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	PR
Protection of personal information		tection of data
Personal information		sonal data
Child < 18 years		ld < 16 or 13 years
Data subject (natural or juristic person)		ta subject (natural person only)
Responsible party (natural or juristic person)		ntroller (natural or legal person)
Operator (natural or juristic person)		cessor (natural or legal person)
Information officer		ta protection officer
Information Regulator		pervisory Authority
Risk assessment		ta protection impact assessment
Biometric information		netic 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

12. 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

We will look at each one of these in more detail in future webinars

13. THE REGULATION OF THE PROCESSING OF SPECIAL PERSONAL INFORMATION

This is set out in Chapter 3 (Part B – Sections 26 to 33) of the Act.

- 26. Prohibition on processing of special personal information
- 27. General authorisation concerning special personal information
- 28. Authorisation concerning data subject's religious or philosophical beliefs
- 29. Authorisation concerning data subject's race or ethnic origin
- 30. Authorisation concerning data subject's trade union membership
- 31. Authorisation concerning data subject's political persuasion
- 32. Authorisation concerning data subject's health or sex life
- 33. Authorisation concerning data subject's criminal behaviour or biometric information

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**:*

> *(c) 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*

(d) the criminal behaviour of a data subject to the extent that such information relates to

(iii) the alleged commission by a data subject of any offence; or

(iv) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

Processing of personal information of children

34. Prohibition on processing personal information of children

35. General authorisation concerning personal information of children

So, YES, POPIA applies to all schools!

14. CODES OF CONDUCT ISSUED BY THE INFORMATION REGULATOR

This is set out in Chapter 7 of the Act.

- Issuing of codes of conduct
- Process for issuing codes of conduct
- Notification, availability and commencement of code of conduct
- Procedure for dealing with complaints
- Amendment and revocation of codes of conduct
- Guidelines about codes of conduct
- Register of approved codes of conduct
- Review of operation of approved code of conduct
- Effect of failure to comply with code of conduct

We will look at each one of these in more detail in future webinars

15. PROCEDURES FOR DEALING WITH COMPLAINTS

This is set out in Chapter 10 of the Act, as well as Regulation 7.

Submission of complaint

1. Any person who wishes to submit a complaint contemplated in section 74(1) of the Act must submit such a complaint to the Regulator on **Part I of Form 5**.
2. A responsible party or a data subject who wishes to submit a complaint contemplated in section 74(2) of the Act must submit such a complaint to the Regulator on **Part II of Form 5**.

Regulation 10 deals with Settlement of Complaints (by the Regulator)

16. PROVISIONS REGULATING DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATION

The Act also is aimed at providing rights to people when it comes to unsolicited electronic communications.

This is set out in Chapter 8 of the Act, as well as the Regulations.

- Direct marketing by means of unsolicited electronic communications
- Directories
- Automated decision making

We will look at each one of these in more detail in future webinars

17. GENERAL ENFORCEMENT OF THE ACT

This is set out in Chapter 10 of the Act.

- Interference with protection of personal information of data subject
- Complaints
- Mode of complaints to Regulator
- Action on receipt of complaint
- Regulator may decide to take no action on complaint
- Refe1Tal of complaint to regulatory body
- Pre-investigation proceedings of Regulator
- Settlement of complaints
- Investigation proceedings of Regulator
- Issue of warrants
- Requirements for issuing of warrant
- Execution of warrants
- Matters exempt from search and seizure
- Communication between legal adviser and client exempt
- Objection to search and seizure
- Return of warrants
- Assessment
- Information notice
- Parties to be informed of result of assessment
- Matters referred to Enforcement Committee
- Functions of Enforcement Committee
- Parties to be informed of developments during and result of investigation
- Enforcement notice
- Cancellation of enforcement notice
- Right of appeal
- Consideration of appeal
- Civil remedies