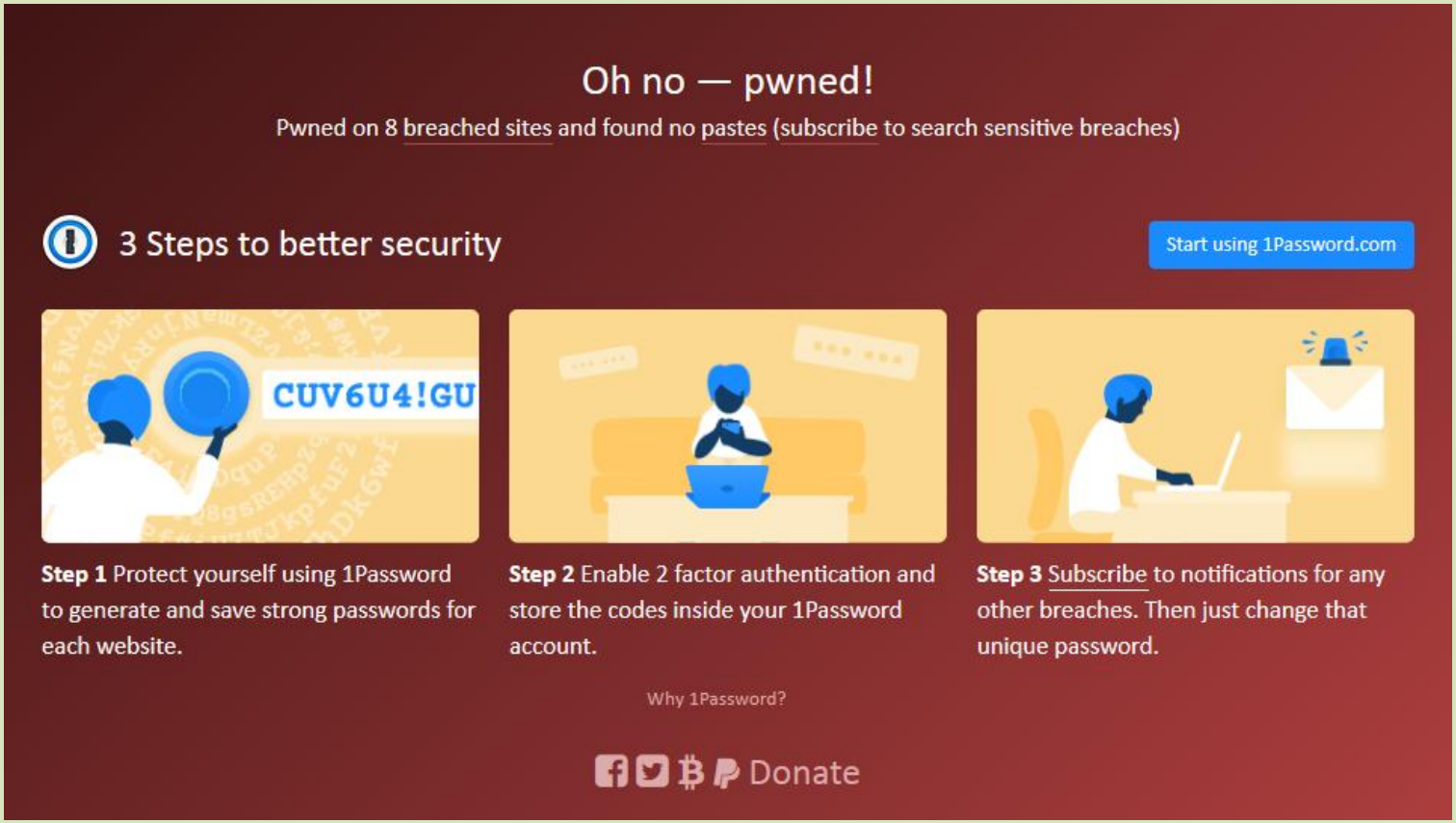
Implications and Compliance of the Protection of Personal Information (POPI) Act

11 February 2020

associates
HOPKINS
COETZEE
YOUR HR BUSINESS PARTNER

Test

- **Go to https://www.haveibeenpwned.com** Enter any of your email addresses to see whether they've already been exposed to hackers.



Presentation overview

- Background
- What is the POPI Act
- Definitions and key concepts
- Non-compliance to POPI Act
- Pre POPI Act: Practices of accessing information
- Compliance to the Act
- Institutional Risks of access to personal Information
- Implementation timeline
- Recommendations to implementation
- Handout
- Q&A

What is the POPI Act all about?

- The POPI Act aims to encourage the **protection of personal information that is processed by both public and private bodies**. To do this, the Act will introduce certain **conditions** that will establish the **minimum requirements** that businesses must comply with when processing personal information.

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

  Basically, it's a code of conduct that **all businesses must comply with.**

When will the Act be implemented?

- While the Act hasn't been implemented just yet, it's fair to assume that it *will be* some time this year. Once the Act is in place, parties will be given a **one-year transition period** to comply — but the roll-out of a comprehensive POPI compliance plan can take between six months and two years to finalise. So if you haven't already — you'd best start working on it!

'Regulator wants POPIA in force by Q2 2020 - ITWeb, 27 January 2020'

What counts as ‘personal information’?

In terms of the Act, personal information is data that can be **used to identify a person**. It is defined as “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.” This information about a person includes, but is not limited to:

- Race
- Gender
- Sex
- Pregnancy
- Marital status
- National / ethnic / social origin
- Colour
- Sexual orientation
- Age
- Physical or mental health
- Disability
- Religion / beliefs / culture
- Language
- Educational / medical / financial / criminal or employment history
- ID number
- Email address
- Physical address
- Telephone number
- Location
- Biometric information
- Personal opinions, views or preferences

What counts for ‘special personal information’?

- Religious or philosophical beliefs
- Race or ethnic origin
- Trade union membership
- Political persuasion
- Health of sex life
- Biometric information

Who will the POPI Act affect?

- Put simply — just about everyone.

  All companies will be affected by the Act, but in particular, companies that deal with a large amount of personal information — think banks, insurance companies, medical aids, etc.

  However, *all* companies need to have **systems in place to deal with personal information**. Plus, the POPI Act also has guidelines about direct marketing — so any brand sending messages or emails to consumers without them opting in, beware!

How will the POPI Act affect my business?

- Firstly, it will affect **the way you manage information**. You'll need to classify any consumer data that you hold and identify whether it constitutes as 'personal information'.

  You'll also be required to **identify any 'records' and 'sensitive' information you might hold** — remember that there is different criteria for handling personal information and non-personal information.

  It will also affect **the way you notify stakeholders**. Third parties will have to be notified as soon as possible if there is a privacy breach and personal information is compromised.

Why should I comply with the Act?

- Well, for starters — it's the law.

  Also, there are other benefits to complying with the Act. According to *POPI.biz*, consumer studies have shown that in 90% of cases, **consumers would rather do business with companies that are transparent and comply with legislation than any other business**.

  Let that sink in.

Your concern with data privacy compliance

- According to the third biennial **Ernst & Young 2018 Global Forensic Data Analytics Survey**, respondents indicated only 33 percent have an established plan for GDPR compliance, with another 39 percent signifying they are unfamiliar with the GDPR.
- While Europeans naturally are more aware and prepared — with 60 percent having a GDPR compliance plan in place — other regions have more work to do: Africa and the Middle East (27 percent), the Americas (13 percent) and Asia-Pacific (12 percent).
- The primary principle behind the GDPR is that it views personal data as the property of the individual, not data controllers or processors.

https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance

Our Approach: Risk Management

Risk Category	Possible Risks Areas		
Strategy	• Planning • Business Portfolio • Management Activity • New Business/Growth Opportunities	• Strategy Development • Business Performance Management • Target Setting/Vision/Goals • Investor Relations	• Joint Venture Mgt • Rationalisation • Communicaiton of strategic direction set b Board
Human Resources	• Workplace Industrial Relations • Employment Practices • Remuneration and Entitlements • Succession Planning	• Recruitment and Retention • Workers Compensation • Skills availability/Training and Development • Leadership • Diversity	• Employee Safety and Health • Performance Incentivisation • Communication • Contractors / 3rd parties
Information Technology	• Data Management • Data Security • Systems Development / New systems	• Systems Maintenance • Availability • Data Integrity • Service delivery	• 'e' Commerce • Outsourcing manageme • Interface with 3rd partie • Sharing of classified inofrmation
Marketing	• Competitive Positioning • Market Research • Image • Trademarks • Strategic alliance networks • Pricing / Costing	• Patents • Reputation • Customer Service • New Products • Project management	• Research and Development • Product portfolio • Product Liability • Obsolescence • "e" Commerce

Our Approach: Risk Management

Risk Category	Possible Risks Areas		
Supply Chain / Distribution	• Logistics • Purchasing/procurement	• Inventory Management • Contract Management	• Import Clearance • Continuity managemen
Environment	• Regulatory Compliance • Contamination	• Loss of Containment • Complaints Management • Handling Image/ reputation	• Community / Governm Relations
Legal	• Regulatory Compliance • Commercial Relationships	• Acquisitions/Divestments • Intellectual Property	• Competition Law • Contractual Obligations
Finance	• Funding / Treasury • Investments • Taxation	• Debt Management • Supplier Payments • Capital Expenditure	• Financial Controls and Reporting • Fraud • Insurance
Physical Assets	• Security • Natural Disaster	• Fire • Explosion	• Impact • Capital Expenditure
Operations	• Manufacturing upscaling • Technical Engineering	• Capacity Planning • Costs of upscaling to Production	• Reliability Managemen & partners • Safe Operations
Government	• Sovereignty • Politics • War	• Legislative Change • Corruption • Terrorism	• Tax law change • Change to party in pow
Economics	• Interest Rates	• Commodity	• Currency

Key Role Players for POPI

Data subject	• The person to whom PI relates
Responsible party	• Public or private body or any other person which determines the purpose of and means for processing PI
Operator	• Person who processes PI for a RP in terms of a contract or mandate, without coming under the direct authority of that party
Competent person	• Any person legally competent to consent to any action or decision being taken in respect of any matter concerning a child
Information Regulator	• A juristic person established in terms of the Act accountable to the National Assembly and appointed by the Minister of Justice

The Core - 8 Conditions of POPI

Accountability	•RP to ensure conditions for lawful processing
Processing limitation	•Minimality – adequate, relevant and not excessive •Consent, Justification, Objection •Collection directly from Data Subject
Purpose specification	•Specific, explicitly defined and lawful purpose •Records of PI must not be retained longer than is necessary for achieving the purpose •Exemption: record required by law, historical, statistical or for research •Destroy/delete/de-identify a record of PI once purpose achieved
Further processing limitation	• To be compatible with original purpose of collection if not, consent for further processing is required

The Core - 8 Conditions of POPI

Information Quality	•RP must take steps to ensure PI is complete, accurate and not misleading
Openness	•Records of the processing cycle for operations must be maintained and made available to the DS •Obligation on RP to notify the DS upon collection of PI
Security Safeguards	•Integrity and confidentiality of PI must be maintained to prevent loss, damage, unauthorised destruction, unlawful access or processing •Operator must notify RP if there are reasonable grounds to believe that the PI was accessed by an unauthorised person and the RP has to notify the Regulator and the DS
Data Subject participation	• Right to be informed - DS can be requested free of charge if PI held •Where DS requests copy of the record, the RP can charge a fee •DS can request correction or deletion of PI that is inaccurate, irrelevant, out of date, excessive, incomplete, misleading or unlawfully obtained

These conditions are largely based on the principles contained in the *CoE Convention, OECD Guidelines and the EU Directive*.

Condition #1 - Accountability

- Section 8 – The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

  Ask yourself this:
  1. Is there currently an individual / a department responsible for overall information security compliance?
  2. Is each department currently being monitored with information security standards?

Plan of Action – The Information Officer

DUTIES AND RESPONSIBILITIES OF INFORMATION OFFICER

(1) An information officer's responsibilities include -

(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.

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

Sec. 56 provides for the designation & delegation of deputy information officers.

Condition #2 – Processing limitation

Sec 9-12: PERSONAL INFORMATION MAY ONLY BE PROCESSED IF:-

(a) the data subject ***consents to the processing; or***

(b) processing is ***necessary to carry out actions*** *for the conclusion or* ***performance of a contract*** *to which the data subject is party; or*

(c) processing ***complies with an obligation imposed by law*** *on the responsible party; or*

(d) processing ***protects a legitimate interest of the data subject****; or*

(e) processing is necessary for the proper performance of a ***public law duty by a public body;*** *or*

(f) Processing is necessary for **pursuing the legitimate interests of the responsible party or of a third party** to whom the information is supplied.

In layman's terms

- That personal information is processed in a **lawful manner** that does not **unreasonably infringe upon the privacy** of the individual to whom the personal information relates (clause 8)
- That only the **minimum amount of personal information** be processed as is relevant to **achieve the purpose for which it is required**. An organisation may not request more information than is necessary to achieve a particular purpose (clause 9)
- That the **explicit consent of the individual** is obtained prior to the processing of personal information. If the individual **objects** to such processing, the organisation may not continue with the processing of that information (clause 10)
- That the organisation must collect the personal **information directly from the individual except in situations that are specifically excluded** from the Act, for example, if the information is contained in a public record or was deliberately made public to the purpose for which it is needed.

Ask yourself this…

1. Is there a formal policy for the processing of personal information.
2. Does your policy for processing of information identity the basis in terms of which the information may be processed? (e.g. consent, legislation, contract?)
3. For which purposes does your business process the different categories of information?
4. How does your business assess whether the type of personal information is adequate for, and relevant to, the purpose for which it is collected?
5. How does your business ensure that the type of information requested and provided is not excessive for its purpose?
6. Does your business have procedures in place for de-identifying personal information?
7. Does your business obtain the consent of individuals before processing their personal information?

Ask yourself this…

8. When is consent obtained?
9. How is consent obtained?
10. Does your business record instances of non-consent?
11. Does your business supply personal information to third parties?
12. If yes, does your organisation obtain consent from the relevant individual to supply their personal information to third parties?
13. Does your business obtain personal information directly from the individual concerned?
14. Does your business use intermediaries or agents to collect personal information?

Condition #3 – Purpose Specification

1. Sec 13-14: Steps must be taken to ensure that the **data subject is aware of the purpose** of the collection of the information.
2. **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 is required or authorised by law;

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

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

   (d) the data subject has consented to the retention of the record.
3. Records of personal information may be retained for periods in excess for **historical, statistical or research purposes** if the responsible party has established appropriate safeguards against the records being used for any other purposes.
4. A responsible party must **destroy or delete a record of personal information or de-identify it as soon as reasonably practical** after the responsible party is no longer authorised to retain the record.
5. The destruction or deletion of a record of personal information must be done in a manner that **prevents its reconstruction**.

In layman's terms

1. Ensure that personal information is only processed for **specific, explicitly defined and legitimate reasons** relating to the functions or activities of the organisation;
2. Take steps to make the **data subject** (person whose personal information is being processed) **aware of the purposes** for which the personal information will be processed; and
3. Establish mechanisms to ensure that **personal information is only kept for as long as it is required** to fulfil the purpose for which it was collected.

Ask yourself this…

1. For which purposes does your business collect personal information?
2. Does your business classify personal information in terms of the purpose for which it is processed?
3. Does your business inform relevant persons about the specific purposes for which their personal information is required?
4. Does your business clearly identify the names and categories of all people and organizations to whom the information will be supplied?
5. When and how does your business inform relevant persons of the purposes for which their personal information is required?
6. Does your business offer relevant persons the opportunity to restrict the purposes for which their personal information will be processed:
7. Does your business offer relevant persons the opportunity to object to the recipients to whom the personal information will be supplied?

Ask yourself this…

8. Does your business document retention policy make provision for the retention of records containing personal information?
9. What is your business' process for destroying and / or de-identifying records at the end of the retention period?
10. Does your business inform relevant persons about the duration for which the record will be retained and how these records will be destroyed at the end of the retention period?

Keeping the information longer…

1. If the organisation is required to keep the information in terms of any other law;
2. If the organisation needs to keep the information for a lawful purpose related to its activities (as long as any further purpose is communicated to the data subject);
3. If the organisation is contractually bound to keep the information (as long as the data subject's rights are not unreasonably intruded upon); or
4. If the data subject consents to the organisation keeping the information for an extended period

Condition #4 – Further processing limitation

Sec 15: Further processing of personal information must be **compatible with the purpose** for which it was collected.

- Once an organisation has identified and obtained consent for specific, legitimate and explicitly defined purposes, the processing of such personal information may only occur insofar as it is **necessary for the fulfilment of those purposes**.
- Thus, the Further Processing Limitation requires that an organisation may only use personal information for **those purposes that were specified at the time** that the individual consented to the processing of the information.
- If personal information is to be used for any other purpose or disclosed to any other recipients, **the further consent of the individual must be obtained**.

To assess whether further processing is compatible with the purpose of collection, the responsible party must take into account:

- the **relationship between the further processing and the original purpose** for which the information was collected, i.e. how close is the link between the original purpose and the intended further processing.
- the **nature of the information**, e.g. is it sensitive personal information.
- the **consequences of the further processing** for the individual, e.g. is the individual likely to benefit from or be prejudiced as a result of the further processing.
- the **manner in which the information was collected**, e.g. was the information collected directly from the individual or obtained from an indirect source.
- any **contractual rights and obligations** between the organisation, the individual and any other party (the fulfilment of such rights may possibly depend on the occurrence of the further processing)

Information will also be deemed compatible if:

- the individual **consents** to the further processing.
- the personal information is **publicly available**.
- it is necessary **in terms of any law**, to further a legal or public interest or to prevent serious harm.
- the personal information is **used for historical, statistical or research** purposes but has been de-identified.
- such processing has been **exempted in terms of the Act**

Ask yourself this…

1. Does your business process personal information for any other purpose except the identified purposes that are disclosed to the individual concerned?
2. What type of personal information does your business generally subject to further processing?
3. How does this further processing affect the individual to whom the information relates?
4. Does your business inform the individual concerned when personal information is used for a purpose other than originally disclosed?
5. When and how is this communicated to the individual?

Condition #5 – Information Quality

- Sec 16: The responsible party must take reasonably practicable steps to ensure that the personal information is **complete, accurate, not misleading and updated** where necessary.

Neither *"reasonableness" nor "practicality" is defined in the* Act. As a result, what is *"reasonable"* or *"practicality" is defined in the Act.* As a result, what is *"reasonable" or "practicable" is going to depend* largely on the circumstances of a particular organisation or industry.

Ask yourself this…

1. Does your business have a process for checking the accuracy and completeness of records containing personal information?
2. Does your business provide the opportunity to individuals to periodically verify and update their personal information?
3. How and when are individuals made aware of these processes?
4. Does your business have a process for monitoring and tracking updates to personal information?
5. Who is responsible in your organisation for ensuring that records containing personal information remain relevant, accurate and up-to date?

Condition #6 - Openness

Sec 17-18: Personal information may only be processed **by responsible party (RP)** that has notified the regulator

If personal information is collected the responsible party must take **reasonable practical steps to ensure that the data subject is aware of**:-

- the information being **collected**;
- the name and address of the **responsible party**;
- the **purpose** for which the information is being collected;
- whether or not the supply of the information by that data subject is **voluntary or mandatory;**
- the **consequences** of failure to provide the information;
- any particular **law authorising or requiring** the collection of the information;
- any further information such as the recipient or category of recipients of the information, nature or category of the information and existence of **the right of access to and the right to rectify** the information collected

Exclusions

The organisation will not have to comply with the data subject notification requirement in certain situations, including the following:

1. if the individual consents to the non-compliance or the non-compliance will **not be prejudicial to the individual**.
2. if the non-compliance is necessary for the **maintenance of law and order or in the interests of national security.**
3. to enforce legislation for **SARS** purposes.
4. if compliance is **not reasonably practicable** in the circumstances of the particular case (e.g. in the case of an emergency).
5. if the information will be used in such a way that the **individual will not be identified or for historical, statistical or research** purposes.

Ask yourself this…

1. Has your organisation compiled a manual and made it available in terms of the Promotion of Access to Information Act?
2. Does your business regularly review and / or update the manual?
3. Who in your business is responsible for liaising with the Regulator in terms of the Promotion of Access to Information Act?
4. Does your business use personal information for historical, statistical and research purposes?
5. Has your business identified all the relevant legislation which requires the collection, storage or disclosure or personal information for various purposes?

Condition #7 – Security Safeguards

Sec 19-22: The underlying theme of Condition 7 is that all personal information should be kept **secure against the risk of loss, unauthorised access, interference, modification, destruction or disclosure**.

Clauses 18 - 21 of the Act set out the specific requirements of this principle in some detail. In terms of the Act the obligation to maintain the security of personal information is made up of the following elements:

- the organisation's responsibility **to implement security measures to safeguard personal info**rmation held by the organisation;
- the organisation's responsibility **in respect of personal information that is processed by third parties** on behalf of the organisation;
- the organisation's responsibility to **notify stakeholders if personal information has been compromised** in any way.

Ask yourself this…

1. Does your business' risk management strategy include risks related to the processing of personal information?
2. Does your business have an information security policy? If so, does the policy make specific reference to personal information?
3. Does your business have strong identification and authentication controls to limit access to personal information?
4. Does your business back up personal information on a regular basis?
5. Does your business limit the number and categories of employees who have access to personal information? How?
6. Does your business enter into agreement with third parties who process personal information on behalf of the business? If yes, do these agreements address issues relating to information security safeguards, confidentiality, legal compliance and jurisdiction of laws?
7. How does your business ensure the reliability of third parties before allowing them to process personal information?
8. What is the manner of notification used by your organisation in the event of personal information breaches?

Condition #8 – Data Participation

Sec 23-25: Condition 8 empowers individuals to **access and/or request the correction of deletion of any personal information held about them that may be inaccurate, misleading or outdated**. This enables them to have a level of direct influence over the processing of their personal information. *(Access for Date Subject through the Promotion Access Information Act)*

Accessing personal information:

In terms of clause 22, an individual may make two types of requests, namely:

* **confirmation of whether an organisation holds any personal information** about them; or

* **a description of the personal information held about them**, including details of any third parties that may have access to that information

Ask yourself this…

1. Does your business have systems in place through which individuals can access and amend their personal information?
2. Does your business have an information officer to deal with requests relating to personal information?
3. Does your business notify individuals (employees and customers) about the manner in which they may access and/or update their personal information?
4. What is the form and manner in which individuals may request access to information?
5. Does your business charge any fees for accessing personal information?
6. If yes, are these fees in line with those set in terms of the Promotion of Access of Information Act?
7. How does your business verify the identity of individuals who requests access to personal information?
8. Does your business have a system to track requests for access to personal information?
9. Does your business have a verification procedure to ensure accuracy and completeness of personal information?
10. Does your business have a system to notify third parties of updates, corrections or deletion of personal information?

Transborder flows

- Sec 72: Transfer of personal information outside the RSA
  - A responsible party in the RSA **may not transfer personal information** about a data subject to a third party who is in a foreign country unless
    * **The third party who is the recipient of the information is subject a binding to a law**, corporate rules, or **binding agreement** which provides an adequate level of protection that -

    * Effectively **upholds principles for reasonable processing** of the information that are substantially similar to the conditions for the lawfull processing of personal information relating to the data subject who is a natural person, and where applicable a juristic person.

In summary: Managing your risk

- The requirements **of privacy by design** and **by default** have been made more adaptable to the context of the data controller's business by taking into account the **nature, scope, context and purposes of the data controller's processing activities**, as well as the likelihood and magnitude of the risks to the rights and freedoms of individuals.
- Data controllers established outside the EU do not need to appoint a representative in the EU for processing activities that are "occasional" and "unlikely to result in a risk" to the rights and freedoms of individuals.
- The level of security measures that are considered "appropriate" is determined by **analysing a broad range of factors**, including the available technology; the cost of implementation; the nature, scope, context and purpose of the data controller's processing activities; and the likelihood and magnitude of the risks involved

In summary: Managing your risk

- Data protection **impact assessments are required** for processing activities that likely involve “high risk” to the rights and freedoms of individuals, such as discrimination, identity theft, fraud, or financial loss.
- The requirement to **consult with data protection authorities** prior to commencing certain processing activities is limited to processing that “would result in a high” degree of risk “in the absence of measures to be taken by the controller to mitigate the risk”.
- The obligation to **report data breaches** extends to those breaches that are “likely to result in a high risk for the rights and freedoms of individuals”. If the compromised data are encrypted or otherwise protected so that it remains unintelligible, the data controller is not required to report the breach.
- One of the **conditions under which personal data may be transferred** to a third country or international organisation is if “the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers”

Project Management: Risk Responses

- The choices of response strategies for THREATS include:
  - **AVOID:** Focus on eliminating the cause and thus, eliminating the threat.
  - **MITIGATE:** There are certain risks that cannot be eliminated. However, their impact can be reduced.
  - **TRANSFER:** Transfer the risk to some other party. Insurance purchases, warranties, guarantees, etc are examples of risk transfers.
  - **IGNORE:** Impact is negligible and can be ignored under normal operational conditions.

Key risk indicators

- Historically, management has tracked **key performance indicators (KPIs)** to help detect issues affecting the achievement of objectives.
- In recent years, organizations have also been developing **key risk indicators (KRIs)** to help signal an increased risk of future losses or an uptick in risk events.
- KPIs and KRIs are tactical in nature, can be collected at any time, reported on a regular basis or as requested by management (e.g., as part of a balanced scorecard), and typically include **KPIs and/or metrics** (e.g. financial, market, SCM) that provide insight into an organization's risk position.

Purpose/Outcome

- It is therefore important that management develops an understanding of the 8 conditions for the lawful processing of personal information and are able to apply those principles to the processing of employees' personal information in their organisations.
- As the eight conditions for the lawful processing of personal information will affect nearly every area of business that processes personal information, the consequences are that this will require behavioural changes, changes to legal documents, internal structural changes (i.e. information technology upgrades, assurances that a data base cannot be accessed and physical firewalls and safety measures), and an analyses of subcontracting practices.

POPI for Business

- Privacy infringement
- Loss of Intellectual Property
- Defamation
- Loss of sensitive information
- Security compromise - issues of national security
- Financial loss

POTENTIAL FOR LITIGATION

Brand Damage

Reduce risk in 4 steps

- **Invest in Data Governance.** Any organization that has already accumulated large amounts of data while doing business with SA customers is subject to the strict penalties going forward and retroactively. With that in mind, data governance is critical. Prepare your data and the processes you used to gather, store, manage and use it. Designate an IO to manage your data governance.
- **Build and Implement Technological Infrastructure to Support POPI Compliance and the Protection-by-Design Approach.** Develop a data and analytics infrastructure that is specifically controlled, portable and compliant with your goals. Also, managing data lineage lets you know the history of the data in a snapshot, so having a system focused on illuminating that lineage is important.
- **Improve Your Data Security Practices.** You are probably always on watch for the most impenetrable security for your organization's benefit, but POPI adds a new level of intensity in the search. Focus on privacy rights, proper use of data, notification of use, consent and rectification when it comes to data security.
- **Build a POPI Compliance Team and Make Communication Its Foundation.** Train your existing employees on POPI compliance, and encourage questions and open communication. You may also need to enlist the expertise of external experts – or hire someone permanently - in legal compliance and data protection.

10 Steps To POPI Act Compliance Checklist

1. Formalise your POPI Act compliance project
2. Appoint an Information Officer (for the business)
    a) Appoint Risk & Compliance Manager (Agency)
3. Perform a POPI Audit (gap analysis versus the POPI Act)
    a) Business vs Projects assessment
4. **Analyse what and how Personal Information is processed; what records contain Personal information; what user rights exist for your PI**
    a) Intellectual property audit
    b) Information security audit
5. Implement POPI Act compliance policies
    a) Privacy policy
    b) Information security policy
    c) Intellectual property policy
    d) Innovation management
6. Review your web sites and publish privacy notice
7. Update / create your PAIA manual
8. **Implement POPI compliant PI management processes, including acquisition, processing, retention, security, and descruction procedures**
9. Train staff (& stakeholders) about their roles in POPIA compliance
10. Make POPIA compliance "Business-As-Usual"

In Summary

- **EIGHT PRINCIPLES FOR COMPLIANCE**
  - There are eight **principles** that form the foundation for organisations to ensure they are compliant. To be properly prepared for POPI, anyone handling and processing personal data needs to ensure it is processed **fairly, lawfully and in a transparent** manner; used for **specified, explicit and legitimate** purposes; and is used in a way that is adequate, relevant and limited.
  - Anyone handling and processing personal data also needs to ensure it is **accurate and kept up-to-date**; **kept no longer than is necessary**; and processed in a manner that **ensures appropriate security** of the data.
  - Data is categorised in two groups: **personal and sensitive**. Personal data is information such as HR records and contact information, whereas sensitive data is often health related, biometric or genetic.


Thank You