POPI ACT Presentation

What is POPI

- POPI will regulate the **processing** of **personal information (PI)** by **responsible parties (RP)**
- Conditions:
  - PI must be collected directly from the data subject (subject to exceptions)
  - PI must be collected for specific, explicitly defined purpose
  - PI can only be processed with DS' consent, under contract or other limited ground
  - PI must not be retained for longer than necessary for purpose for which collected
  - PI can only be processed further if compatible with original purpose
  - PI must be complete, accurate not misleading and updated where necessary
  - RP must take reasonably practicable steps to ensure that the DS is aware of PI being collected and purpose for which collected
  - RP must take appropriate and reasonable measures to protect PI
  - PI can't be sent offshore unless DS has consented or equivalent protection
- No fault civil liability if damage results from certain breaches
- In serious cases, fine or imprisonment not exceeding 10 years or both

Purpose of POPI

- This is to ensure the constitutional right to privacy while balancing this right against -
  - other rights such as the right of access to information
  - protection of important interests including the free flow of information
- To promote the protection of personal information processed by public and private bodies
- To provide for the establishment of an Information Regulator
- To provide for the rights of persons regarding unsolicited communications and automated decision making
- To regulate the flow of personal information across the borders of the Republic
- Facilitate international commercial relationships
- Keep up with international trends, e.g. EU data protection

Scope of POPI

- **This is the processing** of **personal information** entered in a record by or for a **responsible party**
  - where the responsible party is living in South Africa
  - or not living in South Africa, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.
- Subject to certain exclusions:
  - in the course of a purely personal or household activity
  - that has been de-identified to the extent that it cannot be re-identified again
  - journalistic, literary or artistic purposes under certain circumstances
  - etc.

What is Personal information

- Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including:
  - 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;
  - education or the medical, financial, criminal or employment history of the person
  - any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
  - the biometric information of the person; the personal opinions, views or preferences of the person
  - 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
  - the views or opinions of another individual about the person; and
  - 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

Data Subject etc..

- Data Subject
  - The person to whom Personal Information relates
- Responsible Party
  - A private or public body or any other person
  - which alone or in conjunction with others
  - determines the purpose of and means for processing personal information
- Operator
  - An operator is a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party

What is processing

- Any operation or activity or any set of operations concerning personal information (whether or not by automatic means) including:
  - the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
  - dissemination by means of transmission, distribution or making available in any other form; or
  - merging, linking, as well as restriction, degradation, erasure or destruction of information

Consent

- “consent” means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

Conditions for Processing

1. Accountability
2. Processing limitation
3. Purpose specification
4. Further processing limitation
5. Information quality
6. Openness
7. Security safeguards
8. Data subject participation

Accountability

- Responsible party must ensure that all the conditions and the measures that give effect to them are complied with.
- i.e. statement of responsible party’s accountability for lawful processing

Processing limitations

- Processing must be done lawfully and in a manner that does nor infringe the privacy of the data subject
- PI can only be processed if the processing is adequate, relevant and not excessive, given the purpose for which it is processed
- PI may only be processed if:
  - Data subject consents to processing
  - Processing necessary to perform under a contract to which data subject is party
  - In terms of an obligation imposed on RP by law
  - Processing protects legitimate interest of data subject
  - Processing necessary for performance of public duty by public body
  - Processing necessary to pursue the legitimate interests of the RP or 3rd party to whom PI was supplied

Processing Limitations

- Data Subjects may withdraw consent to processing, but RP can still process if e.g.:
  - necessary for fulfilling contract with DS
  - required by law
- Collection of PI must take place directly from the data subject unless:
  - PI is contained in a public record or deliberately made public by the data subject
  - Data subject has consented to collection from another source
  - Collection from another source would not prejudice a legitimate interest of the data subject
  - Collection is necessary for one of a variety of state purposes including the combatting of crime, national security etc
  - Collection from another source is necessary to maintain the legitimate interests of the RP or a 3rd party to whom PI supplied
  - Direct collection would prejudice a lawful purpose of collection
  - Direct collection is not reasonably practicable in the circumstances

3. Purpose specification

- PI must be collected for a **specific, explicitly defined** and lawful purpose
- Data subject must be aware of purpose of collection (see “Openness”)
- RP must destroy / delete or de-identify PI when no longer authorised to retain it
- The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

Retention of Records

- Records of PI must not be retained for longer than necessary to achieve the purpose for which the PI was collected or subsequently processed unless:
  - retention required by law
  - RP reasonably requires record for its functions or activities
  - retention required by contract
  - DS has consented to retention
- Records of personal information may be retained for longer periods for historical, statistical or research purposes IF the responsible party has established appropriate safeguards against the records being used for any other purposes.
- If PI used to make a decision regarding the DS, the RP must retain the record:
  - for as long as prescribed by a law code of conduct or
  - otherwise for as long as needed for RP to request access to the record

4. Further processing limitation

- Further processing must be compatible with purpose of collection
- Relevant factors for this include:
  - Relationship between original purpose and purpose of further processing
  - Contract between the parties
- POPI also sets out circumstances where further processing IS compatible with original purpose including:
  - DS consented to further processing
  - obligation imposed by law
  - conduct of legal proceedings
  - historical, statistical or research purposes

5. Information Quality

- RP must take reasonably practicable steps to ensure that PI is complete, accurate not misleading and updated when necessary
- When taking these steps the RP must take account of the purpose for which the PI is collected or further processed

6. Openness

- Before or as soon as reasonably practical after collection…
- RP must take **reasonably practicable** steps to ensure that the DS is aware of (most importantly):
  - PI being collected
  - Where PI collected from (if not direct from DS)
  - Name and address of RP
  - Purpose for which collected
  - RP intends to transfer PI to a “third country” or international organisation and the level of protection afforded to PI there
- Number of circumstances not necessary including:
  - Consent of DS
  - No prejudice to legitimate interests of DS if non-compliance
  - Compliance not reasonably practicable
  - PI not used in a form from which DS can be identified
  - PI used for statistical, historical, research purposes

7. Security Safeguards

- Responsible party must secure the integrity and confidentiality of PI in its possession or under its control
- By taking **appropriate**, **reasonable** technical and organisational measures to prevent:
  - Loss, damage or unauthorised destruction of PI
  - Unlawful access to or processing of PI

Prescribed Security Measures

- The responsible party must take **reasonable** measures to:
  - Identify all reasonably foreseeable internal and external risks to PI
  - Establish and maintain appropriate safeguards against the risks identified
  - Regularly verify that the safeguards are effectively implemented
  - Ensure that safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards
- “The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.”

Operators

- If an operator is processing PI for a responsible party it must:
  - Process the PI only with the knowledge or authorisation of the responsible party
  - Treat the PI as confidential and not disclose it
  - “unless required by law or in the course of the proper performance of [its] duties”
- Same is true where any other party processes for the RP OR the operator
- The **responsible party** must i.t.o. a written contract ensure that an **operator** also establishes and maintains the prescribed security measures
- Operator must immediately inform responsible party where reasonable grounds to believe PI has been accessed or acquired by an unauthorised person.

Notification of Security Compromises

- Where reasonable grounds exist to believe that PI has been accessed or acquired by an unauthorised person, the RP must notify the Regulator and the data subject
- Notification must take place ASAP after discovery of the compromise, subject to
  - Legitimate needs of law enforcement
  - Need to investigate the scale of the breach and restore integrity of RP's information system
- Sufficient information must be given to data subject to allow for protective measures to be taken

8. Data Subject Participation

- Data subject can request
  - whether a RP holds PI about the data subject (no charge)
  - the record / description of that PI including all 3rd parties who have access to that PI

- Data subject may also require the RP to:
  - correct or delete PI that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully
  - Delete PI that RP is no longer authorised to retain under principle 3 (purpose specification)

Processing of special personal information

- A responsible party may not process personal information concerning
  - 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
  - the criminal behaviour of a data subject to the extent that the information relates to
    - the alleged commission by a data subject of any offence; or
    - any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
- Subject to specific conditions

Enforcement

- Following complaint and investigation Regulator may issue an enforcement notice:
  - take steps or refrain from taking steps within stated period OR
  - stop processing PI specified in the notice or stop processing PI for the purpose or in the manner specified within stated period
- Failure to comply with enforcement notice penalties = fine or imprisonment not exceeding 10 years, or both
- Regulator may issue administrative fines
  - essentially an admission of guilt fine
  - max of R10 million
  - RP may elect to be tried in court

Transborder Information Flows

- Responsible party in RSA may not transfer PI to a 3rd party in a foreign country unless:
- Recipient is subject to a law, binding corporate rules or binding agreement that provide an adequate level of protection that:
  - effectively upholds principles for reasonable processing of PI that are substantially similar to the conditions for the lawful processing of PI
  - includes substantially similar provisions on transborder information flows to 3rd parties in a foreign country OR
- Data subject consents to transfer; OR
- Transfer necessary for performance of contract between RP and DS or implementation of pre-contractual measures in response to DS's request; OR
- Transfer is necessary for conclusion or performance of a contract concluded in the interest of the DS between RP and 3rd party OR
- Transfer is for the benefit of the DS, but
  - it is not reasonably practicable to get the data subject's consent, and
  - the data subject would be likely to give it.

Direct Marketing 1

- No Direct marketing UNLESS
  - data subject has given consent
  - RP may only request consent ONCE
- OR Data Subject is an existing customer
  - contact detail obtained in context of sale of good or service
  - direct marketing is of similar goods/services
  - data subject given opportunity to object to direct marketing when data collected and with each communication
- All direct marketing communications must contain:
  - identity of person on whose behalf sent
  - contact details for unsubscribe

Direct Marketing 2

- Distribution of marketing databases:
  - PI can only be **distributed** by collector of data with DS' consent (explicit)
  - PI can only be **received** by the "marketer" if the DS has consented to the distribution
  - Marketer must probably still obtain consent from DS to market to the DS
  - Marketer must notify the DS that it has received the PI **and** the source

Information Officer Duty

- Information Officer
  - Duty to ensure compliance with POPI