The Protection of Personal Information Act: Unpacked

On 01 July 2020, the Protection of Personal Information Act, 2013 (POPIA) came into effect and governs the processing of personal information by public and private bodies across the board. The 12-month grace period for compliance commenced on 1 July 2020 effectively giving private and public bodies until 30 June 2021 to comply with the wide-ranging requirements of the Act.

What is the purpose of POPIA?

The purpose of POPIA is to balance a person’s right to privacy, which is enshrined in the Constitution against the right to information.

POPIA achieves this by regulating processing activities and by placing obligations on the persons/entities processing personal information.

Definitions

A Responsible Party (the University) is the person or entity acting independently or jointly with other responsible parties that determines the purpose and means of processing personal information.

An Operator (consultants/entities appointed by the University) processes personal information for, on behalf of a Responsible Party in terms of a contract or mandate without being under direct control of the Responsible Party.

Information Regulator is empowered to monitor and enforce compliance by public and private bodies with the provisions of POPIA.

The Responsible Party appoints Information Officer (the Registrar) whose responsibilities include:

- Encouraging compliance by the University community with POPIA and ensuring lawful compliance with the conditions for the lawful processing of Personal Information;
- Maintaining and updating the University’s POPIA and to create a culture of compliance; and
- Assisting the Information Regulator with investigative conducted in terms of POPIA

Provisions relating to Trans-Border Information

Restrictions apply to the transfer of personal information outside South Africa. Personal information may not be transferred outside South Africa:

- Without the prior written consent of the individual;
- For the personal information of a Data Subject;
- To non-signatories of POPIA; and
- To any public or private body that is not an information regulator.

Preparedness and Response Plan:

- Developing a clear and effective incident/responding plan in collaboration with the Dean of the Faculty or the Head of the Division, ICT, Finance, Legal and Human Resources and other relevant stakeholders;
- Training employees and other operational staff to respond to breaches of POPIA;
- Installing emergency procedures and protocols to respond to breaches of POPIA;
- Developing a clear and concise notification plan to notify the Information Regulator as well as the Information Regulator in the event of a data breach;
- Developing a data breach response protocol to respond to breaches of POPIA;
- Developing a data breach response protocol to respond to breaches of POPIA.

Security Compromises

Data breaches can be as result of:

- Phishing;
- Phishing;
- Malicious/uncollected activity which interfere with the operating of an email attack, or a cyber attack (e.g. a denial of service attack or an email attack).

The 8 Conditions for Lawful Processing

As prescribed by the Act

1. Accountability

The Responsible Party (the University) must ensure that their Personal Information is processed lawfully, and it is a reasonable manner that does not infringe the privacy of the individual.

2. Processing Limitation

The Responsible Party (the University) must ensure that only relevant Personal Information is processed.

3. Purpose Specification

Personal Information must be collected by the Registrar for a specific purpose.

4. Further Processing Limitation

Further processing of Personal Information (i.e. for purposes other original purpose) must be in accordance and compatible with the original purpose of collection.

5. Information Quality

Practical and reasonable steps must be taken to ensure that the Personal Information is complete, accurate, not misleading and updated.

6. Openness

The Responsible Party (the University) must be open.

7. Security Safeguards

The Responsible Party must:

- Secure the integrity and confidentiality of Personal Information in its possession or under its control by implementing appropriate, reasonable, organisational and technical measures;
- Identify all necessary reasonable risks;
- Ensure that the security protocols are reviewed and updated regularly;
- Ensure that any contract with Operators contains provisions requiring the security measures by the Operator to preserve the integrity and confidentiality of the Personal Information.

8. Data Subject Participation

Data Subjects have the right to access their Personal Information at no cost.

Useful Tips:

- All information taken/collected must be handled safely and securely.
- Only copies of documents which are strictly essential for carrying out duties may be removed with the express written approval of the line manager. The originals must remain on site.
- Always use a secure mode of communication and never send personal or sensitive information over an insecure channel.
- Data breaches can be as a result of data leaks which can compromise identities and personal information thus adding another dimension to the legal and reputational consequences such as hefty financial consequences.
- Non-compliance can result in serious consequences. The infringement of the provisions has a trebling consequence such as a hefty fine, 30 years imprisonment or both a fine and imprisonment.

Remote workplace tips

The COVID-19 pandemic has forced employers to rethink and to stretch their workplace policies and to implement measures to stop the spread of the virus. This has led to the introduction of new risks such as data leaks which can compromise identities and personal information that will need to be considered in the context of remote working. Employers need to ensure that the responsibilities to also ensure the protection of the Personal Information is protected.

Non-compliance

Non-compliance can result in serious consequences. The infringement of the provisions has a trebling consequence such as a hefty fine, 3 years imprisonment or both a fine and imprisonment.