Presentation prepared by the E2 Group

POPI Act

Protection of Personal Information Act

Agenda

1. What is the POPI Act?
2. Who does it apply to?
3. POPI vs GDPR
4. Basics of the POPI Act:
    a. Objective
    b. Terminology
    c. Responsible person Vs. Operator
    d. Lawful processing
6. Penalties
7. So what do we do now?
    a. Understand our obligations
    b. Conduct a basic PI Audit
    c. Designate an information officer
    d. Implement security issues
    e. Update our SLA’s

What is the POPI Act?

- The POPI Act is a comprehensive data protection law that regulates the processing of personal information in South Africa. It's designed to **protect people from data breaches** and cybercrime, and to **prevent intrusive marketing** practices.
- The right to privacy has long been recognized under Article 14 of the South African Constitution. The POPI Act will put some meat on the bones of this fundamental principle by providing **clear rules** and a **means of enforcement**.
- The POPI Act became law on November 19, 2013 but hasn't yet come fully into force.

Who Needs to Comply with the POPI Act?

The POPI Act is **very broad** in scope and applies to just about every business and public body operating in South Africa. And to be clear, **this includes foreign companies** that are not based in the country.

According to Section 3.1, the POPI Act applies to any "responsible party" that is

- Based in South Africa, **or**
- Based outside of South Africa, so long as it **processes personal information inside South Africa** (unless it is merely "*forwarding personal information through South Africa*")

This means that **non-South African companies** will need to comply with the POPI Act if they have customers (or prospective customers) in South Africa.

POPI Act vs GDPR

The POPI Act is a fairly comprehensive law and is often compared to the **EU General Data Protection Regulation** (GDPR).

Like many modern data protection laws, the POPI Act shares certain terminology and concepts with EU laws.

You'll be at an advantage if you're already familiar or compliant with the GDPR or its predecessor, the **Data Protection Directive**.

Basics of the POPI Act

Objectives

The POPI Act lists several objectives, including:

- **Promoting** the **protection** of **personal information**
- **Establishing standards** for data protection
- **Bringing about new personal rights** around direct marketing and automated decision-making

Basics of the POPI Act

Key terminology

Personal Information

The POPI Act defines **personal information** by providing a non-exhaustive list of examples, including:

- Information about a person's **identity or beliefs** (e.g. age, race, religion, disability)
- Information about a person's **educational, medical, financial, criminal** or **employment history**
- **Identifiers** such as name, ID number, contact information, or online identifier (e.g. cookies)
- **Personal views**
- **Private correspondence**

Processing

Processing means, in effect, doing something with the data. Again, the POPI Act defines this similarly to the GDPR (see our article What Activities Count as Processing Under the GDPR?).

Examples of activities that constitute the processing of personal data include:

- Collecting an email address via a web form
- Storing a list of customers' addresses
- Sending a person marketing communications

Basics of the POPI Act

Key terminology continued

Responsible Parties

Responsible parties are the main subject of the POPI Act. Responsible parties **determine the purposes and means** of the processing of personal information. Under the GDPR, responsible parties are known as data controllers.

Your business can act as a responsible party in several scenarios, for example when it:

- Collects a person's address in order to mail them a product
- Shares a person's email address with an email marketing company
- Stores the resumes of job applicants in a filing cabinet.

A responsible party decides **how and why** to process personal information.

Operator

means a person who processes personal information for a responsible party in terms of a contract or mandate but does not come under the direct authority or control of the responsible party.

Basics of the POPI Act

Responsible Party Vs. Operator

As set out above, responsible parties determine the purpose for processing information, what information is processed, for how long and how it is processed. Where an operator is involved, the responsible party will still determine the purpose for processing etc, but will outsource the processing of the information to the operator. The responsible party therefore still makes all decisions in relation to the information and the operator acts in accordance with these decisions and on the instructions from the responsible party.

The responsible party remains ultimately accountable for ensuring that POPIA is complied with by both itself and all operators providing services to the responsible party. The outsourcing or sub-contracting of any processing activities to operators does not absolve the responsible party from liability. If the operator contravenes POPIA, the responsible party will still be held liable by the Information Regulator.

Basics of the POPI Act

Conditions for lawful processing

The conditions for lawful processing can be summarized as follows:

- **Accountability** - The responsible party must **ensure compliance** with the POPI Act
- **Lawfulness** - The collection of personal information must **not be excessive**, it must **be legally justifiable**, and it must not be collected from **third parties without good reason**
- **Purpose limitation** - Personal information must only be collected in connection with a **specific purpose** and must not be stored for **longer than necessary**
- **Restriction on further processing** - Personal information may only be processed for a purpose other than that for which it was collected under **specific conditions**
- **Information quality** - Personal information must be **complete and accurate**
- **Openness** - Personal information must be processed in a **transparent** manner
- **Security safeguards** - Personal information must be processed **securely** and the responsible party must provide **notification of any data breaches**
- **Data subject participation** - People must be allowed to **access** their personal information and **request that it is corrected or deleted** if it is inaccurate

Penalties for Non-Compliance

The POPI Act provides **new powers** to penalize people and businesses who fail to comply with the Act. Such penalties vary in severity depending on the nature and seriousness of the offence.

Penalties for violating the POPI Act include:

- **Administrative fines** of up to 10 million South African Rand
- **Prison sentences** up to 10 years

What do we do now?

1. Understanding our **legal obligations** under the Act
2. Conduct a **personal information audit**
3. Designate an **Information Officer**
4. Implementing information **security measures**
5. Update our **Service level agreements**

Understand our legal obligations under the Act

- Understanding the Act
- Reviewing process
- Informing Clients of our liability in terms of being an operator

Conduct a Personal Information Audit

Our company handles a lot of personal information. Some examples our found of relevance to us:

- You may be **storing** personal information in paper files, on hard disks, on web servers
- You might be **collecting** personal information via web forms, cookies, and mail
- You could be **sharing** personal information with marketing companies, analytics providers, and mail carriers
- These are just a few examples. Think carefully about **personal information flows** within your company.
- You can't comply with the rules in the POPI Act unless you know what personal information is in your control.

Designate an Information Officer

- All organizations, public or private, are required to designate an **Information Officer** under the POPIA.
- This role is comparable to that of a Data Protection Officer under the GDPR. However, whereas a Data Protection Officer is not always required under EU law, the requirement to appoint an Information Officer falls on **all South African companies**.
- The Information Officer can be anyone within your company, but their appointment must be approved by the head of your company.
- An Information Officer's duties include:
- Ensuring the company complies with the POPI Act
- Dealing with data subject rights requests (see below)
- Working with the Information Regulator

Implement Security Measures

One of the most important aspects of data protection law is the requirement to **store and transfer personal information in a secure way**.

You can think of your security responsibilities under the POPI Act as a three-part process:

- Risk assessment
- Technical measures
- Breach notification

Risk Assessment

Section 19.2 (a) of the POPI Act requires the responsible party to "*identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control.*"

Consider the following questions in relation to each set of personal information in your possession:

- Do we **need** to collect this personal information?
- How long do we need to **retain** it?
- Who else needs **access** to it?
- How might someone **illegally** gain access to it?

Technical

- There are many ways to secure personal information in transit and storage. At the broadest level, these consist of:
- **De-identification** (anonymization) - Scrubbing personal information of all identifiers. This is the most effective way to secure personal information, but will be appropriate only if you'll never need to re-associate it with an individual data subject.
- **Pseudonymization** - Swapping out identifying details in a set of personal information, which can then be re-identified with reference to additional information, stored separately.
- **Encryption** - Scrambling the entire contents of a set of information using mathematical techniques. This can be performed on a single file, in transit (via TLS/SSL protocols), or on an entire hard disk.

Breach Notifications

Section 22.1 of the POPI Act imposes an obligation on responsible parties to **notify the Information Regulator** of data breaches "*as soon as reasonably possible.*" Under certain conditions, you must also **notify the individuals** who have been affected by the breach.

- This topic will be on the mind of many South Africans following the high-profile Liberty Holdings data breach.
- To ensure you can mitigate the damage caused by a data breach, you should consider creating a Data Breach Policy. This will enable all staff to quickly and effectively identify and respond if the worst happens.

Thank you

End