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

Here's what you need to know:

Personal Information is broadly defined as information relating to an identifiable, living natural or juristic person ("Data Subjects"). As you can see POPIA refers to the personal information of juristic persons, which means that the University will be able to rely on POPIA to protect their data.

Processing of Personal Information by a responsible party/an operator includes actions such as requesting, collecting, storing and processing or otherwise using the Personal Information of a person/juristic entity and must be lawful and in compliance with the provisions of POPIA..

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, or 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;
- Attending to requests made to the University ito POPIA; and
- Assisting the Information Regulator with investigations conducted ito of POPIA.

The 8 Conditions for Lawful Processing

As prescribed by the Act

1 Accountability

The Responsible Party (the University) must ensure compliance with the provisions of POPIA. Operators must comply with the provisions of the contract concluded with a Responsible Party.

2 Processing Limitation

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

- lawfully; and
- in a reasonable manner that does not infringe the privacy of the individual

3 Purpose Specification

Personal Information must be collected (by authorised staff) 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

POPIA leans on the Promotion of Access to Information Act 2 of 2000 (PAIA). The purpose of PAIA is to allow access to any information held by the State, and any information held by private bodies that is required for the exercise and protection of any rights.

The Responsible Party must:

- **Maintain the documents of all processing operations under its responsibility ito PAIA.**
- **Take practical and reasonable to ensure that the Data Subjects are made aware:**
  - that their Personal Information is being collected;
  - where it is collected from;
  - how it will be used;
  - the details of the Responsible Party;
  - the purpose for which the Personal Information is being collected; and
  - consequences of non-compliance .

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, organizational, and technical measures to:
  - Identify all reasonably foreseeable risk;
  - Develop a compliance framework by taking cognizance of centralized, consistent and institute appropriate safety protocols/practices to mitigate against the identified risks.
  - Ensure that the safety protocols are reviewed and updated regularly.
- Ensure that its contracts with Operators contain provisions regulating 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.

Provisions relating to Trans-Border Information

Restrictions apply to the transfer of personal information outside South Africa. Penalties apply to offences.

Security Compromises

Data breaches can be as a result of:

- human error (i.e. erroneously sending an email);
- theft of devices;
- system glitches;
- malicious/criminal activity which include inter alia
  - phishing attacks; or
  - cyber attacks.

Preparedness and Response Plan:

- develop a clear and effective incident/reporting 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;
- test internal responses to perceived/real breaches and implement a response protocol to minimize the risk. It would be prudent to engage with independent cyber security experts to restore the integrity of the information system or to upgrade the security protocols;
- create training/awareness programmes within the organization to encourage compliance with POPIA and to create a culture of compliance;
- develop a clear and concise notification plan to notify the Information Regulator as well as the Data Subjects. The notification must be made as soon as it is reasonably possible to do so after the discovery of the breach taking into account the legitimate needs of law enforcement or other measures to determine the nature and extent of the breach. The notification must be in writing or as directed by the Information Regulator.
- Operators must notify the Responsible Party immediately of any suspected or actual data breach.

Non-compliance

Non-compliance can result in serious consequences. The infringement of the provisions has far-reaching consequences such as a **hefty fine, 10 years imprisonment or both a fine and imprisonment.**

Protection of Personal Information: Remote workplace tips

The COVID-19 pandemic has forced employers to rethink and to stretch their workplace policies and to become more flexible by directing staff to work remotely increasing the risk of security breaches and data leaks which can compromise identities and personal information thus adding another dimension to the organization's responsibility towards ensuring compliance with POPIA. Employees now bear the responsibility to also ensure that the Personal Information is protected.

Useful Tips:

- All information taken/accessed offsite must be handled safely and securely.
- Only copies of documents which are absolutely essential for carrying out duties may be removed with the express written approval of the line manager. The originals must remain on-site.
- An accurate and updated register setting out the details of the employee, description of the document, reason and time of removal of must kept by the line manager.
- The documents must be stored in a safe/ secure cupboard/area.
- If there is travel involved then the documents must be placed in sealed bag and should remain under the supervision of the employee at all times.
- Laptops, computers and cellphones must be password controlled and the Personal Information must be encrypted.
- Only software approved by the ICT Department must be used and anti-virus software and personal firewalls must be installed and updated regularly.
- Computers or laptops should be logged off when unattended.
- All participants in a video conference must be notified of the purpose of the meeting and must consent to the meeting being recorded.
- Switch off cameras and microphones when not in use. Remove any personal/ business information from view when using the camera/during screen sharing.
- Work related email accounts must only be used for work related purposes.
- All files must be encrypted.
- It is the employees duty to ensure that emails are sent to the correct recipients.

Compiled by

Shobhna Morar

Betina Flemming

Tasneem Wadvalla

These are guidelines only. They are designed to assist you in ensuring compliance with POPIA. If you have any queries or difficulties please contact Mr Nkosinathi Mavimbela at the Legal Office: Nkosinathi.Mavimbela@wits.ac.za 0117171307.

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG