The Protection of Personal Information (POPI)

Why POPI?

In basic terms, the purpose of the POPI Act is to ensure that all South African institutions conduct themselves in a responsible manner when:

- collecting,
- processing,
- storing, and
- Sharing another entity's personal information by holding them accountable should they abuse or compromise your personal information in any way.
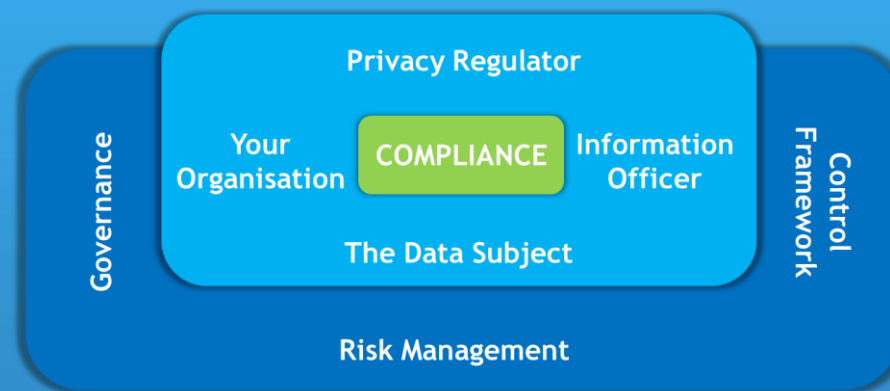
This implies that content pertaining to an individual may not be used unless:

- the data subject is informed how the organisation collects, uses, retains and discloses personal information
- the data subject's indication of agreements to his/her personal data being processed
- the data subject has the option to:
  - Opt Out – Personal information will be processed unless the data subject objects
  - Opt In – Personal information will be processed only if the data subject agrees

Countries in Africa at different stages of Privacy law adoption

The POPI Act Enforcement Landscape

Privacy Regulator

Governance

Your Organisation   **COMPLIANCE**   Information Officer

The Data Subject

Control Framework

Risk Management

• Criminal • Contact Details • ID Number • Opinions • Nationality • Gender • Race

The Regulator will:
1. Establish an effective date
2. Provide education
3. Monitor performance and enforce penalties
4. Handle complaints
5. Facilitate cross-border cooperation

Your Organisation must:
1. Take full Accountability
2. Limit Processing
3. Ensure Purpose specification
4. Limit Further Processing
5. Ensure information Quality
6. Maintain Openness
7. Ensure Security Safeguards
8. Involve the data subjects

The Information Officer will:
1. Be registered with the Regulator
2. Encourage compliance
3. Deal with requests
4. Assist Regulator with investigations
5. Ensure compliance

The individual can/must:
1. Knowledge of collection & access
2. Request access to PI
3. Object to storage of PI
4. Object to direct marketing
5. Give explicit permission for direct marketing
6. Automated profiling
7. Complain to Regulator
8. Institute civil proceedings

• Marital status • Biometric • Employment history • Physical or mental health • Education

Challenges to Privacy Program Success

- Lack of PI **Culture** and Attitudes at all levels
- An ineffective **Governance** Structure
- Restricted **Global framework**, rules and requirements
- Lack of **Resources** dedicated to creating and managing a privacy program
- Partial **Data** clarification and management

Implications of POPI on Policies and Processes

Applies to
- All Private & Public Sectors
- Natural and juristic persons (company, a close corporation, a body corporate or a trust)
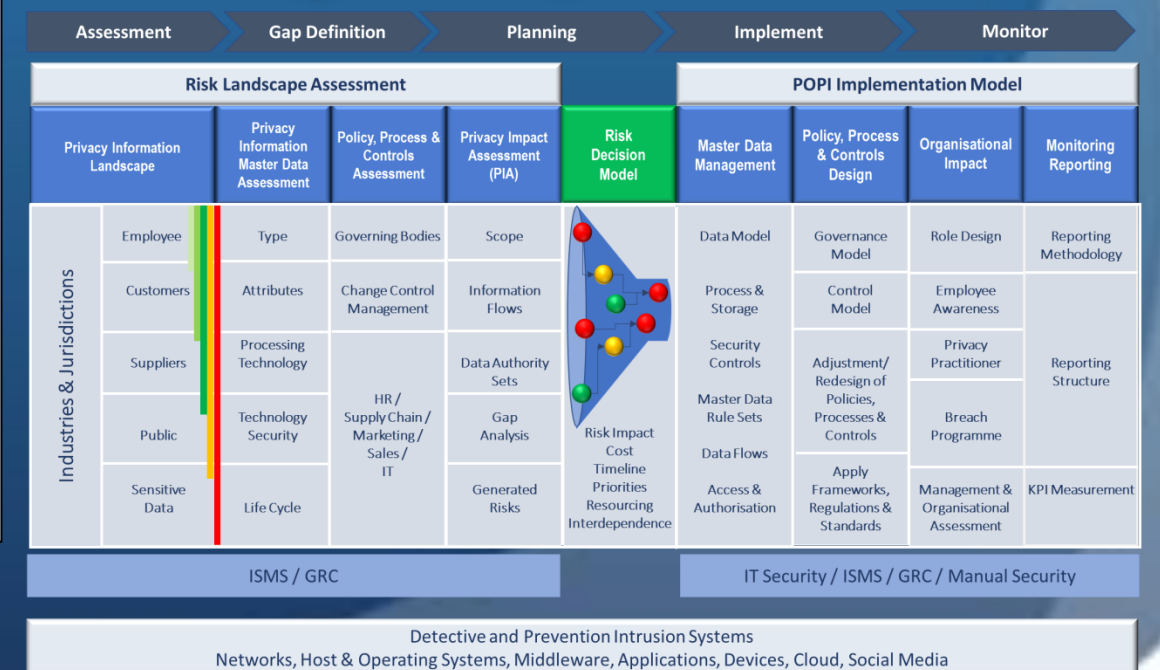- Hard copy and electronic records

Influences
- Employees
- Trading partners
- Information held on behalf of third parties

Impacts on
- Governance & Compliance
- Policies, Processes, Procedures
- Controls & Reporting
- Physical & Digital Security
- Risk Management & Audit
- Master Data Management

Magna POPI Compliance Framework

Assessment	Gap Definition	Planning	Implement	Monitor

Risk Landscape Assessment / POPI Implementation Model

	Privacy Information Landscape	Privacy Information Master Data Assessment	Policy, Process & Controls Assessment	Privacy Impact Assessment (PIA)	Risk Decision Model	Master Data Management	Policy, Process & Controls Design	Organisational Impact	Monitoring Reporting
Employee	Type	Governing Bodies	Scope		Data Model	Governance Model	Role Design	Reporting Methodology
Customers	Attributes	Change Control Management	Information Flows		Process & Storage	Control Model	Employee Awareness	
Suppliers	Processing Technology		Data Authority Sets		Security Controls	Adjustment/ Redesign of Policies, Processes & Controls	Privacy Practitioner	Reporting Structure
Public	Technology Security	HR / Supply Chain / Marketing / Sales / IT	Gap Analysis	Risk Impact Cost Timeline Priorities Resourcing Interdependence	Master Data Rule Sets		Breach Programme	
Sensitive Data	Life Cycle		Generated Risks		Data Flows / Access & Authorisation	Apply Frameworks, Regulations & Standards	Management & Organisational Assessment	KPI Measurement

Industries & Jurisdictions

ISMS / GRC	IT Security / ISMS / GRC / Manual Security

Detective and Prevention Intrusion Systems
Networks, Host & Operating Systems, Middleware, Applications, Devices, Cloud, Social Media