FAIRBRIDGES WERTHEIM BECKER

Est. 1812

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

"POPIA"

Outline

- Introduction to POPIA
- Implementation – What does it entail?
- Developments since POPIA became effective and the grace period ended.

Introduction – The Act

- THE ACT's purpose - to ensure 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 for an abuse or compromise of personal information in any way
- THE ACT originates from Section 14 of the Constitution
- THE ACT has become applicable from 1 July 2021 and there was a grace period for the implementation from 1 July 2021 until 30 June 2022.

Introduction - Personal vs Special Personal Information

“Personal Information” comprises of any type of information that identifies you as an individual.

- Identity number
- CCTV camera surveillance within a building
- Phone number/ Email address
- Car Vehicle Registration Number

‘‘Special Personal Information’’ as referred to in section 26:

- Biometric information
- Trade union membership
- Race or ethnic origin
- Health / sex life of an individual

Section 27(1)(a) stipulates that the prohibition on processing of Special Personal Information as referred to in Section 26 does not apply if the processing is carried out with the consent of a data subject referred to in Section 26.

Introduction – Why do we collect Personal Information?

- Engaging in direct marketing
- Recruitment and employment purposes
- Providing professional services as per client mandate and as required by Law and/or the various collective agreements
- Administering, managing and developing our services
- Security, quality and risk management activities
- Complying with any requirement of law, regulation or a professional body
- Audit and record keeping.

Introduction - Responsible Party vs Operator

- "The Responsible Party" – determines the purpose and means for processing the personal information and controls processing of information
- "The Operator'' means 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
- "Processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, 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

Introduction - Pertinent Definitions

- "Biometrics'' means a technique of personal identification, based on physical, physiological or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition
- "Consent" means any voluntary, specific and informed expression of will, in terms of which permission is given for the processing of personal information
- "Data subject'' means the person to whom personal information relates
- "Electronic communication'' means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
- "Record'' means any recorded information, regardless of any form or medium, including any of the following:
  - Writing on any material [in the possession or under the control of a Responsible party] information produced, recorded or stored by means of:
    - tape-recorder or computer
    - equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored.

Implementation - Conditions of Lawful Processing

8 Conditions for the Lawful Processing of information:

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

Implementation – Notification Requirements

- Section 18(1) of THE ACT sets out the requirements for notification to data subjects – including but not limited to clients, contractors, employees and visitors to premises.
- All the requirements set out hereunder should be reflected and presented to data subjects who should be made aware prior to collecting information from them, providing services and/or gaining entry to premises.
- The purpose of obtaining such personal information must be justified and steps be taken to make data subjects aware of such reasons for collecting such personal information from them.
- Consent goes hand in hand with notification to data subjects and data subjects must provide their informed consent ideally via electronic signature on a digital device or signing a form/consent.

Implementation – Notification Requirements (continued)

- The Responsible Party (which in this case would be members in the Electrical Engineering Industry) when collecting personal information must take reasonably practicable steps to ensure that the data subject is aware of:
  - The information being collected from them and where the information is not collected from the data subject, the source from which it is collected
  - The name and address of the responsible party
  - The purpose for which their information is being collected
  - Whether or not the supply of information by that data subject is voluntary or mandatory
  - The consequences of failure to provide the information
  - Any legislation authorising or requiring the collection of information

Implementation – Notification Requirements (continued)

- The Responsible Party must ensure that the data subject is aware of any further information such as the :
  - Recipient or category of recipients of the information
  - Nature or category of the information
  - Existence of the right of access to and the right to rectify the information collected
  - Existence of the right to object to and the right to rectify the information collected
  - Right to lodge a complaint to the information regulator and the contact details of the information regulator.

Implementation – Consent

- Consent is vital when it comes to processing the information and is where the focus will be in terms of POPIA
- On such notification, the responsible party shall notify the data subjects of how they intend to process such information.
- The notification should further stipulate that Data subject's give their consent to the responsible party to retain such personal information for purposes of:
  - Security purposes for the Responsible Party's premises
  - Onboarding new clients and projects
  - Audit and reporting to regulatory bodies
  - Obtaining employee information
  - Invoicing clients etc
- Consent should be obtained thereafter in writing and be explicit – electronic or physical signature on a consent form

- The Responsible Party bears the burden of proof that the data subject's consent has been obtained.

Implementation – Consent for Verification Data

- Personal information must be collected DIRECTLY from a data subject, unless an exception within section 12(2) applies. Therefore, it may be required to obtain the data subject's consent to collect their personal data from third party sources for verification purposes – for example taking on a new client and confirming their ability to repay you and verify their data provided
- Verification data can be collected from various sources such as credit bureaus. How is the data quality and correctness verified?
    - One needs to establish who the responsible party is. We as the Electrical Engineers would be a joint responsible party with, for example, credit bureaus, licensing department or any other third-party information provider for verification of the data.
    - Against what database is this information cross-checked? Are electronic sources intercepted subject to a computer?
- Data Subjects must be notified and consent to our conducting verifications of and concerning the data obtained from them, in order to try enforce security safeguards.

Implementation – Consent for Verification Data

- Security measures to protect the information must be implemented, especially since there is a higher risk to privacy with sensitive information being collected and stored on the responsible party's database

- How long is the verification information kept for? This must align with Section 14.

- Whilst the scanning of the data collected is registered over the internet, there may be a risk of compromise to the data subjects information and therefore measures, must be implemented in terms of Section (19) (12) in order to protect the information in transit as follows:

    - Identify all reasonably foreseeable internal and external risks to personal information in its possession
    - Establish and maintain appropriate safeguards against the risks identified
    - Regularly verify that the safeguards are effectively implemented and
    - Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

- It is advisable for such an entity to consult an outside expert to advise on assisting such entity with implementing such safeguard and Data Protection measures

Implementation – Employees

- Personal Information and sensitive data may be easily accessible to staff members who may share this information with “unauthorized persons” in the office corridors or throughout the office or beyond.

- The first question one needs to ask is, are we the operator or are we the responsible party?
  - If we are the operator, we are obliged to keep the information confidential, and all the employees of the operator should be required to sign a confidentially/non-disclosure agreement

- If we are the Responsible Party, one would have to lawfully process this information. In doing so, we would have to make it clear to employees that such information:
  - would have to be kept confidential and also advise the employees that disciplinary measures will be taken against them should such confidentiality be breached
  - Staff training and awareness concerning this subject should also take place internally
  - The entity should formulate a privacy policy within the Company Employees must be contractually obliged to comply with confidentiality requirements, and to comply with the responsible party's privacy policy.

Implementation – Security Measures within the Work Place

- If employees work in offices with a door, they should be provided with a set of keys to and must ensure the door is locked as soon as they leave the office on a daily basis
- All employees should have passwords to log on to their computers and must ensure they log off when they are away from their computers.
- All employees should have locks on their drawers and cupboards connected to their desks and shall lock them when not in use.
- All files and documents should be neatly packed and locked away in the cupboards on daily basis.

Implementation – POPIA vs Confidentiality Clause

- POPIA Clauses deal with the Protection of Personal Information and this applies to both natural persons and companies.

- Confidentiality Clause is where an individual or company guarantees to deal with particular data as a commercial secret and guarantees to not disclose such information to others without correct authorisation.

Implementation – Summary

- NOTIFICATION to new and existing clients, employees, visitors, contractors and sub-contractors is required coupled with explicit and signed CONSENT from the data subjects

- The Notification is to contain:

  - The information being collected from them;
  - Name and address of the responsible party;
  - The purpose for which their information is being collected;
  - Whether or not the supply of 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 information;
  - Where such information is being transferred to;
  - Right to lodge a complaint to information regulator;
  - Safeguards implemented to protect such information.

- A privacy policy must be drafted and be presented in writing if required.

Implementation – Summary: Privacy Policy

- A Privacy Policy should contain the following:
  - Duration that the data is to be retained, subject to the business requirements of entity.
  - Consideration to be given to entity's insurance policy which may stipulate such information should be retained for a certain number of days.
  - Entity can either accept responsibility to protect data subject's information.
  - Alternatively, Entities can insert a disclaimer that data subjects enter their premises at their own risk.
  - Ultimately consider accountability.
  - How much responsibility an entity is prepared to take on to protect the data they have collected.
  - The entity abides by all South African Legislation that prevents all data subjects' information from being hacked.

Implementation – Security & Data Breach Policy

- **What is a security breach?**
  - A security breach occurs when any type of data is accessed by an individual who is not authorized to access it.
  - Any type of data is lost, altered, disclosed or destroyed.
  - Any type of data is damaged that was stored or processed in any way by the company or by a data provider acting on behalf of company.
  - Examples of Security breaches comprise of laptop loss, hacking, Phishing or denial of service, theft of lost of data, human error(e.g., sending email to the wrong recipient) by electronic means.

- **What is security breach procedure internally in the company?**
  - Notify the information officer and /or deputy information officer.
  - Complete the notification or security breach form within 1 hour of the security incidents.

Consequences for Non-Implementation

ADMINISTRATIVE FINES AND PENALTIES IN TERMS OF THE ACT.

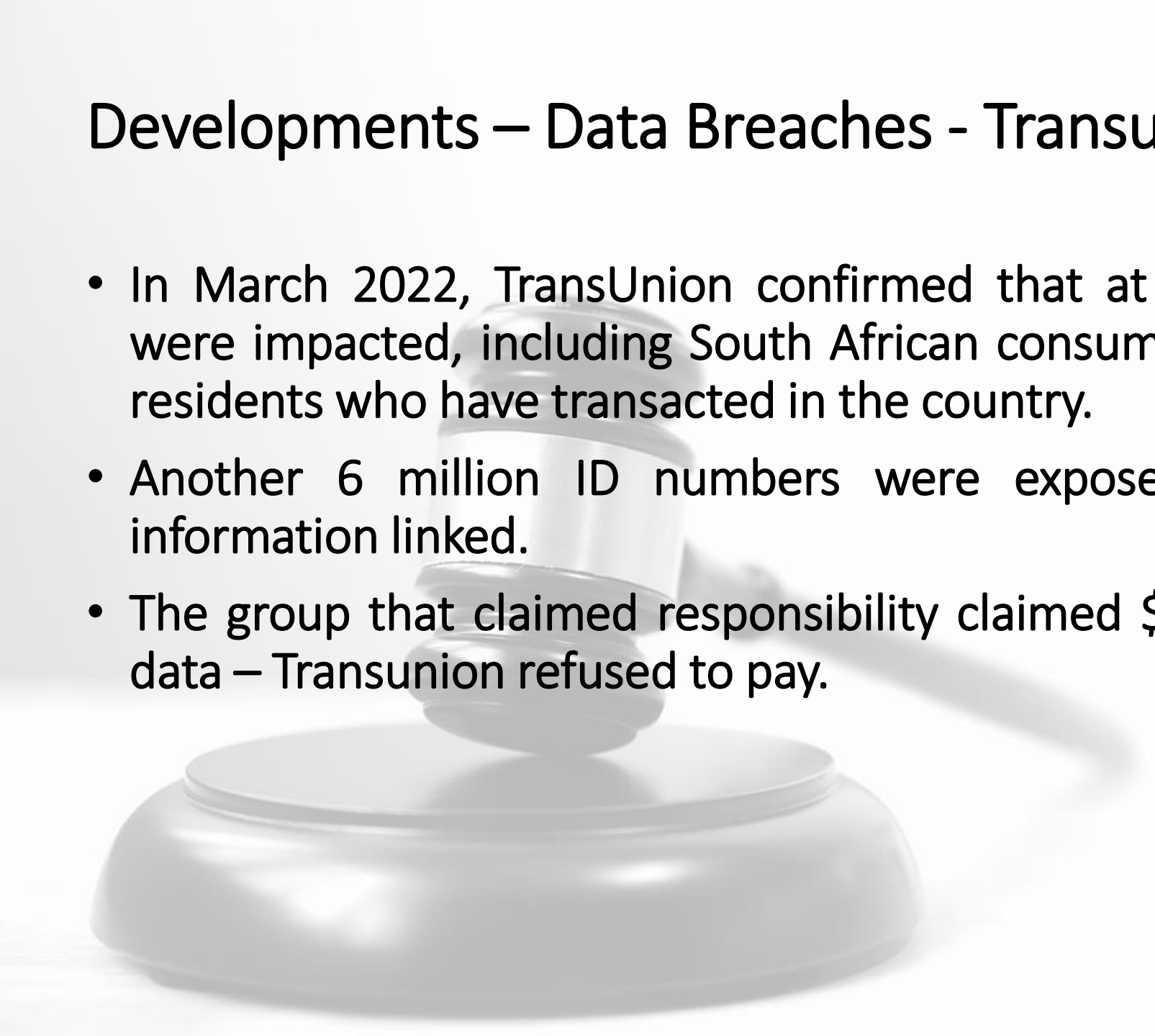
- Any person convicted of an offence in terms of THE ACT could face a fine of up to R10 000 000 or imprisonment not exceeding 10 years depending as to what contravention has been committed.

Developments – Data Breaches - EXPERIAN

- A consumer credit reporting company, declared on 19 August 2020, that it experienced a breach of data which has exposed some personal information of approximately 24 million South Africans, and 793,749 business entities, to a suspected fraudster.
- South Africa's Information Regulator says it has received information from a whistle-blower that the personal information of South Africans, exposed by the Experian data breach has found its way to the 'dark web'. The dark web allows criminals to anonymously sell stolen personal information.

Developments – Data Breaches - Transunion

- In March 2022, TransUnion confirmed that at least 3 million customers were impacted, including South African consumers and non-South African residents who have transacted in the country.
- Another 6 million ID numbers were exposed that had no personal information linked.
- The group that claimed responsibility claimed $15 million to not leak the data – Transunion refused to pay.



Developments – Data Breaches and the Potential Costs

- Facebook: $5 billion
- Amazon: $886 million
- Twitter: $150 million
- Uber: $148 million

➢ In South Africa, the average cost of a data breach was $3.21 million. (IBM Security Cost of a Data Breach Report)

Developments – Information Regulator

- Chairperson – Advocate Pansy Tlakula
- The Information Regulator is, empowered to monitor and enforce compliance by public and private bodies with the provisions of the POPIA Act. The Information Regulator is also responsible for issuing codes of conduct for different sectors and making guidelines to assist bodies with the development and application of codes of conduct.
- In February 2023, the Chairperson of the Information Regulator reported that they had received over 500 notifications of data violation but have not yet issued a single fine – including the Transunion breach noted above.

Developments – Dealing with Complaints Lodged with Information Regulator

- Once the Information Regulator has shared a complaint lodged against the company with it the defaulting party must timeously provide their side of the story to such complaint.

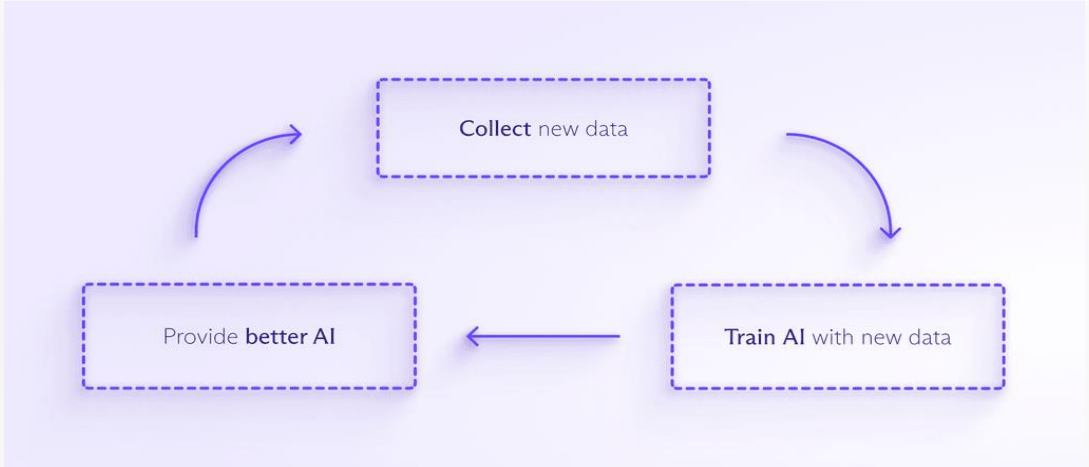
- If the defaulting party is of the view that they are guilty of such complaint, they should canvas ways to settle with the complainant.

- If the defaulting party is of the view that are not guilty, they shall draft a comprehensive response to set complaint and may have justification for committing such an act.

- The onus responsibilities on the Information Regulator to investigate such complaint and to possibly refer it to an enforcement committee for further determination.

Developments – Artificial Intelligence (AI)

- AI is a powerful tool that could lead to all sorts of new developments and breakthroughs. However, as with any tool, we must make sure it's used and developed responsibly.
- A major example would be ChatGPT, which is a Company developed by AI in the United States.However, there's been little examination of the privacy questions that AI raises.
- Massive amounts of data are required to train and improve most AI models. The more data that's fed into the AI, the better it can detect patterns, anticipate what will come next, and create something entirely new. As more and more data is being gathered, so AI enables more sophisticated analysis of large data volumes. As the importance of data rises, so do the associated legal issues.
- In some cases businesses are free to use the data they hold for whatever purpose they want, including developing AI algorithms. However, if personal data is used to develop, train or test AI algorithms, that processing will need to be fair and lawful and comply with data protection laws. In addition, if the data relates to a third party, it might be confidential or provided under a limited licence.



Developments – Artificial Intelligence (continued)

- From a compliance perspective, businesses in South Africa will firstly need to ensure that their AI system is compliant with POPIA
- Section 71(1) - governs automated decision-making. This is relevant to AI systems given their problem solving ability. This section protects data subjects from being subjected to a decision based solely on automated decision-making .
- Section 57(1)(a):
  - A Responsible Party must obtain prior authorisation from the Information Regulator if it intends to process any unique identifiers of data subjects (i) for another purpose than intended at collection, and (ii) with the aim of linking the information with information processed by other responsible parties.
  - As an example: an AI system deployed by Business A intends to combine the identity number of an employee with data collected by Business B to determine whether the employee is more susceptible to a certain work-related risk based on his or her age. In this instance, Business A would have to approach the Information Regulator before it could utilise the AI system. The responsible party must consider not only what information will be processed by the AI system but also how the AI system will use it, to ensure that all data protection compliance requirements have been met.
- Organisations must proceed with caution when the data inadvertently contains personal information. The organisation should consider whether the information can be input in de-identified (masked) or encrypted form, which would exclude it from the application of POPIA. If not, the responsible party must ensure that data subjects are aware that their personal information is being used to test an AI system. If data subjects are not aware of this or it differs to the original purpose of collection, the organisation would need to obtain consent.
- While the deployment of AI systems creates great opportunities for organisations, it is important for them to understand the laws that apply to the data being input into the system to ensure that use of data in the AI system is not in breach of any laws.

CALL TO ACTION:

- **The following documentation and/or Agreements need to be revised and drafted to make provision for POPI:**

  - Non-disclosure and Confidentiality Agreements;
  - Sale Agreements and Terms of sale;
  - Instruction forms;
  - Client information forms;
  - Credit applications; and
  - Any other form and/or document that contain personal information of a client or deals with the collection, distribution or any other form of processing of personal information of a client.

FAIRBRIDGES
WERTHEIM BECKER

Est. 1812

CONTACT US!

Jodi Poswelletski

011 268-0250 / 071 224 4665

Email: jodi.p@fwblaw.co.za

THANK YOU!