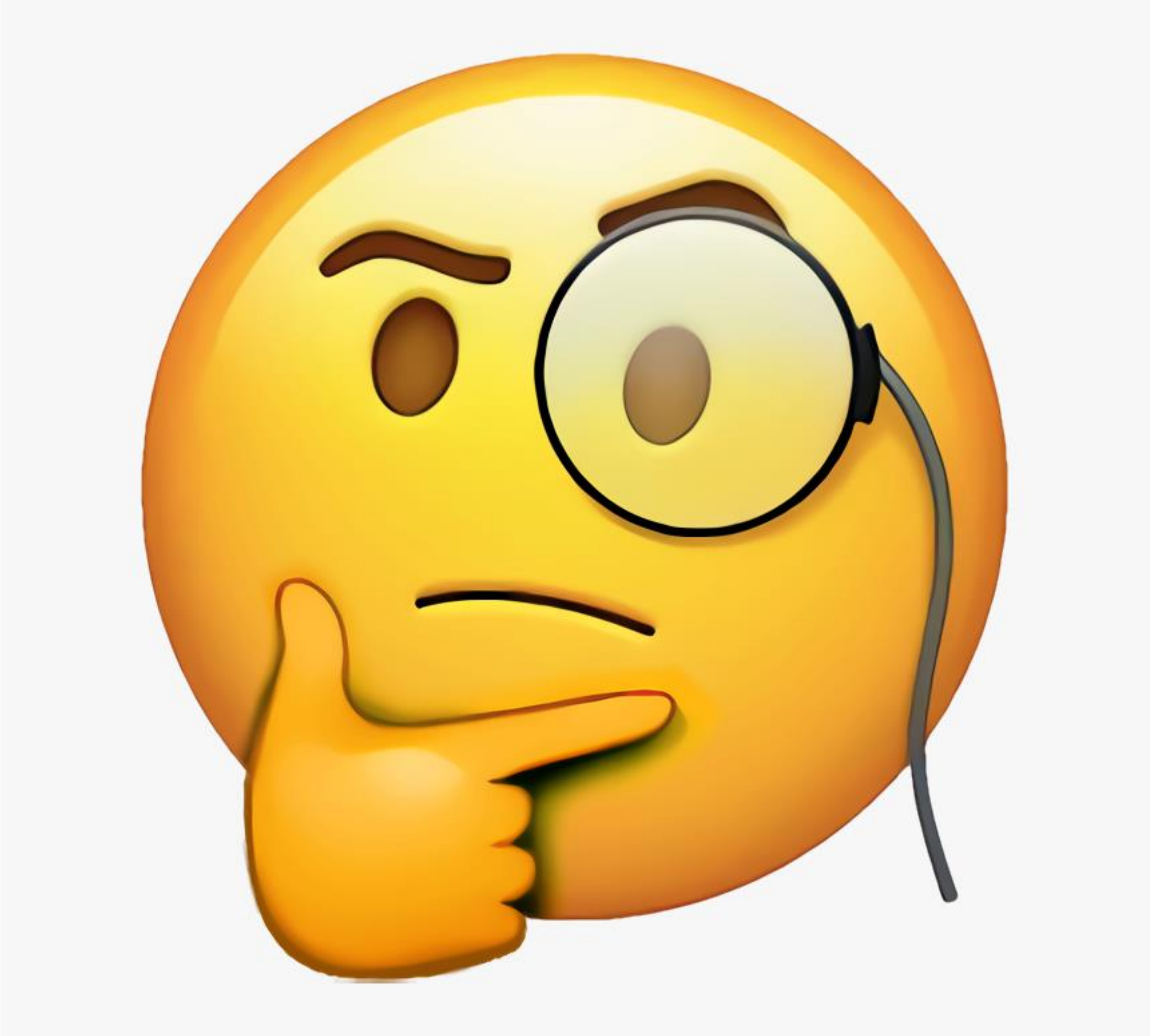
Think about it...

Do you have security cameras, biometrics?

Do you use google analytics?

Do you collect website cookies?

Do you use Zoom, WhatsApp, social media, etc?



Employee data incl. next of kin & children information

MODULE 3

STEP 5

POLICIES & PROCEDURES

Step 5 – Policies & Procedures

The following items are dealt with here:

1. *Contents of this step on the Checklist*
2. Review existing relevant policies
3. Ensure your policies are reasonable and appropriate
4. Make sure your policies are enforceable
5. Decide how often these will be reviewed
6. Ensure that all staff are familiar with them – remember to have evidence to this.

Bonus Document: Formulating policies example

- ➢ *Available to you as a Source Document*

Checklist – Step 5

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

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

SA | ACCOUNTING ACADEMY

Module 4

Step 6 & 7

PAIA:

Revise / Draft & Upload your Manual

Steps 6 & 7 – PAIA Compliance

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

The following items are dealt with here:

1. *Contents of these steps on the Checklist*
2. Other PAIA considerations
3. Information Officer responsibilities

Bonus Document: PAIA Manual template from Regulator

- ➢ *Available to you as a Source Document*

Checklist – Steps 6 & 7

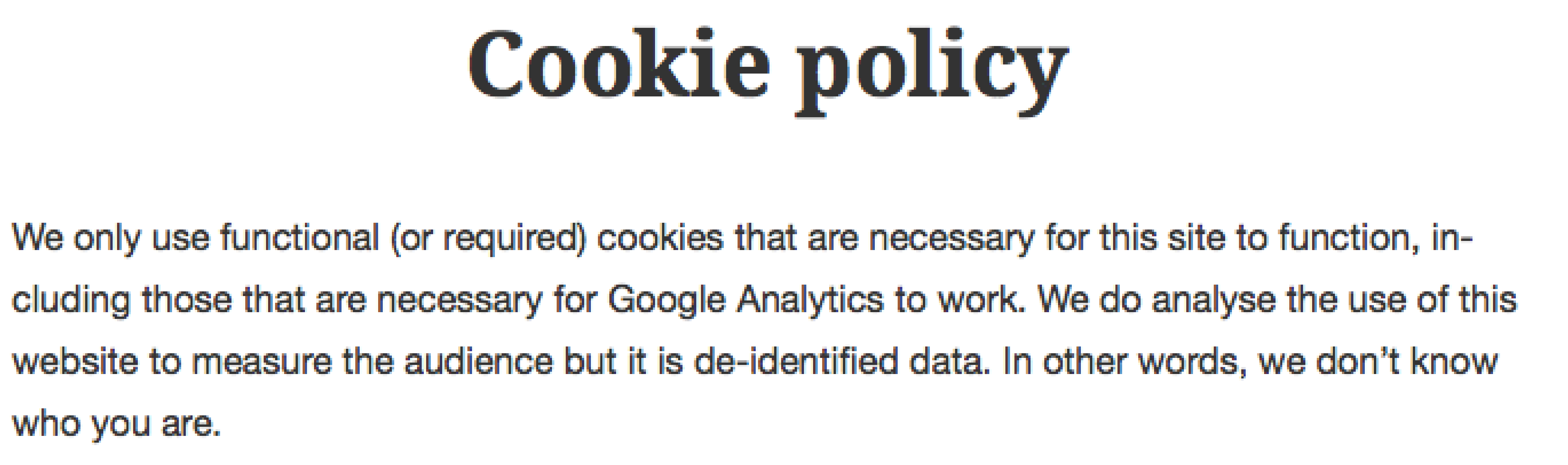
6. Review your websites & online platforms

- ❑ 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

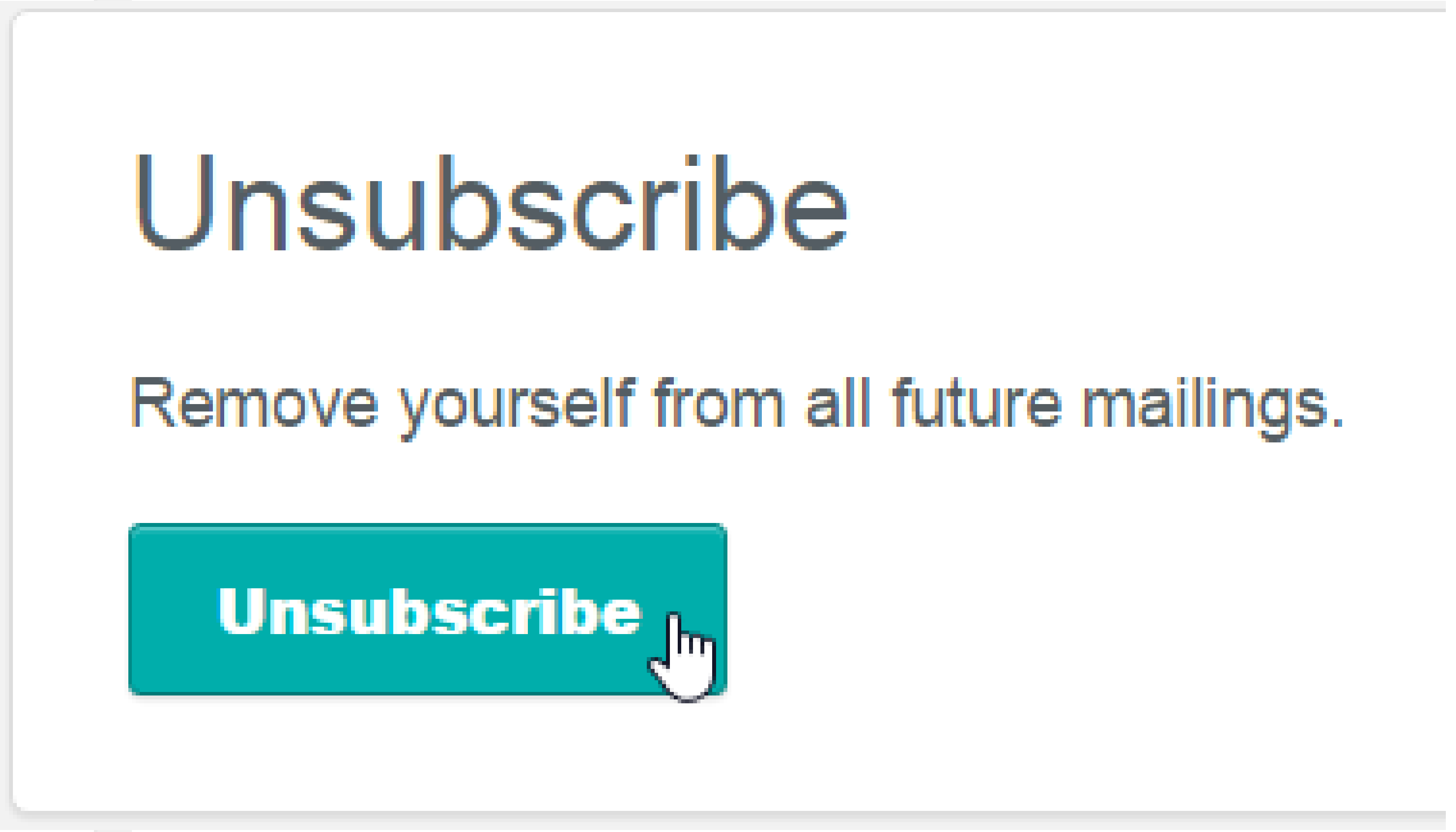
- ❑ Confirm whether your organisation needs a Promotion of Access to Information Act (PAIA) manual
- ❑ Confirm whether you are a Public or Private Body as per the PAIA
- ❑ Review the proposed contents of your manual
- ❑ Ensure your PAIA manual follows the prescribed layout and includes the necessary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

Other Considerations - PAIA



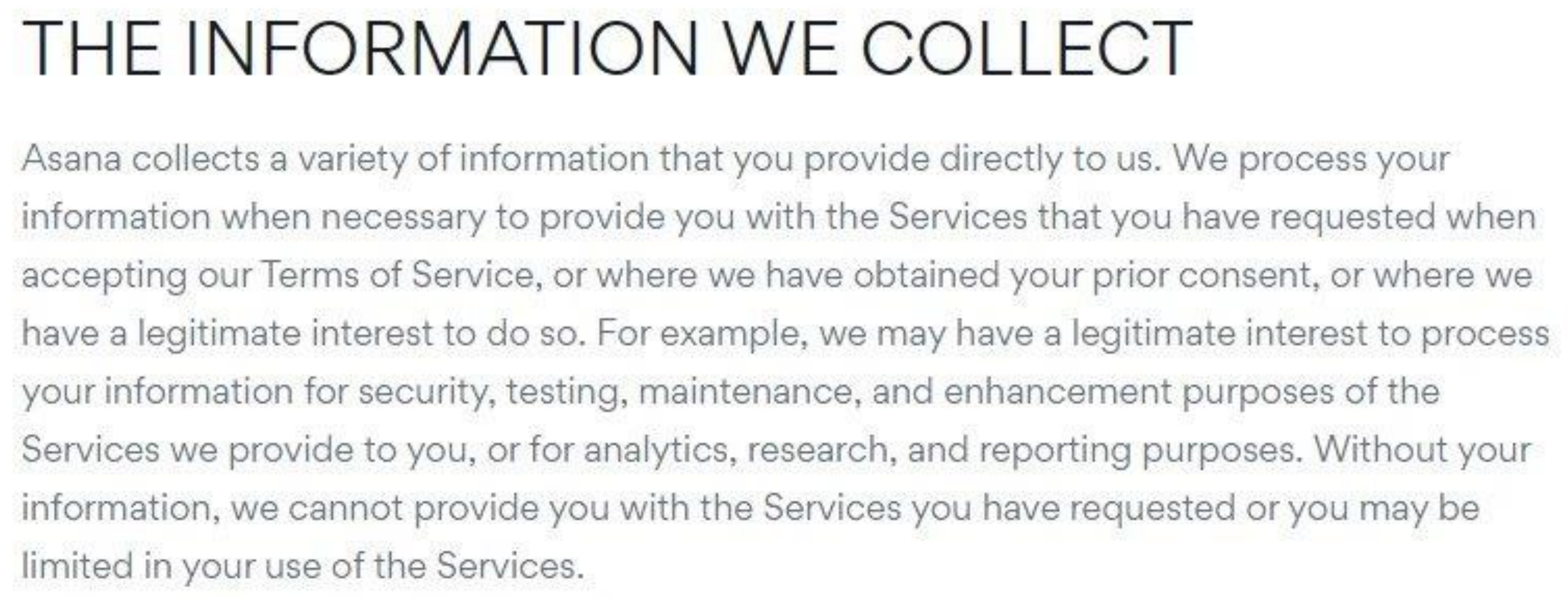
Cookie policy

We only use functional (or required) cookies that are necessary for this site to function, including those that are necessary for Google Analytics to work. We do analyse the use of this website to measure the audience but it is de-identified data. In other words, we don't know who you are.



Unsubscribe

Remove yourself from all future mailings.



THE INFORMATION WE COLLECT

Asana collects a variety of information that you provide directly to us. We process your information when necessary to provide you with the Services that you have requested when accepting our Terms of Service, or where we have obtained your prior consent, or where we have a legitimate interest to do so. For example, we may have a legitimate interest to process your information for security, testing, maintenance, and enhancement purposes of the Services we provide to you, or for analytics, research, and reporting purposes. Without your information, we cannot provide you with the Services you have requested or you may be limited in your use of the Services.

Module 5

Steps 8, 9 & 10

Compliance maintenance

Steps 8-10 – Stay compliant

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

The following items are dealt with here:

1. *Contents of these steps on the Checklist*
2. Let’s discuss:
    - Privacy by design – Privacy the new norm
    - Develop a compliance dashboard for monitoring
    - Have continuous health checks (ad-hoc)
    - Design on-going training

➢ **Quick reference to specific example: Privacy by design**

Checklist – Steps 8, 9 & 10

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

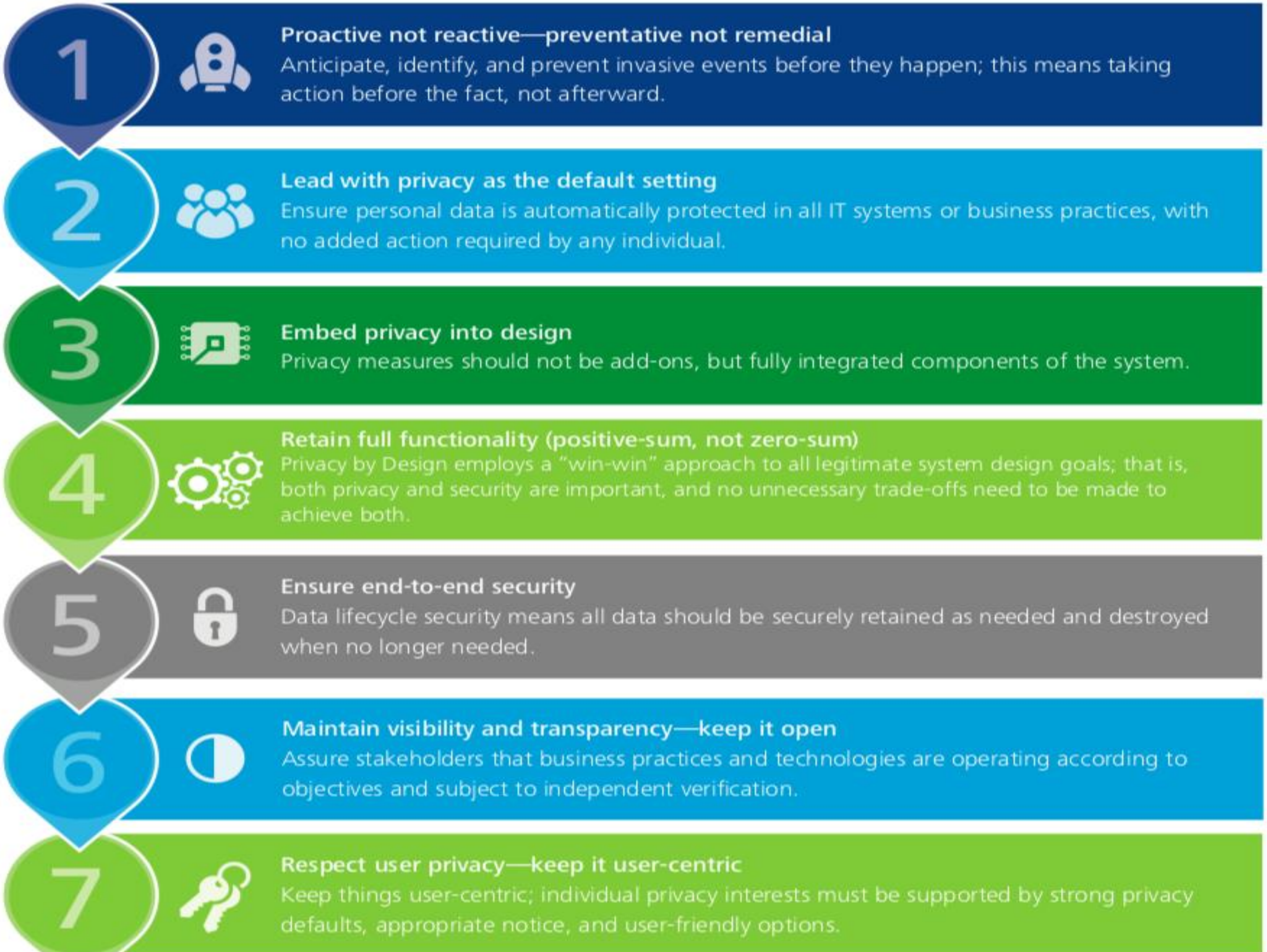
❑ Look to special needs such as the IO/DIO roles

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"

Privacy by design



Proactive not reactive—preventative not remedial
Anticipate, identify, and prevent invasive events before they happen; this means taking action before the fact, not afterward.

Lead with privacy as the default setting
Ensure personal data is automatically protected in all IT systems or business practices, with no added action required by any individual.

Embed privacy into design
Privacy measures should not be add-ons, but fully integrated components of the system.

Retain full functionality (positive-sum, not zero-sum)
Privacy by Design employs a "win-win" approach to all legitimate system design goals; that is, both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.

Ensure end-to-end security
Data lifecycle security means all data should be securely retained as needed and destroyed when no longer needed.

Maintain visibility and transparency—keep it open
Assure stakeholders that business practices and technologies are operating according to objectives and subject to independent verification.

Respect user privacy—keep it user-centric
Keep things user-centric; individual privacy interests must be supported by strong privacy defaults, appropriate notice, and user-friendly options.

SA | ACCOUNTING ACADEMY

Module 6

Step 11

Security Safeguards

Step 11 – Security Safeguards

ACCOUNTING ACADEMY
Connect. Partner. Succeed

The following items are dealt with here:

1. *Contents of these steps on the Checklist*
2. Hacks in the news…
3. Some safeguards to consider

Checklist – Step 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

NAH, I'M NOT WORRIED ABOUT CLOUD SECURITY. MY STORED DATA IS SO DISORGANIZED THEY'D NEVER BE ABLE TO FIND ANYTHING!
© D.Fletcher for CloudTweaks.com

Experian hacked, 24m personal details of South Africans exposed

By Admire Moyo, ITWeb's news editor.
Johannesburg, 19 Aug 2020

Read time 2min 00sec

See also

Momentum Metropolitan hacked

Garmin falls victim to second cyber attack in a year

Some Safeguards to consider

- 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!

✓ *Feedback from previous Q&As*

➢ *This document is available to you as a Source Document*

Access to our POPIA Experts

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

Xtreme Systems
Where customers are partners.

Assisted by:

Jacques Klopper
Director

+27 79 885 4543
jacques@xtremesystems.co.za

Karabo Letlhaku
Account Executive

+27 84 550 9798
karabol@montanadc.com

What's Next???

The following items are dealt with here:

1. You need to **complete your own Checklist for Steps 3 to 11**
   - ➢ *This Checklist is available to you as a* ***Source Document***
2. Date for the next instalment of the POPIA Compliance Series:
   - **Thursday, 8 October 2020**
   - **Step 3 - Subject Data: What must be in place on premises to physically and digitally protect the data**
     - ❑ We will discuss the easiest way that you data can be compromised as well as a the most scary...
3. *Watch your e-mail inbox to book in advance for the rest of the webinar series and receive a discount!*

QUESTIONS?

Previous FAQs

This FAQ Summary is available to you as a Source Document

Formal Q&A Session

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

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

Remember: A Q&A summary will also be uploaded to your profile

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

technicalquestions@accountingacademy.co.za

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

Thank you for your participation!

SA | ACCOUNTING ACADEMY

Your source for accounting knowledge