POPIA IN A NUTSHELL
WEBINAR MATERIAL: 9 JULY 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: THE MORE DIFFICULT PARTS OF THE ACT

These are the sections that you might need some outside help on…not the understanding thereof, but the application of the requirements and the practical implementation…

1. 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

2. 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!

3. 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

4. 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)

5. 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

6. 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

MODULE 3: OBLIGATIONS PLACED ON EMPLOYERS

1. GENERAL COMPLIANCE WITH POPIA

Werksmans article – 26 June 2020

With effect of 1 July 2020 a number of material provisions of the Protection of Personal Information Act 2013 ("POPIA") will come into operation.

A number of these provisions impose substantive obligations on businesses (including employers) regarding the processing of personal information.

Positive obligations are placed on employers to, among others, ensure that they comply with the provisions of POPIA regarding the processing of their employees', customers' and service providers' 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.

Employers will have 12 months, from 1 July 2020, to ensure that such measures are in place.

It is important that adequate provisions be inserted into contracts of employment and that workplace policies and procedures are implemented to ensure compliance with POPIA.

These should include:

a) The designation of an information officer;

b) Procedures ensuring information is processed in a lawful manner;

c) Ensuring that the processing of personal information is done in accordance with the eight conditions provided for in the legislation;

d) Obtaining consent from employees for the processing of their personal information;

e) Providing training and information to human resources practitioners as well as employees in order to ensure that information is processed lawfully and that employees, as 'data subject's, are aware of their rights;

f) Putting in place measures to ensure the processing of 'special personal information' is lawful; Dealing with any cross-border processing of information; and

g) Implementing procedures to address and deal with any complaints from, among others, employees regarding the processing of their personal information;

Consideration may also be given to obtain legal assistance with preparation and/or reviewing of abovementioned and to advise on all aspects of POPIA.

2. RETENTION PERIODS FOR PERSONAL INFORMATION

This is set out in Section 14 of the Act

1. Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless-

    (a) retention of the record is required or authorised by law;

    (b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention of the record is required by a contract between the parties thereto; or

(d) the data subject or a competent person where the data subject is a child has consented to the retention of the record.

2. Records of personal information may be retained for periods in excess of those contemplated in subsection **(1)** for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.
3. A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must-

    (a) retain the record for such period as may be required or prescribed by law or a code of conduct; or

    (b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

4. A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2).
5. The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.
6. The responsible party must restrict processing of personal information if-

    (a) its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;

    (b) the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;

    (c) the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

    (d) the data subject requests to transmit the personal data into another automated processing system.

7. Personal information referred to in subsection (6) may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.
8. Where processing of personal information is restricted pursuant to subsection (6), the responsible party must inform the data subject before lifting the restriction on processing.

3. SAFEGUARDING THE INFORMATION THAT IS COLLECTED

This is set out in Sections 19 to 22 of the Act

- ☑ 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

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

- How to inform the Information Regulator of any security breach?
- How to inform the Data Subject that their personal information has been compromised?
- Which procedures are followed when sharing personal information with an external operator?
- Which procedures are followed when sharing personal information with an external operator?
- How are safeguards continually updated?
- How are we alerted when personal information is accessed or modified without authorisation?
- How to determine which employees are permitted access personal information and what information they are permitted to access?
- How do we establish and maintain appropriate safeguards against the identified risks?
- How to prevent personal information from falling into unauthorised hands?
- How to identify any foreseeable internal and external risks to personal information?

SAAA will host a separate webinar on this in the nearby future

MODULE 4: WORKPLACE POLICIES & PROCEDURES

1. DO WE REALLY NEED ANOTHER MANUAL?

The answer is YES! Most definitely! As stated previously, this is the responsibility of the Information Officer.

A **POPIA Manual** will ensure that you document your workplace policies and procedures, and also set out how you can demonstrate compliance with the Act and Regulations.

Almost every bit of information that we have included and eluded to in this webinar material, you will have to include in your policies & procedures Manual.

It will also function as an important tool in training all your staff on the requirements, implications, implementation and consequences of POPIA.

SAAA will be able to assist you with this in the nearby future.

2. WHEN AND HOW TO ASK FOR CONSENT UNDER THE POPIA

Some of the POPI experts have dubbed ***consent*** the c-word, mostly because it is misunderstood and abused so often.

Here's why. Whenever someone asks me for my consent, I immediately think that whatever they want to do will be intrusive or unexpected, it's like asking consent to do a credit check or to load a debit order on to my bank account. Serious stuff.

In terms of the POPIA, consent is one of the six lawful grounds for processing personal information and in most cases consent is not the appropriate justification for processing.

If consent is difficult, rather use an alternative. And if you go ahead and ask for consent, knowing that you would still process the personal data, asking for consent would be misleading and inherently unfair. We also do not advise you to make consent a precondition of a service as it is unlikely to be the most appropriate justification.

What are the other lawful grounds for processing personal information?

Now that we know that asking for consent is not the only justification for processing personal information, let's look at other lawful grounds for processing personal information. We can lawfully process personal information if

- it is necessary to conclude or perform in terms of a contract
- we need to comply with an obligation imposed by law
- we are protecting the legitimate interest of a data subject
- it is necessary for the proper performance of a public law duty
- we are pursuing the legitimate interest of the responsible party or of a third party

Only if we're certain that we cannot rely on any one of the above grounds we consider asking for consent.

It is appropriate to ask for consent if you can offer someone not only a real choice, but also the opportunity to control how you use his or her information. This will also help to build a trusting and engaging relationship. However, if you cannot offer a genuine choice, consent will never be the appropriate basis for processing someone's personal information.

What do we need to know about asking for consent?

If you must ask for consent, then make sure your consent is:

- **specific** – the consent must relate to a specific processing purpose
- **informed** – you must give the person (data subject) enough information about the consent before he or she has to make a decision about whether to give consent or not
- **explicit** – the data subject must give consent through a clear, specific, and affirmative act. The consent must be distinct from any other action. A good example would be to give consent to receive direct marketing. If I purchase a product from an online store, my consent to receive direct marketing from that store cannot be hidden in the purchasing contract.

Remember that the data subject can withdraw his or her consent at any time. You must be ready to act on such a withdrawal.

IF YOU HAVE TO ASK, DO IT PROPERLY.

Make sure your request for consent:

- is separate from any other contract that may apply;
- is in an opt-in format, this means that you should stay clear of any pre-ticked boxes or any type of default consent;
- is written in plain language;
- provides specific information about the processing activity to which it relates;
- has your organisation's details and those of any third party you will be sharing the information with;
- allows a person to consent separately for different purposes and types of processing; and
- informs a person that they are entitled to withdraw consent and the process they must follow to do so.

How do you manage consent?

Please look at these tips to manage consent effectively. You must:

- have a process in place to update your consents regularly
- allow data subjects to withdraw their consent at any time; for example, if they unsubscribe
- remove data subjects from your contact list when they unsubscribe
- not penalise data subjects when they withdraw their consent

If you are wondering whether your request for consent is unnecessary or (gasp) unfair, get in touch with a specialist and they will help you make sure it's not.

SAAA will host a separate on this in the nearby future.

3. WHAT STEPS WILL YOU HAVE TO TAKE TO COMPLY?

Responsible parties will have to take various steps to comply.

Here is one simplistic example:

1. Appoint an Information Officer.
2. Draft a Privacy Policy.
3. Raise awareness amongst all employees.
4. Amend contracts with operators.
5. Protect the information that you are privy to!

6. Report data breaches to the regulator and data subjects.
7. Check that they can lawfully transfer personal information to other countries.
8. Only share personal information when they are lawfully able to.

SAAA will facilitate help with this function by connecting you with an expert consultant

4. HOW TO START YOU POPIA COMPLIANCE PROGRAMME

Article by "A lady who was a lawyer in her previous life"

It's week 5 000 of the national lockdown, so we reckon everyone will appreciate a change of focus (since we can't change the scenery). From what we can tell, most people's pace during lockdown is either crazy-busy or bored-to-tears. So, for those of you leaning towards the bored spectrum, here are seven things you can do to kickstart your POPIA compliance project – even during a worldwide pandemic.

1. Assemble a project team

Identify the following members (at least) to form part of the team:

- Executive sponsor: This person will authorise the project and control the budget.
- Business lead: This person will be responsible for the day-today management of the project. (This is you, right?)
- Risk, compliance and legal: You will need someone from each of these areas to provide advice. Wondering why? There should be an interdisciplinary approach to your data protection.
- IT lead: This is a key stakeholder because they are often responsible for information security management.

2. Do an information governance (IG) maturity assessment

Ask everyone on the project team, and maybe a few other senior managers, to complete an Information Governance Maturity Assessment. If you rate below 3, you need to focus on other areas of your business before you can move on to POPIA compliance. You need to know how to interpret the results.

Refer to the section on Information Governance in Module 5 below

3. Work out a high-level project plan

We usually start POPIA compliance projects with the following steps:

- Determine the aim of the compliance project.
- Identify the high-level POPIA compliance risks.
- Agree on priorities for the project.
- Agree on your risk appetite.
- Define roles and responsibilities.
- Draft a POPIA Compliance Framework.

4. Work out a budget

Once you have an idea of what needs to happen and who will be on the team, you can get a sense of how much outside help you'll need to get the ball rolling. Ask a few service providers for quotes. The lockdown is the perfect time to have these conversations.

5. Do a preliminary investigation

Set up some time with senior managers and get a sense of where and how your organisation uses personal information. You can start by asking these questions:

- What customer information do you collect?
- How do you collect it?
- Where is it stored?
- What employee information do you have and where do you store it?
- What services providers do you use that have access to your customer or employee information?
- Do you do direct marketing? How?
- Do you sell datasets that contain personal information?

6. Review your current policies

Get copies of all your information governance and information security management policies and review them. Do they include anything relating to the protection of personal information? If not, add time for policy development to your project plan. You should include the list of the additional policies to develop and the current policies that need an update in your POPIA Compliance Framework.

7. Draft your POPIA Compliance Framework

The framework should:

- Define the aim and principles of your POPIA compliance programme.
- Identify the roles and responsibilities within the programme.
- Include a policy development and alignment plan.
- Set out a policy implementation plan.
- Describe your approach to risk assessments.
- Describe your approach to compliance monitoring.

8. Last, but not least

Stay safe and healthy! Don't start your POPIA compliance project now just for the sake of being productive during lockdown.

It's okay if POPIA is not your *first* priority at the moment – but it needs to become a priority and part of your next 1-year plan!

5. FAST-TRACK YOUR POPIA IMPLEMENTATION

By adopting the following key accelerators, organisations can fast-track their POPIA implementation:

1. **Secure accountability with relevant executives**

   Accountability is critical for any privacy programme to succeed. It is important for organisations to determine their view of privacy and how they plan to comply with the regulatory requirements. Based on this, agree on a number of key objectives that can be further developed into a strategy and framework to drive the implementation project.

2. **Allocate the Privacy Officer role**

By default, the head of the organisation is the Privacy Officer. However, POPIA allows for this role to be delegated. Decide now who will be responsible – will it be the Compliance Officer, Head of Risk or somebody else in the organisation? Take this individual on the journey from the start.

3. **Follow a risk-based approach**

   Many POPIA programs have been derailed due to teams trying to implement the requirements of POPIA without considerations of their unique business context. A risk-based approach to POPIA compliance, agreed with the Board or Steering Committee, will ensure focus remains on prioritising the most important POPIA compliance requirements first.

4. **Integrate with existing compliance structures**

   POPIA is a compliance requirement and much effort can be saved by integrating it into existing compliance structures and processes, such as compliance management, risk management, internal audit and audit and risk committee reporting. Without an appropriate compliance process in place, it may be challenging for organisations to drive POPIA in isolation.

5. **Align with other initiatives**

   It is important to coordinate your POPIA initiatives with related initiatives within your organisation, particularly in areas such as cybersecurity, data classification and PCI compliance to avoid unnecessary duplication of effort and ensure alignment to business objectives.

6. **Drive behavioural change through training and awareness**

   Change management is a critical part of embedding privacy into the culture of the organisation. Through training and awareness, the culture of the organisation can embrace change in how they handle data, which then results in changed behaviours.

7. **Get help outside the organisation**

   Develop a risk-based and prioritised implementation plan. Look inside for skills, but reach out for assistance from professionals, such as those with multi-disciplinary teams between privacy, legal, data, advisory and cyber security specialists where you don't have the skills within your organisation.

6. 10 KEY QUESTIONS YOU SHOULD BE ASKING

1. Where do I start?
2. How can I prioritise my implementation activities to comply with POPIA?
3. What is the POPIA impact for my organisation?
4. What data do I process and why?
5. Where is data stored?
6. Who do I share data with and why?
7. Is my data secure?
8. How do I maximise the value of my data in a legally compliant way?
9. Is my organisation affected by other privacy laws in countries I operate out of?
10. **Do I need HELP to answer some of the above questions?** ***If YES, then contact a specialist!!!***

MODULE 5: WHAT'S NEXT?

If it turns out that you are ready for POPIA, the first step is always to draft a POPIA Compliance Framework and to check whether you have the right policies.

If you are not ready, take a deep breath. Doing POPIA just for the sake of doing it by the effective date, is not a good idea. Firstly, because you probably have bigger things to worry about. Secondly, you will end up frustrating the heck out of your organisation and wasting precious time, resources and money on false starts. Record the results of your information governance maturity assessment and create a strategy to address the deficiencies. By all means, include POPIA in that picture, but make sure that it is in the right place.

1. CREATING TRUST IN A DIGITAL WORLD

Data protection is at the forefront of the minds of boards, customers, users, and regulators.

How you use data in the digital economy will require you to understand the connections between business, technology, people and regulation.

Using the relevant experts outside your business, can help you assess your privacy risks and deploy privacy transformation initiatives that resonate with your unique business priorities and risks while managing regulatory change.

2. INFORMATION GOVERNANCE

Information governance can be defined as 'the activities and technologies that organisations employ to maximise the value of their information while minimising associated risks and costs.'

A more complex definition is 'an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.'

You should assess your entity's Information Governance, or better yet – **get an OUTSIDE SPECIALIST TO HELP YOU**.

You can use an assessment to measure your information governance progress, by using e.g. an **Information Governance Maturity Assessment**.

- *A 9-page Assessment has been included in your Source Documents – feel free to use it, if you have spare time and capacity.*
- Read the description of the principle of good information governance (IG) and choose the level that best describes your business.

Let's ask ourselves: 'Why do so many POPIA projects fail?' and 'What can we do at the beginning of projects to head trouble off at the pass?'.

After a lot of trial and error, this is our answer:

- do an information governance maturity assessment,
- pay attention to the results, and
- pick the right project for your organisation (hint, it might have nothing to do with POPIA).

Why are we talking about Information Governance?

With all the hype around POPIA and data protection, organisations are forgetting that personal information is not the only class of information that is essential for doing business. For many organisations, personal information won't

even be the most valuable information they use. Measured in Rands and cents, their intellectual property may be more valuable.

Here are some other forms of information:

- all intellectual property (trademarks, designs, inventions, trade secrets, know-how, content or publications the organisation created, technical documents)
- information on the organisation's website
- financial information
- contracts and information about contract negotiations
- strategies and plans
- policies and procedures
- internal memoranda, minutes of meetings and agendas
- emails
- research and statistics
- personal information of customers and prospective customers (leads), employees and employment candidates, suppliers and service providers.

Information governance is often referred to as a 'super-discipline'. It includes records management, information security, risk management, compliance management, legal and e-discovery issues, IT governance, data governance, privacy, corporate governance….

What is an Information Governance Maturity Assessment?

Information governance maturity assessments help organisations to spot areas that are in need of improvement. Specialists also use it to assess whether an organisation is ready for a POPIA project.

Refer to the Information Governance Maturity Assessment included in your Source Documents

Who should complete it?

Resist relying only on your perspective, because information governance is multi-disciplinary.

Ask stakeholders across the organisation to complete the information governance maturity assessment. Get perspectives from IT, legal, compliance and risk management, human resources, sales, operations, executive management, information security and records management. The more the merrier!

What do the results of an Information Governance Maturity Assessment mean?

Refer to the document included in your Source Documents

3. KNOWLEDGE IS POWER!

Knowledge is power!

And training your staff on POPIA is vital AND legally required!

The best advice is this – If you can, use an external specialist that understands your needs and will see you through every step of the way…and beyond!

What can you do? Increase your knowledge on POPIA by reading relevant information, and speaking to consultants.

You will need to inform and train your management team on the following:

- An overview of the laws that your organisation must comply with.
- How your organisation currently complies.
- How big is the impact?
- Your current maturity?
- What is the timeline?
- What could happen if you do not comply?

Your management team will be vital in ensuring that compliance filters via the top-down approach.

Helping you to help your clients with POPIA Compliance

SAAA will be hosting a POPIA webinar every month to ensure that you have access to the best information summaries and access to relevant experts to help you with POPIA compliance!

- **This will include e.g. a Compliance checklist, as well as other helpful tools that you can implement in your own organisation, as well as for your clients**
- **Special discount for SAAA patrons when using expert consultants that you will need to implement and maintain POPIA**

MODULE 6: 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***.

2. 2020 COPYRIGHT, SA ACCOUNTING ACADEMY