YOUR GUIDE TO THE PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

NATIONAL LOTTERIES COMMISSION
a member of the dtic group

The National Lotteries Commission is required to fulfil its mandate and ensure that the Commission performs its functions efficiently and effectively in compliance with our enabling legislation and any other applicable legislation.

Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy. The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.

The Protection of Personal Information Act 4 of 2013 (POPIA) came into effect on 1 July 2021 aims to promote the protection of personal information processed by the NLC as well as regulates matters connected therewith.

What is personal information?

- Race, gender, sex, pregnancy and marital status
- Any physical, postal or e-mail address of a person. Any identifying number of a person
- Information relating to the financial, education, medical or employment history of a person
- The biometric information of a person
- The personal opinions, views or preferences of a person
- The views or opinions of another individual about a person

Know your role players

There are four role players involved in the implementation of POPIA

Information Regulator (A)
the person empowered to monitor and enforce compliance with POPIA.

The data subject (C)
the person to whom the information relates.

The responsible party (B)
the person who determines why and how to process. For example, profit companies, non profit companies, governments, state agencies and people.

The operator (D)
a person who processes personal information on behalf of the responsible party. For example, an IT vendor.

Know your information officer

The Information Officer for the NLC is the Commissioner, Ms TCC Mampane

The NLC's Deputy Information Officers are Ms Gugulethu Yako and Mr Sikhumbuzo Thomo

You can contact the above for the following:

1) Reporting Data Breaches
2) General enquiries on processing of Personal Information
3) Encouraging compliance with POPIA requirements

Breach

A data breach occurs where occurs you believe personal information has been compromised or shared with unauthorized / unintended recipients or if data lost, shared or destroyed (intentionally or accidentally).

Examples of Data Breaches (but not limited the following)

Physical or electronic

- leaking of personal information to unauthorised recipients (internal and external stakeholders)
- hacking including information in transmission
- theft of personal information through physical or electronic means
- accidental loss and unauthorised use of personal information. (loss of laptops, notebooks, files including personal information)
- Exposure of personal information including information laying in open spaces and documents discarded unlawfully
- Human Error - erroneously sending an email to an unintended recipient

8 conditions of lawful processing

Accountability

This condition provides that a responsible party must ensure that the remaining conditions are complied with at the time of determination of the purpose and means of the processing and during the process itself.

Information quality

The responsible party must take reasonable steps to ensure that the personal information is complete, accurate and not misleading and updated where necessary. The responsible party should always have regard to the purpose for which the personal information was collected.

Security safeguards

This condition relates to the responsible party having to ensure that integrity and security of the personal information which it collected, is secured. Therefore, the responsible party should develop a system that prevents the risk of information "leaks".

Data subject participation

This condition provides that a responsible party should allow the data subject to participate where its information is concerned. The responsible party must develop a prescribed manner in which the data subject can have access to the personal information obtained by the responsible party, can request that it be corrected or deleted, if the need arises. It is important to note that the manner of access by a data subject is subject to the provisions of section 18 and 15 of PAIA.

Non-compliance compromises the NLC and may lead to investigation by the Information Regulator, penalties and reputational harm.

Processing limitation

This condition ensures that the rights of the data subject are not violated by placing limitations on what personal information can be processed, why its being processed and how it should be processed.

- **WHY?** – Personal information may only be processed if the reason/purpose for processing it is adequate, relevant and not excessive.
- **HOW?** – Personal information may only be processed if the data subject consents to it. The responsible party has to prove that the data subject has competently consented to the processing. If the data subject objects to the processing of the personal information, the responsible party may not process the information. The personal information can only be collected or obtained from the data subject who it relates to except for exceptions listed in section 12(2) of the Act.

Purpose specification

Personal information can only be processed for a specific purpose which is explicitly defined and lawful and which is related to the function of the responsible party.

The responsible party must ensure that steps are taken to make the data subject aware of the purpose of the collection of personal information. The personal information which has been collected shall not be kept for longer than is necessary to achieve the purpose for which it was collected. It may be stored and retained for periods in excess of the above mentioned if the responsible person is able to safeguard against the records being used for any other purposes.

Further processing limitation

Further processing must be in accordance with or compatible with the purpose for which it was collected. In order for the processing to be compatible, the responsible party should consider the following:

A) The **relationship** between the purpose of the intended further processing and the purpose for which the information was collected;
B) The **nature** of the information concerned;
C) The **consequences** of the intended further processing of the data subject;
D) The **manner** in which the personal information was collected; and
E) Any **contractual** rights and obligations between the parties

Openness

This condition provides that the responsible party must maintain the documentation of all processing operations under its responsibility as contemplated in section 14 of the Promotion of Access to Information Act (PAIA). The responsible party must also ensure that the data subject is aware of certain aspects, some of these will be listed below, however for the sake of brevity, only a few will be listed (please refer to section 18(1) of the Act for the complete list):

A) The **information** being collected and where it is not obtained from the data subject, the source from which it is collected;
B) **The name and address** of the responsible party;
C) **The purpose** for which the information is being collected; and
D) **The consequences** of the failure to provide the information.

Useful tips*

- All information taken/accessed off-site must be handled safely and securely
- Only copies of documents that are essential for carrying out duties may be removed with the express written approval 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 document must be stored in a safe/secure cupboard/area
- If there is travel involved then the documents must be placed in a sealed bag and should remain under the supervision of the employees at all times
- Laptops, computers and cell phones 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 it comes to using the camera/ during screen sharing
- Work-related email accounts must only be used for work-related purposes
- All files must be encrypted
- The employees must ensure that emails are sent to the correct recipients.

* https://issuu.com/witsmarketing/docs/popia_infographic

POPIA Framework Information: External stakeholders | Staff