POPIA WEBINAR SERIES – STEP 1 & 2
THE COMPLIANCE CHECKLIST: 6 AUGUST 2020

Table of Contents

MODULE 1: INTRODUCTION & THE BASICS OF POPIA

1. INTRODUCTION

Finally! The much-anticipated POPI Act or POPIA (Protection of Personal Information Act of 2013), commenced on 1 July 2020. This Act gives effect to the constitutional right to privacy in South Africa.

The sections that make up the main body of the Act are applicable immediately, and a number of these provisions impose substantive obligations on businesses (including employers) regarding the processing of personal information. It is also important that their employees are equally aware of, and comply with these obligations when processing any such information on behalf of the employer.

Even though employers will have 12 months, until 30 June 2021, to ensure that such measures are in place, the time to act is now, and all organisations need to become compliant as soon as possible.

POPI vs POPIA

What is POPI?

POPI stands for *Protection of Personal Information*.

Regardless of whether there is a law or not, organisations should be considering what Personal Information they capture, manage and store, and how best to secure this. It makes common, logical sense that this information is sensitive, and shouldn't be exposed. One of the principles that we all should consider is "privacy by design". This means that we should consider privacy implications in all our processes and systems, and build security and privacy concepts into the day-to-day operation of our organisations. POPI is all about Privacy, and this means security. In order to secure information, organisations need to clearly understand what information is gathered and kept. This is going to require a detailed investigation and shouldn't be seen as a trivial exercise. Once understood, steps need to be taken to protect the information.

What is POPIA?

POPIA stands for the *Protection of Personal Information Act*, Act No. 4 of 2013 or POPI Act.

This is the law and is something that most (if not all organisations) will need to follow. Is there a difference between POPI and POPIA? Yes and no. POPI is the act of protecting Personal Information. This implies that all the policies, procedures, processes and practices in the organisation relating to personal information, are in fact doing POPI. You cannot "do" POPIA, as this is merely the name of the law. In summary, in order to comply with POPIA, you need to implement a POPI programme. In order to implement, there are a number of steps which need to be followed and a number of documents and instruments which need to be developed.

Which term should we use?

The Information Regulator prefers POPIA, and has requested that everyone uses POPIA when referring to the Act.

In conclusion = POPI Act is the same as POPIA

2. WHAT ARE THE OBJECTIVES OF THE ACT?

POPIA aims to give effect to the constitutional right to privacy, which is set out by the Constitution of South Africa, by introducing measures that will ensure that personal information is processed by organisations in a fair, transparent and secure manner.

The sections which will commence on 1 July 2020 are crucial parts of POPIA and brings with it the duty to comply with the conditions for processing as stipulated in terms of POPIA. This not only includes aspects in relation to lawful

processing but also security of information. It also includes how companies will deal with direct marketing going forward.

POPIA recognises in its preamble that section 14 of the Constitution provides that everyone has the right to privacy. In section 2 of POPIA it is recorded that the purpose of POPIA is to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at –

- balancing the right to privacy against other rights, particularly the right of access to information; and
- protecting important interests, including the free flow of information within the Republic and across international borders.

It is time to focus!

The South African society is able to claim the protection afforded by POPIA form 1 July 2020. The road has been long to get to this point. The problem is the road to full compliance will be very short. Companies will be required to be in full compliance with POPIA within 12 months after POPIA comes into effect. This means that entities, not only private but also public, will have to ensure compliance with POPIA by 1 July 2021.

And the Act applies retrospectively… Which means that even your information that you have NOW, must be compliant. But most people will only start worrying about compliance 12 months from now, and then it is definitely too late!

3. WHO DOES THE ACT APPLY TO?

In a nutshell…just about everybody!

POPIA impacts all South African organisations, both public and private, that collect, create, use, store, share or destroy personal information.

Private body

"private body" means-

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person, but excludes a public body;

Public body

"public body" means-

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(b) any other functionary or institution when:

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation;

The POPI Act does not stop you from processing and does not require you to get consent from data subjects to process their personal information. Whoever decides why and how to process personal information is responsible for complying with the conditions. There are eight general conditions and three extra conditions. The responsible party is also responsible for a failure by their operators (those who process for them) to meet the conditions.

The POPI Act is important because it protects data subjects from harm, like theft and discrimination.

The biggest impact is on organisations that process lots of personal information, especially *special personal information*, *children's information,* and *account numbers*. The most affected industries are financial services, healthcare, and marketing.

So, any natural or juristic person who processes personal information, including large corporates and government. The data protection laws of many other countries exempt SMEs, but not currently in South Africa. Maybe the Information Regulator will exempt some natural person and SMEs from complying. Only time will tell in this regard. Some processing of personal information is excluded.

POPIA sets the conditions for when it is lawful for someone to process someone else's personal information.

Exclusions

Some processing of personal information is excluded.

This Act does not apply to the processing of personal information:

1. in the course of a purely personal or household activity;
2. that has been de-identified to the extent that it cannot be re-identified again;
3. by or on behalf of a public body—
    - which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or
    - the purpose which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information.
4. solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression

4. THE ROLE PLAYERS

It is very important to use the correct terminology – as per the Act.

Data subject

- the person to whom the information relates
- can be a natural or juristic person

Responsible party

- the person who determines why and how to process
- can be a natural or juristic person
- *e.g. profit companies, non-profit companies, governments, state agencies and people*
- Called *controllers* in other jurisdictions

Operator

- a person who processes personal information on behalf of the responsible party in terms of a contract or mandate, without coming under the direct authority of that party
- can be a natural or juristic person
- *e.g. an IT vendor*
- Called *processors* in other jurisdictions

Information officer

of, or in relation to, a—

- public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or
- private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act

Duties and responsibilities of the Information officer:

Set out in Section 55 of POPIA

(a) the encouragement of compliance, by the body, with the conditions for the lawful processing of personal information;

(b) dealing with requests made to the body pursuant to this Act;

(c) working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body;

(d) otherwise ensuring compliance by the body with the provisions of this Act; and

(e) as may be prescribed.

Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator.

Additional Responsibilities of Information Officers:

Set out in Regulation 4

1. An information officer must, in addition to the responsibilities referred to in section 55(1) of the Act, ensure that:
   (a) a compliance framework is developed, implemented, monitored and maintained
   (b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
   (c) a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
   (d) internal measures are developed together with adequate systems to process requests for information or access thereto; and
   (e) internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

2. The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

Information Regulator

- An Information Regulator has been appointed by the President on the recommendation of the National Assembly and is answerable to the National Assembly.
- *Refer to nr 10 in this section for more detail on the Information Regulator*

5. WHAT DOES IT MEAN TO "PROCESS" INFORMATION?

"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;

6. WHICH TYPE OF INFORMATION IS PROTECTED?

Personal information is protected under POPIA.

What is included in "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;

(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;

Special personal information

This means personal information as referred to in Section 26

***A responsible party may**, subject to section 27, **not process personal information concerning**:*

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(b) the 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.

7. INTERACTION WITH GDPR

GDPR = General Data Protection Regulation

Deals with:

- Data protection of Personal data

POPIA is the South African equivalent of the European Union's GDPR. It sets some conditions for responsible parties (called controllers in other jurisdictions) to lawfully process the personal information of data subjects (both natural and juristic persons).

If your organisation is GDPR compliant, it is almost assured to be POPIA compliant as well – but you will need the formal documentation (policies & procedures) as required by POPIA to demonstrate compliance.

The table below summarises the most important differences between POPIA & GDPR:

POPIA	VS	GDPR
Protection of personal information		Protection of data
Personal information		Personal data
Child < 18 years		Child < 16 or 13 years
Data subject (natural or juristic person)		Data subject (natural person only)
Responsible party (natural or juristic person)		Controller (natural or legal person)
Operator (natural or juristic person)		Processor (natural or legal person)
Information officer		Data protection officer
Information Regulator		Supervisory Authority
Risk assessment		Data protection impact assessment
Biometric information		Genetic or Biometric information

8. PENALTIES AND FINES

This is set out in Chapter 11 of the Act.

The risks of non-compliance include reputational damage, fines and imprisonment, and paying out damages claims to data subjects. The biggest risk, after reputational damage, is a fine for failing to protect account numbers.

- **Penalties** range from R1 000 000 and/or 1 year imprisonment to R10 000 000 and/or 10 years imprisonment – depending on the severity of the offense.
- **Administrative fines** of up to R10 000 000 may be imposed by the Regulator on the responsible party – as set out in an infringement notice.

9. OTHER CONSEQUENCES OF NON-COMPLIANCE WITH POPIA TO CONSIDER

Non-compliance with POPIA can have serious repercussions for organisations, their employees and their customers.

Impact on organisation

REMEMBER: You must be able to DEMONSTRATE compliance!!!

- Financial penalties
- Criminal sanctions
- Loss of revenue resulting from negative press
- Damaged reputation
- Losing customer trust

Impact on employee

- Disciplinary action and dismissal
- Misuse of personal data
- Private or confidential data being published

Considerations for the auditors & accountants

- The need to account for provisions/contingent liabilities in terms of possible lawsuits, fines and penalties
- NOCLAR & Reportable Irregularities:
    - Especially where the auditor/accountant is performing an audit or independent review, all aspects of **NOCLAR (Non-Compliance with Laws and Regulations)** must be reported in accordance with our Codes of Conduct.
    - POPIA is yet another Act that must be kept in mind when assessing NOCLAR
    - The extent of the non-compliance must be evaluated and a possible Reportable Irregularity must always be considered (for reporting to IRBA or CIPC, as appropriate).
- The effect on the entity's solvency & going concern

10. THE INFORMATION REGULATOR

Website = https://www.justice.gov.za/inforeg/

The Information Regulator (South Africa) is an independent body established in terms of Section 39 of the Protection of Personal Information Act 4 of 2013. It is subject only to the law and the Constitution and it is accountable to the National Assembly.

The Information Regulator is, among others, empowered to monitor and enforce compliance by public and private bodies with the provisions of the Promotion of Access to Information Act, 2000 (Act 2 of 2000), and the Protection of Personal Information Act, 2013 (Act 4 of 2013).

There is a large body of staff working under the Information Regulator.

The Information Regulator's duties are varied and he/she has the power and authority to handle all matters relating to the POPIA Act.

The Information Regulator must immediately be advised in the event of a breach which resulted in Personal Information falling into the wrong hands.

11. LINKS TO RELEVANT LEGISLATION

These links and sites are useful to you in your journey to developing and maintaining your POPIA implementation.

☑ The Act

- Protection of Personal Information Act, 2013 The POPIA Act

☑ The Regulations

- *Contains 19 Forms on 44 pages re objections, requests, complaints, investigations, etc.*
- Protection of Personal Information Act, 2013 - Regulations POPIA Regulations
- Protection of Personal Information Act, 2013 - Draft regulations for comment POPIA Draft Regulations

☑ The Promotion of Access to Information Act, 2000 PAIA

☑ The Promotion of Access to Information Amendment Act, 2002 The PAIA Amendment Act

MODULE 2: POPIA COMPLIANCE CHECKLIST – WHERE ARE WE NOW?

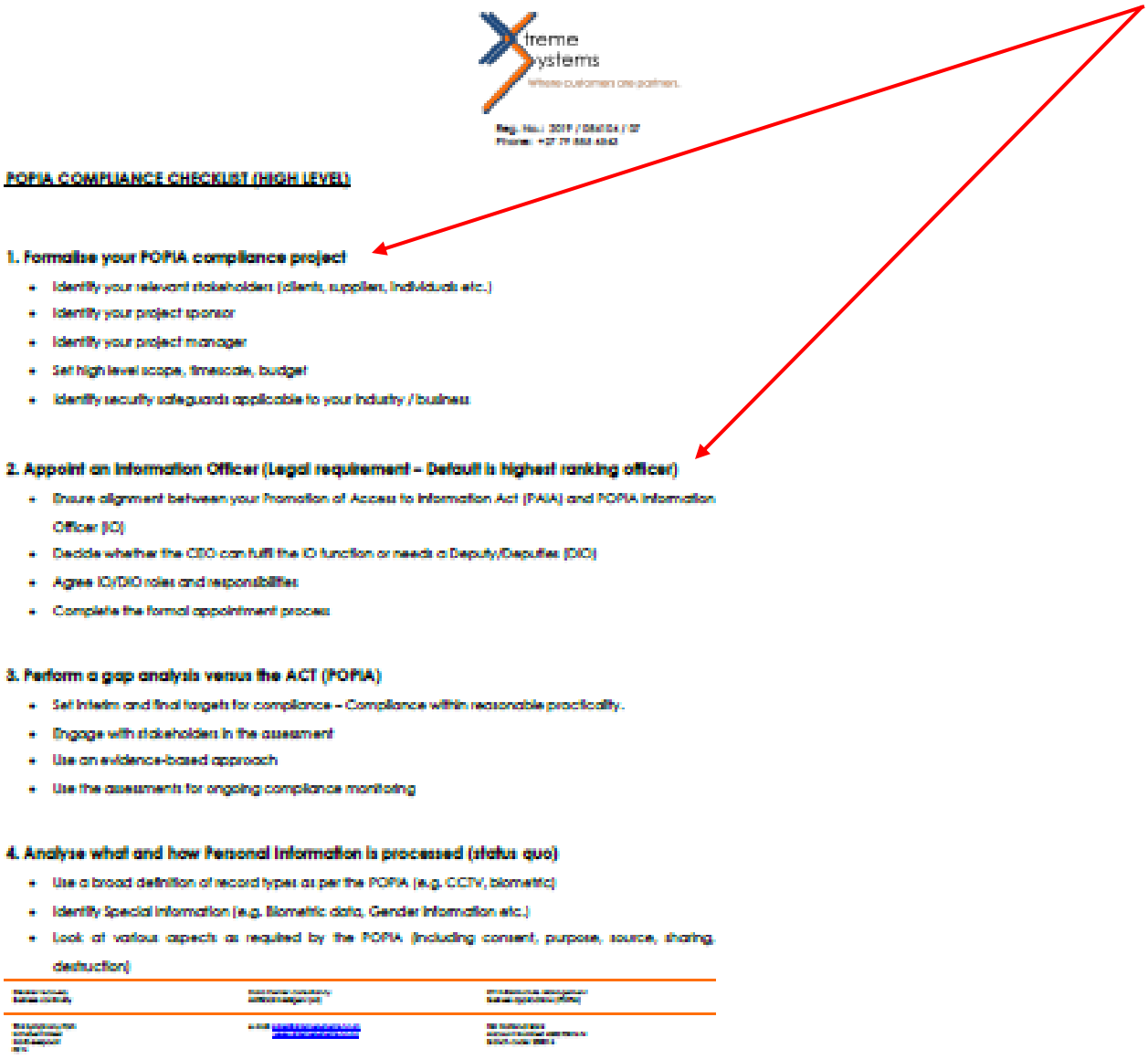
1. THE BIG PICTURE – WHAT IS INCLUDED IN THE WEBINAR SERIES?

Let's look at the entire webinar series, so that we understand where we are in the process as a whole...

Date	Webinar name *"Getting POPIA Compliant - Step xx…"*	
6 August 2020	Step 1: Completing your Checklist during this Consultative phase	**Completing your Checklist during this Consultative phase**
6 August 2020	Step 2: Appoint an Information Officer	
3 September 2020	Step 3: Perform a gap analysis versus the POPIA	
8 October 2020	Step 4: Analyse what and how Personal Information is processed (status quo)	
5 November 2020	Step 5: Review / draft POPIA compliance policies based on findings	
3 December 2020	Step 6: Review your websites & online platforms	
14 January 2021	Step 7: Update / create your PAIA manual	
4 February 2021	Step 8: Implement POPIA compliant PI management processes	
4 March 2021	Step 9: Train internal stakeholders on their roles in POPIA compliance	
8 April 2021	Step 10: Adopt POPIA compliance as "Business-As-Usual"	
6 May 2021	Step 11: Information security Safeguards	
3 June 2021	Final evaluation of your POPIA Compliance	
24 June 2021	Last-minute tweaks – emergengy changes to finalise your project	

2. WE ARE IN THE CONSULTATIVE PHASE AND WE ARE…PLANNING!

With reference to the POPIA Compliance Checklist (High Level) that was previously provided to you, we are dealing with Steps 1 and 2 in this instalment of the webinar series.



Xtreme Systems

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)

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

3. LET'S RECAP AND EMPHASIZE SOME VERY IMPORTANT ASPECTS

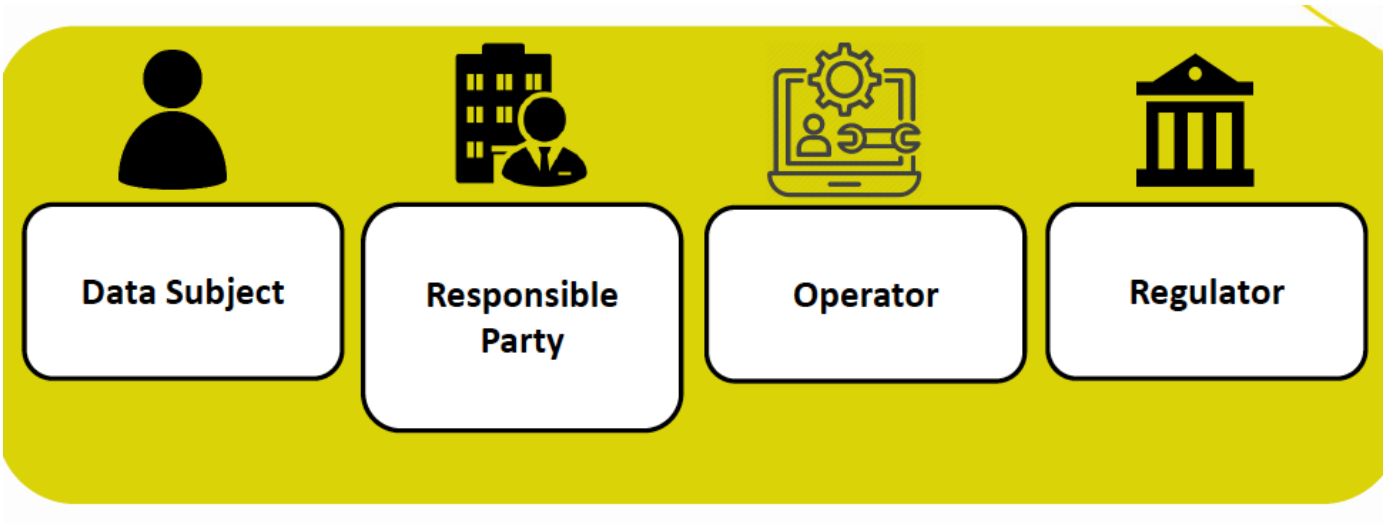
It is important to emphasize some important aspects:

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

Who are the Role Players?



Where do YOU fit in?

Responsible party (controller)

Public/ private body or any other person which, alone or in conjunction with others, determines the purpose of & means for processing personal information

Example: When you are uploading items to Google Drive, Dropbox, We Transfer, etc.

Also, as an employer that has staff under you

Operator (processor)

Person who processes personal information for a responsible party in terms of a contract or mandate without coming under the direct authority of that party – usually a service provider

Example: If you (as an accountant) are performing actions on behalf of your clients, like uploading personal information (ID docs, tax returns) to SARS, etc.

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;

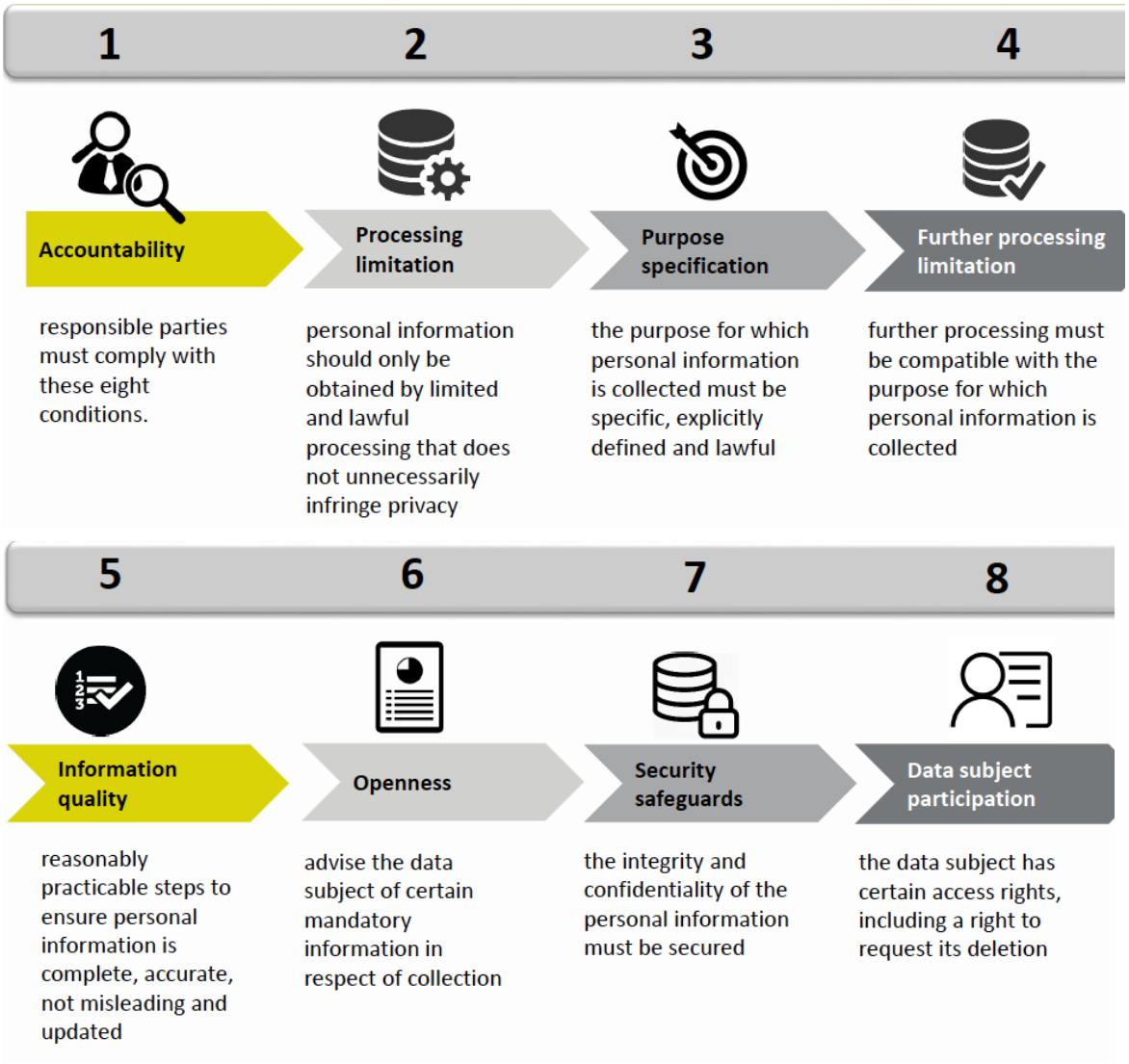
(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

Base for Scope of Work

This is discussed with reference to the 8 conditions

The 8 POPIA Conditions of Compliance



The 8 Conditions for the Lawful Gathering and Processing of Personal Information

This is set out in Chapter 3 (Part A) of the Act.

1. **Accountability**
    - Responsible party to ensure conditions for lawful processing
2. **Processing limitation**
    - Lawfulness of processing
    - Minimality
    - Consent, justification and objection
    - Collection directly from data subject
3. **Purpose specification**

- Collection for specific purpose
- Retention and restriction of records

4. **Further processing limitation**

    - Further processing to be compatible with purpose of collection

5. **Information quality**

    - Quality of information

6. **Openness**

    - Documentation
    - Notification to data subject when collecting personal information

7. **Security safeguards**

    - Security measures on integrity and confidentiality of personal information
    - Information processed by operator or person acting under authority
    - Security measures regarding information processed by operator
    - Notification of security compromises

8. **Data subject participation**

    - Access to personal information
    - Correction of personal information
    - Manner of access

MODULE 3: STEP 1 – FORMALISE YOUR POPIA COMPLIANCE PROJECT

1. 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 juristic persons.
    - Go as far back as possible (use the financial services regulation requirements on how long you should keep data).
- Save all these / file them where they can easily be found should you need to provide evidence of them.
- Create a spreadsheet where you can list to have a quick reference of how old the data is, who has access to it and where it is stored.

2. IDENTIFY YOUR PROJECT SPONSOR

- Depending on the size of the organization or where the Information Officer is the CEO, this can be an additional support to assist the Information officer in preparing for & maintaining compliance. This is a senior role player. This is not the same as a Deputy Information officer who needs to be officially delegated the duties of the Information Officer as dictated by the Act.

3. IDENTIFY YOUR PROJECT MANAGER

- Project manager is also optional, depending on the size of the organization. Reports to the Project sponsor and handles the day to day "tick box" exercises of ensuring compliance.

4. SET HIGH LEVEL SCOPE, TIMESCALE, BUDGET

- This is role is usually appointed to the Project Sponsor.
- Base on the results of (a) above, as well as the 8 conditions of compliance, draw up a scope of work, when deliverables are expected, who will do it and how frequently it will be reviewed to maintain compliance e.g. who will train staff of POPIA? How much will the training cost if outsourced? How frequently will refresher training be held? How will new staff be training on ad-hoc?

5. IDENTIFY SECURITY SAFEGUARDS APPLICABLE TO YOUR INDUSTRY / BUSINESS

- Draw up a list of all internal risks and external risks.
    - E.g. Filing cabinets containing client information is in the printing room where all staff have access to it. OR Ensure that my IT service provider is aware of the risks & penalties I face should they accidentally delete / lose my client information.
- Along each risk, identify a reasonable mitigating action e.g. move filing cabinets to a secure area and provide access to a few identified individuals. OR Revise IT services contract to reflect data protection obligation.

6. BONUS DOCUMENT – DETAILED CHECKLIST FOR STEP 1

All the above detail has been combined in an easy-to-use Checklist for your convenience.

This Detailed Checklist for Step 1 is available to you as a Bonus Document

MODULE 4: STEP 2 – APPOINT AN INFORMATION OFFICER

Remember the Legal requirement – Default is highest ranking officer!

1. ENSURE ALIGNMENT BETWEEN YOUR PROMOTION OF ACCESS TO INFORMATION ACT (PAIA) AND POPIA INFORMATION OFFICER (IO)

- When drawing up the Job description or KPIs for the Information Officer ensure that you include all the duties / responsibilities stipulated in both ACTs.

2. DECIDE WHETHER THE CEO CAN FULFIL THE IO FUNCTION OR NEEDS A DEPUTY/DEPUTIES (DIO)

- After listing the responsibilities as stipulated by the 2 ACTs, it will be clear how much will be required of the Information Officer e.g. taking calls for complaints / having to keep regular updates from the Regulator – Should this be too much for the CEO, a formal delegation, signed by both parties should be drawn.
- Deputy should be senior enough to represent the organization should they need to be in court and should be aware of the penalties associated with the role.
- Information Officer may be outsourced to an expert service provider.

3. AGREE IO/DIO ROLES AND RESPONSIBILITIES

- 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

4. COMPLETE THE FORMAL APPOINTMENT PROCESS

- 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.

5. BONUS DOCUMENT – DETAILED CHECKLIST FOR STEP 2

All the above detail has been combined in an easy-to-use Checklist for your convenience.

This Detailed Checklist for Step 2 is available to you as a Bonus Document

MODULE 5: VARIOUS "PRICKLY" ISSUES

We always try to be forward-looking and to provide you with information before you actually need it.

In this module, we will discuss some "Prickly" issues regarding practical POPIA considerations that have come to our attention.

1. THE GOOGLE & GMAIL ISSUE

Google have issued a document stating that they are compliant from their side.

Refer to the ***Google Cloud data processing amendment to G Suite v2.2 Aug 2020*** document for more detail in this regard.

☑ Visit: **https://cloud.google.com/security/compliance/south-africa-popi**

This Google Cloud document is available to you as a Source Document

2. ISSUES AROUND NON-LOCALISED PROCESSING OF DATA

GDPR = General Data Protection Regulation

Does the GDPR apply to your organisation?

- YES, if it offers goods and services to individuals in the EU?
- YES, if it monitors the behaviour of individuals in the EU?

Localised or Not localised?

POPIA applies:

- responsible party / data controller that is domiciled in South Africa and that makes use of automated or non-automated means to process the personal information. OR;
- responsible party is not domiciled in South Africa but makes use of automated or non-automated means in South Africa unless those means are used only to forward personal information through South Africa.

NB See page 5 and 6 of DLA Piper Data protection report – available to you as a Source Document

POPIA vs GDPR – a simple comparison

STANDARD	POPIA	GDPR
Application	▪ Personal information processed in South Africa	▪ Personal data of all EU data subjects, regardless of jurisdiction
Persons	▪ Juristic and natural	▪ Natural
Roles	▪ Responsible party and operator	▪ Data controller and processor AND ▪ Joint responsible parties, third parties and recipients
Penalties	▪ 10 years imprisonment or R10 million	▪ EUR 20 million or 4% of worldwide turnover
Official	▪ Information Officer to be appointed for all companies and registered with Regulator	▪ Data Protection Officer in terms of [Article 37] for certain organizations
Breach notifications	▪ "as soon as reasonably possible"	▪ Duty to report breaches to supervisory authorities within 72 hours of the breach
Privacy by design	▪ Not addressed	▪ Mandated by [Article 25]
Data protection impact assessments	▪ Not addressed in POPIA, but obligation imposed on information officer in the regulations	▪ Obligation to conduct data protection impact assessments [Article 35] where processing is likely to result in high risks for the rights and freedoms of data subjects and maintaining evidence or documentation of such assessments. ▪ Such assessments involve, inter alia identifying risks and measures to mitigate such risks and include prior consultation with the supervisory authorities.
Data portability	▪ Data subject access request - a record or description of personal information must be given "in a reasonable manner and format and in a form that is generally understandable".	▪ The right for a data subject to receive his or her data in a "structured, commonly used, machine-readable and interoperable format and the right to transmit those data to another controller". [Article 20] Data subjects can order that their data is transferred to another controller or service provider

3. PREVIOUS FAQS

This FAQ Summary is available to you as a Source Document

MODULE 6: WHAT'S NEXT?

You need to complete your Detailed Checklists for Step 1 and Step 2

Date for the next instalment of the POPIA Compliance Series

- **Thursday, 3 September 2020**

Topic:

- **Step 3 - Perform a gap analysis versus the POPIA**

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

DISCLAIMER & COPYRIGHT

1. DISCLAIMER

This work or the webinars and/or seminars related thereto are not intended to constitute professional advice. The views expressed are those of the author and the presenter. While reasonable care has been taken to ensure the accuracy of this publication and the presentation thereof, the author and the presenter expressly disclaim any liability to any person relating to anything done or omitted to be done, or to the consequences thereof, in reliance upon this work or the views expressed by the presenter. Webinar and/or seminar material is for the sole use of the participant and is the copyright of ***SA Accounting Academy***.

1. 2020 COPYRIGHT, SA ACCOUNTING ACADEMY