

PROTECTION OF PERSONAL INFORMATION ACT (POPIA) NO. 4 OF 2013

27 Stiemens street,
JD House,
Braamfontien, Johannesburg

PURPOSE






- (a) To give effect to the constitutional right to privacy which includes the right to protection of personal information processed by public bodies while balancing this right with other rights stipulated in the Constitution of South Africa.
- (b) To promote the protection of personal information including the free flow of information within the country and across international borders.
- (c) To regulate the manner in which personal information may be processed.

APPLICATION

- (a) It applies to the processing of personal information that is entered in a record by or for a responsible party by making use of automated or non-automated means.

Note: It does not prevent any public body from exercising its powers or duties that relate to the lawful processing of personal information of the data subjects!

Contact us:

-  0100235200
-  enquiries@inforegulator.org.za
-  @InfoRegulatorSA
-  Information Regulator SA
-  POPIAComplaints@inforegulator.org.za

EXCLUSIONS

It does not apply to:

- (a) Processing of personal information that relates to personal or household activity.
- (b) Processing of personal information by a public body on matters that involve national security or public safety.
- (c) Processing of personal information solely for the purpose of journalistic, literary or artistic expression. (sections 6 & 7)

EIGHT CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

ACCOUNTABILITY

- (a) The responsible party must ensure that all the conditions for lawful processing of personal information are met. (Section (s) 8)

PURPOSE SPECIFICATION

- (a) Personal information must be collected for a specific and lawful purpose that is related to the function of the responsible party.
- (b) The data subject must be made aware of this. Records of personal information must not be retained for longer than is necessary for achieving the purpose for which it was collected. These must be deleted/destroyed once the responsible party is no longer authorised to retain them. (ss 13-14)

FURTHER PROCESSING LIMITATION

- (a) Further processing of personal information must be in accordance with the purpose for which it is collected. (s15)

OPENNESS

- (a) Notify the data subject when his or her personal information is collected including when transferring it to other countries.
- (b) Maintain records or documentation of all processing operations.
- (c) Inform the **data subjects** about his or her right to lodge a complaint with the Information Regulator. (ss17,18 &72)

INFORMATION QUALITY

Responsible party must take reasonable steps to ensure the personal information is complete and accurate. (s16)

PROCESSING LIMITATION

- (a) Personal information must be processed in a manner that does not infringe the privacy of the data subject.
- (b) The information that must be processed, must be relevant to the purpose and should not be excessive.
- (c) The data subject must give consent for processing of their personal information, **unless processing is based on another lawful ground.**
- (d) The data subject may withdraw or object to the processing of their personal information.

Note: The personal information that must be processed, should be collected directly from the data subject unless otherwise permissible! (ss9-12)

SECURITY SAFEGUARDS

- (a) The responsible party must secure the integrity and confidentiality of personal information in its possession by taking measures to prevent the loss of or damage thereof.
- (b) An operator or anyone processing personal information must treat such information as confidential.
- (c) The responsible party must notify the **Regulator** and data subject of data breaches or if their personal information has been accessed by unauthorised person. ss19-22)

DATA SUBJECT PARTICIPATION

- (a) The data subject, after providing adequate proof of identity, has the right to request the responsible party to confirm if they have his/her personal information and to correct it. **Data subject can also request access to his or her information and the responsible party must oblige. (ss 23-25)**



PROTECTION OF PERSONAL INFORMATION ACT (POPIA) NO. 4 OF 2013

OFFICIALS GUIDE

PROCESSING OF SPECIAL PERSONAL INFORMATION

The processing of special personal information is not prohibited in terms of the following sections:

- (a) General authorisation regarding special personal information (s 27),
- (b) Authorisation regarding data subject's religious beliefs, race, trade union membership, political persuasion (ss 28, 29, 30, 31)
- (c) Authorisation regarding data subject's health and criminal behaviour (ss 32 & 33) and
- (d) Authorisation concerning personal information of children. (s35)

INFORMATION OFFICERS

- (a) The administrative head of a public body is by default the Information Officer of that public body. They are then required to designate officials within that public body to serve as Deputy Information Officers to support the Information Officer.
- (b) S17(1) of Promotion of Access to Information Act (PAIA) stipulates that each public body must, subject to legislation governing the employment of personnel of the public body concerned, designate such number of persons as Deputy Information Officers as are necessary to render the public body as accessible as reasonably possible for requesters of its records.
- (c) S17(2) further states that the Information Officer of a public body has direction and control over every Deputy Information Officer of that body.

Duties and Responsibilities:

- (a) To ensure compliance with lawful processing of personal information by the public body
- (b) Deal with requests that relate to POPIA and work with the Regulator on investigations that relate to prior authorizations. (chapter 6)

Note: Deputy Information Officer must be appointed and delegated to perform some of the duties of the Information Officer! (s56)

PRIOR AUTHORISATION

- (a) The responsible party must, where applicable, obtain prior authorisation from the Regulator in accordance with s57.
- (b) The responsible party must notify the Regulator if information processing would require prior authorisation from the Regulator.

Failure to obtain prior authorisation, would result in the responsible party being guilty of an offence and being liable to a penalty. (ss 57-59).

Note: Applying or obtaining Prior Authorisation is not necessary in a situation where a specific sector has issued a code of conduct and it is being implemented!

DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATIONS

- (a) Direct marketing by means of unsolicited electronic communication which includes automatic calling machines, SMS or email is prohibited unless the data subject has given his/her consent.
- (b) The data subject's consent must be requested in a prescribed manner and form.
- (c) Any communication for the purpose of direct marketing must contain among others contact details of the sender to enable the recipient to request that such communication must stop if they so wish.
- (d) A data subject who is a subscriber to a printed or electronic directory should be able to unsubscribe for free. (ss69-71)

EXEMPTION FROM CONDITIONS FOR PROCESSING OF PERSONAL INFORMATION

- (a) Responsible parties may apply to the Regulator for an exemption from certain requirements and the Regulator may grant an exemption to a responsible party to process personal information even if that is in breach of a condition for the processing of such. This would be on condition that the Regulator is satisfied that the information could assist in prevention of an offence as an example. (ss36-38)

Note: The Regulator may impose reasonable conditions with regards to any exemption that might be granted!

CODE OF CONDUCT

- (a) The Regulator must consult with affected stakeholders before it approves a code of conduct.
- (b) The Regulator must publish the code on its website.

ENFORCEMENT (ss 73-99)

ENFORCEMENT POWERS

Interference with protection of personal information of data subject is considered a breach of:

- (a) the conditions for the lawful processing of personal information and
- (b) the provisions of a code of conduct. It is non-compliance with sections 22, 54, 69, 70-72

Note: Any person who alleges interference with the protection of personal information of a data subject, may submit a complaint to the Regulator in a prescribed manner. (s74-78)

THE REGULATOR HAS THE POWER TO:

- (a) Investigate a complaint,
- (b) Summon and enforce appearance of the responsible party before the Regulator,
- (c) Administer oaths,
- (d) Enter and search premises occupied by a responsible party after obtaining a warrant and
- (e) Search and seize after obtaining a warrant, any equipment or record that was used for processing of personal information.

Any person that contravenes sections 100-106 commits an offence which might attract a penalty, fine or imprisonment.