

# POPIA Readiness Webinar



**INFORMATION  
REGULATOR  
(SOUTH AFRICA)**

*Ensuring protection of your personal information  
and effective access to information*

# ROLES AND RESPONSIBILITIES OF THE INFORMATION REGULATOR

The Regulator is established in terms of Section 39 of the Protection of Personal Information Act No.4 of 2013 (POPIA), which enjoins the Regulator to be independent and impartial, and to perform its functions and exercise its powers without fear, favour or prejudice.

As an independent institution that is accountable to the National Assembly, subject only to the Constitution and the law, the decisions of the Regulator can only be reviewed by a Court of law.

# CONT.

- The Regulator consists of five (5) members, namely the Chairperson and four ordinary members (Members) who are appointed by the President on the recommendation of the National Assembly for a period of five years, which is renewable.
- The Chairperson and two (2) ordinary members are full time and the other two (2) ordinary members are part-time.
- One (1) full time ordinary member is designated for POPIA and the other for PAIA.

# CONT.

- The current Members took office on 1 December 2016 and their five (5) year term ends in November 2021 with the exception of one (1) Member who joined the Regulator on 01 December 2020 after the resignation of one part time member.

# MANDATE OF THE REGULATOR

The Regulator has a wide mandate which is provided for in section 40 of POPIA. Its mandate includes the following:

- to provide education;
- to monitor and enforce compliance;
- to consult with interested parties;
- to handle complaints;
- to conduct research and to report to Parliament;

# CONT.

- to issue, amend or revoke codes of conduct;
- to make guidelines to assist bodies to develop or apply for codes of conduct; and
- to facilitate cross- border cooperation in the enforcement of privacy laws.

# PURPOSE OF POPIA (section 2)

- Give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at:

*“balancing the right to privacy against other rights, particularly the right of access to information; and protecting important interests, including the free flow of information within the Republic and across international borders”.*

# CONT.

- Regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;
- Provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and
- Establish voluntary and compulsory measures, including the establishment of a Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.



# APPLICATION OF POPIA ( section 3)

- POPIA applies to the processing of personal information entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.
- POPIA takes precedence over other laws that regulates processing of personal information – materially inconsistent with POPIA.

# CONT.

- POPIA does not prevent a public or private body from exercising its powers.

# CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

# CONT.

## EIGHT CONDITIONS FOR LAWFUL PROCESSING



# Eight Conditions of Lawful Processing

## Accountability

- Responsible party must ensure compliance with the conditions for lawful processing.

## Processing Limitation

- PI must be processed lawfully, in a reasonable manner that does not infringe the privacy of the data subject.
- Minimality- adequate, relevant and not excessive. Consent, justification and objection; Collection directly from data subject

## Purpose Specification

- Collection for a specific purpose; retention and restriction of records; records must not be retained for a period longer than for the initial purpose.
- Exemptions: record required by law, historical, statistical, research. Destroy /De-Identify a record once purpose is attained.

# CONT.

## Further Processing Limitation

- Further processing must be compatible with the purpose of collection failing which consent must be obtained, further processing is necessary for the maintenance of the law, comply with an obligation imposed by law, conduct of court proceedings, in the interests of national security, prevent or mitigate a serious and imminent threat historical, research, statistical purposes

## Information Quality

- Personal information must be complete, accurate, not misleading and updated.

## Openness

- Responsible party must maintain records, Notification to data subject when collecting personal information

# CONT.

## Security Safeguards

- A responsible party must secure the integrity and confidentiality of personal information
- Information processed by an operator or person acting under authority must do with the knowledge/authority of the responsible party
- Information must be treated as confidential
- Security measures must adhere to security measures and notify the responsible party immediately if there is a breach

## Data Subject Participation

- Data Subject must have access to PI
- Correction or deletion of PI if inaccurate, irrelevant outdated, excessive, incomplete, misleading or unlawfully obtained.
- Manner of access

# REGULATOR'S STATE OF READINESS

- On 1 July 2021 all responsible parties must ensure that all processing of personal information complies with POPIA. The enforcement powers of the Regulator will come into effect on this date.
- On 30 June 2021, the Regulator will be responsible for the promotion and enforcement of the rights protected by PAIA. This function is currently performed by the South African Human Rights Commission ( SAHRC).



# CONT.

- On 1 July 2021 section 58(2) of POPIA shall become applicable to the processing of personal information referred to in section 57 of POPIA (processing subject to prior authorisation).
- Guidance Note on Information Officers and Deputy Information Officers, 01 Apr 2021
- Guidance Note on applications for Prior Authorisation, 11 Mar 2021;
- Guidelines to develop Code of Conduct, 15 Feb 2021.

# CONT.

- Regulations made by the Regulator in terms of section 112(2) of POPIA has or will come into operation as follows:
  - Regulation 5 (application for issuing a code of conduct) came into effect on 1 March 2021;
  - Regulation 4 (responsibilities of Information Officers) will come into effect on 1 May 2021; and
  - Residual regulations will come into effect on 1 July 2021.

# INFORMATION OFFICERS AND DEPUTY INFORMATION OFFICERS (SECTIONS 55 AND 56)

- In terms of both PAIA and POPIA, the CEO or head of the each public and private body is by default an information officer and he or she may designate or delegate a deputy information officer. This is an appointment by operation of law, in terms of which the CEO, DG, HOD of equivalent officers are automatically information officers.
- An Information Officer must be registered by the Responsible party with the Regulator.

# DUTIES AND RESPONSIBILITIES OF INFORMATION OFFICERS

- Encouragement of compliance with the conditions for the lawful processing of personal information;
- Dealing with requests made to the body pursuant to POPIA;
- Working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body;

# CONT

- Otherwise ensuring compliance by the body with the provisions of POPIA;
- Ensure that a compliance framework is developed, implemented, monitored and maintained;
- Ensure that a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

# CONT

- Ensure that a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the PAIA;
- Ensure that internal measures are developed together with adequate systems to process requests for information or access thereto;
- Ensure that internal awareness sessions are conducted regarding POPIA, its regulations, codes of conduct; and
- Information Officers must take up their duties only after the responsible party has registered them with the Regulator.

# DESIGNATION AND DELEGATION OF DEPUTY INFORMATION OFFICERS

- Each public and private body must make provision, in the manner prescribed in section 17 of PAIA, for the designation of such number of persons, if any, as deputy information officers to perform the duties stipulated in section 55(1) of POPIA, POPIA Regulations or any power or duty conferred or imposed on an Information Officer by POPIA to an information officer of that public or private body.
- The Regulator had published a Guidance Note on Information Officers and Deputy Information Officers.

# GUIDELINES ON DEVELOPING CODES OF CONDUCT ( Section 60-68)

- POPIA empowers the Regulator from time to time to issue, amend and revoke codes; to prepare written guidelines that would assist bodies to develop or to apply codes; to approve codes; and to consider afresh, upon application the determinations by adjudicators under approved codes;
- The purpose of a code is to establish a voluntarily accountability tool and to promote transparency for relevant bodies on how personal information should be processed. Codes do not replace the relevant provisions in POPIA, but operate in support of the requirements in POPIA;



# CONT.

A code of conduct cannot limit a data subjects right to privacy, as provided for in POPIA;

- The relevant bodies bound by an issued or approved code of conduct must not perform an act or engage in a practice that breaches the approved code;
- A breach of an approved code is deemed to be a breach of the conditions for the lawful processing of personal information referred to in Chapter 3 and shall be dealt with in terms of Chapter 10 of POPIA; and

# CONT.

- The reason for developing a code may include:
  - providing clarity on how the conditions for lawful processing of personal information are to be applied and complied with given the particular features of a relevant body;
  - providing a functional equivalent means of fulfilling the obligations related to the conditions for the lawful processing of personal information;
  - promoting an organisational paradigm shift change in a relevant body relating to the lawful processing of personal information;

# CONT.

- stipulating conditions for the lawful processing of personal information for specified information or classes of information;
- stipulating conditions for the lawful processing of personal information for any specified activity or class of activity;
- outlining rules and procedures for information matching programmes if such programmes are used within a specific sector;

# CONT.

- outlining how the legitimate interests of data subjects are to be protected insofar as automated decision making affect them;
- enabling the review of a code by the Regulator;
- providing details regarding the expiry of a code; and
- providing a procedure of dealing with complaints.

# PRIOR AUTHORISATION

Section 57 (1) of POPIA provides that a responsible party must obtain prior authorisation from the Regulator, (only once, except where the processing departs from that which has been authorised) prior to any processing if that responsible party plans to-

- process any unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection; and with the aim of linking the information together with information processed by other responsible parties;

# CONT.

- process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;
- process information for the purposes of credit reporting; or
- transfer special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

# CONT.

- Please also note that, in accordance with section 57(2) of POPIA, the Regulator may, from time to time and if necessary, prescribe categories or types of information processing that is subject to prior authorization, if it considers that such processing carries a particular risk for the legitimate interests of the data subject.

The requirement of prior authorisation is not applicable if a code of conduct has been issued and is in operation.

# CONT.

- Unless a Code of Conduct has been issued by the Regulator and has come into force in a specific sector/ industry in which the responsible party operates, the responsible party who is currently processing or intends to process the personal information of data subjects which is subject to prior authorisation must submit their applications prior to processing or any further processing.
- Application form for Prior Authorisation and Guidance Note on Prior Authorisation may be downloaded from the Regulator's website.



# CONT.

## What are the prescribed timeframes for finalising the application for prior authorisation?

- The Regulator may approve or reject an application for prior authorisation within four (4) weeks of receipt of prior authorisation application, unless the Regulator decides to conduct a detailed investigation.
- In the event that the Regulator decides to conduct a more detailed investigation, the Regulator will inform the responsible party in writing of the reasonable period within which it plans to finalise a detailed investigation, which period will not exceed thirteen (13) weeks.

# CONT.

- On conclusion of the more detailed investigation, the Regulator will issue a statement or report about the lawfulness of the information processing. If a statement or report conclude that the information processing is not lawful, such report or statement shall be deemed to be an enforcement notice served in terms of section 95 of POPIA.

# CONT.

- However, if the Regulator fails to finalise the application within the prescribed period of 13 weeks, the responsible party may presume a decision in its favour and continue with its processing. This presumption is rebuttable, meaning that should the Regulator find that information processing is unlawful, the responsible party will have to comply with its directive as contained in the statement or report.

# CHALLENGES

- Functionally, the Regulator operates independently but administratively it still uses the policies and systems of the Department of Justice and Constitutional Development.
- Lack adequate resources to establish the administrative capacity of the Regulator.
- Lack of adequate resources for the effective execution of the broad mandate of the Regulator.
- Lack of critical mass of experts in POPIA in the country.

# CONCLUSION

List of Guidance Notes the Regulator will be issuing before 30 June 2021-

- Guidance Note on Exclusions from POPIA
- Guidance Note on Exemption from the conditions for lawful processing of personal information;
- Guidance Note on notification of security compromises or breaches;
- Guidance Note on processing of personal information across-borders;
- Guidance Note on direct marketing; and
- Guidance Note on application to process special personal information and personal information of children.

# TAKE CONTROL OF YOUR PRIVACY

## INFORMATION REGULATOR

