CDH RETAIL SECTOR WEBINAR PROTECTION OF PERSONAL INFORMATION ACT ("POPIA")

Presented by Preeta Bhagattjee and Christoff Pienaar

14 July 2021

Presented by:

Preeta Bhagattjee
Sector Head & Director
Technology, Media & Telecommunications
Johannesburg
T +27 (0)82 889 0063
Preeta.bhagattjee@cdhlegal.com

Christoff Pienaar
National Practice Head & Director
Technology, Media & Telecommunications
Cape Town & Johannesburg
T +27 (0)83 295 3003
Christoff.pienaar@cdhlegal.com

CDH
CLIFFE DEKKER HOFMEYR

OVERVIEW

- Overview of POPIA and POPIA in context
- Current and ongoing compliance requirements
- Key awareness areas for the retail sector
  - Loyalty programs
  - E-commerce
  - Direct marketing
- Questions and Answers

POPIA OVERVIEW

CLIFFE DEKKER HOFMEYR

WHAT IS POPIA?

STATUS OF POPIA

- Enacted into law on 26 November 2013
- President declared commencement date as 1 July 2020
- Grace period of 12 months to become fully compliant expired on 30 June 2021

INFORMATION REGULATOR (SOUTH AFRICA)

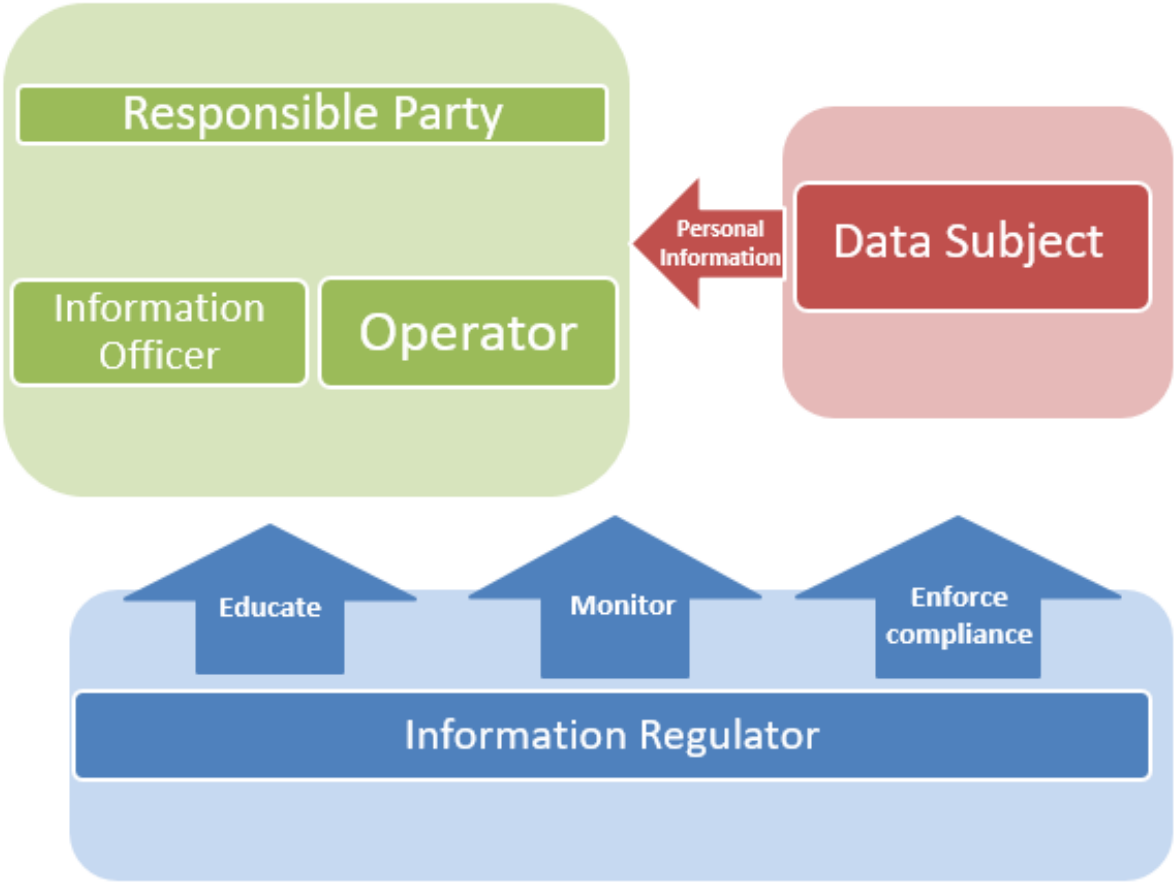
Ensuring protection of your personal information and effective access to information

PURPOSE OF POPIA

To regulate the use of personal information, generally by **businesses**, to ensure that there is a **balance** between the ability of the business to use the personal information for its **legitimate** business purposes, and the data subject's right to privacy.

POPIA applies to personal information of **natural** and **juristic** persons (for example, your employees and your customers)

THE WHO?


Responsible Party
Information Officer
Operator
Personal Information
Data Subject
Educate
Monitor
Enforce compliance
Information Regulator

WHAT IS PERSONAL INFORMATION?

"PERSONAL INFORMATION"

Information relating to an **identifiable, living natural person**, and where applicable **juristic person**, **including**:

- race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth
- education or the medical, criminal, employment or financial history of a person
- identifying number, email address, telephone and physical address
- online identifier
- biometric information
- personal opinions, views or preferences of the data subject
- explicitly or implicitly private or confidential correspondence
- views of others about that person
- name if name would reveal information

"SPECIAL PERSONAL INFORMATION"

Separately defined and separately regulated.

The definition covers a data subject's:

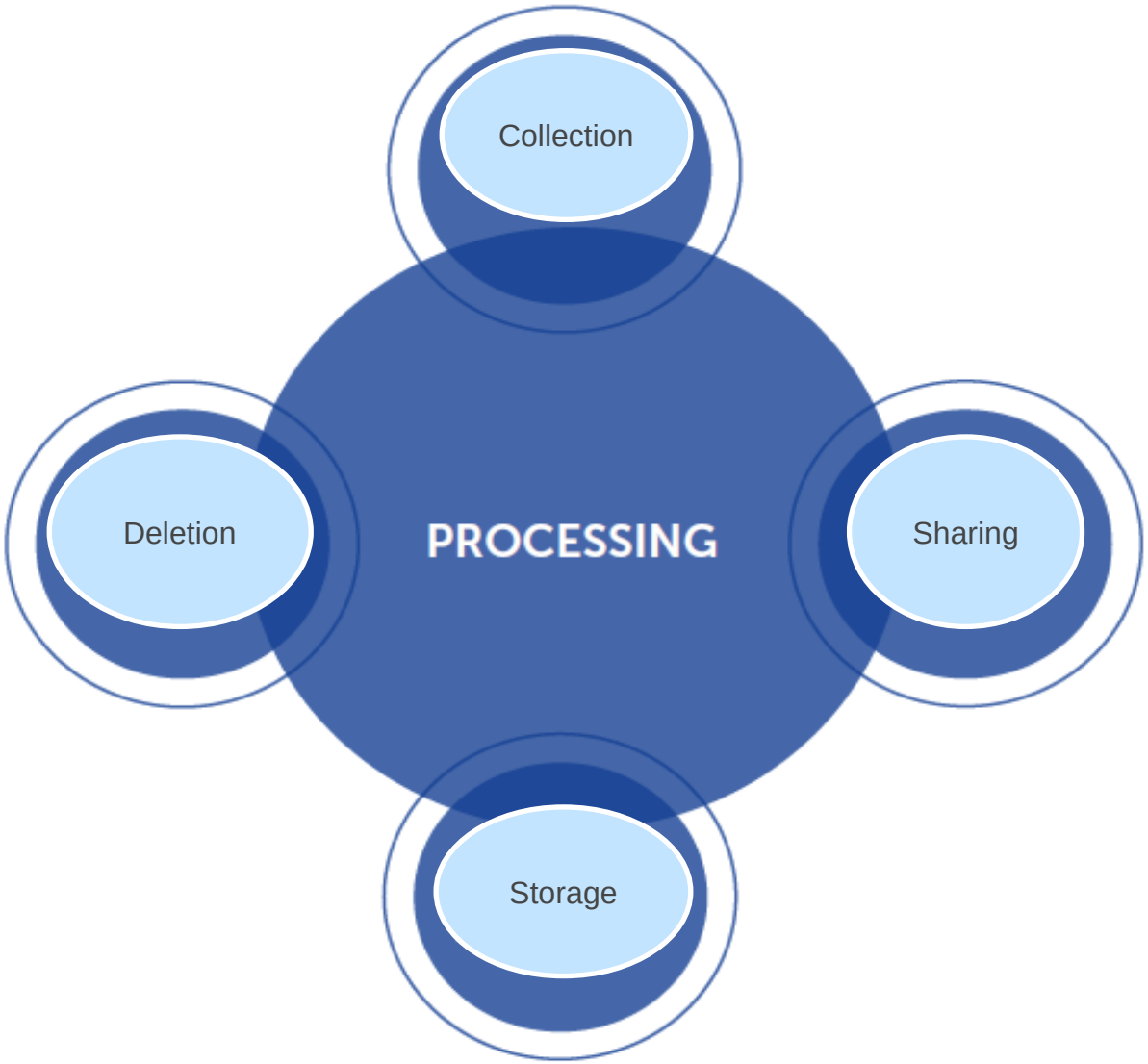
- religious or philosophical beliefs
- race or ethnic origin
- trade union membership
- political persuasion
- health
- sexual life
- biometric information
- criminal behaviour

"PERSONAL INFORMATION OF CHILDREN"

Most restricted category of information; Separately regulated

WHERE WOULD YOU FIND PERSONAL INFORMATION IN YOUR ORGANISATION?

FOOD FOR THOUGHT IN RESPECT OF PROCESSING

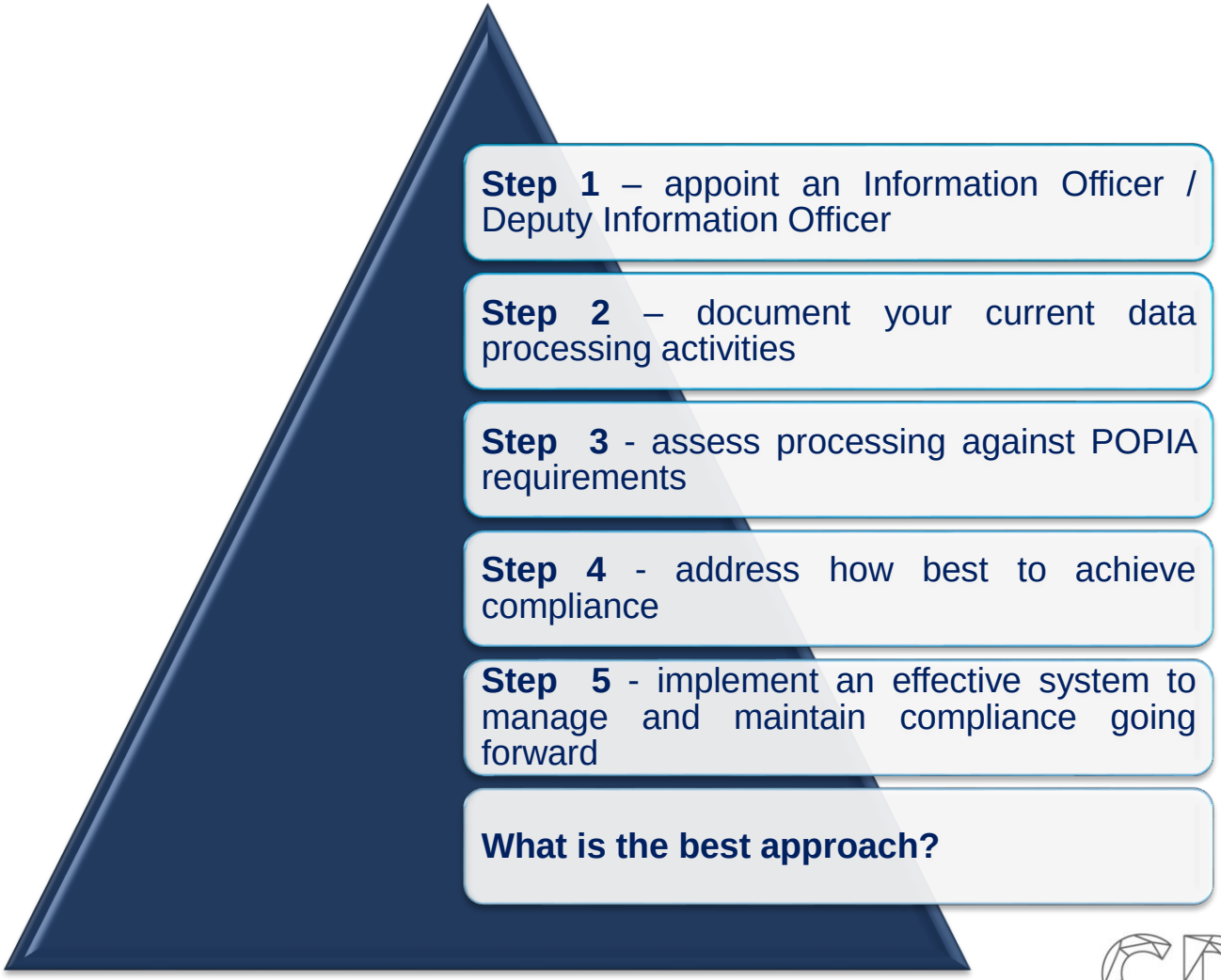


POPIA IN PERPSECTIVE

Though there are similarities between POPIA and its European Union counterpart, the GDPR, there are also distinct differences:

- natural vs. juristic persons
- penalties
- reporting a breach

STEPS TO ACHIEVING POPIA COMPLIANCE



APPOINTMENT OF INFORMATION OFFICERS

- Who are information officers?
- Designation of Deputy Information Officers
- The Information Officer (and/or deputy information officer(s)) must be registered with the Information Regulator

"REGISTRATION OF INFORMATION OFFICERS PORTAL

Please note we are experiencing technical issues with the Portal, which results in it not being accessible at the moment. Our technicians are working on it. The Portal will be accessible as soon as these issues are resolved. We apologise for the inconvenience caused."

- The key is to have an effective "privacy office"

ROLE OF INFORMATION OFFICER

The responsibilities of Information Officers include the following:

- **MANAGE COMPLIANCE** - encouraging compliance with POPIA and PAIA
- **PAIA MANUAL** - develop, monitor and maintain a manual as prescribed under PAIA
- **COMPLIANCE FRAMEWORK** - develop, implement, monitor and maintain a compliance framework
- **DOCUMENT DATA PROCESSING ACTIVITIES**
- **IMPACT ASSESSMENTS** - perform personal information impact assessments

ROLE AND RESPONSIBILITY OF INFORMATION OFFICER CONTINUED

- **COOPERATE WITH THE IR** - assist the information regulator to conduct investigations into any compliance issues or information requests
- **ADDRESS ACCESS REQUESTS** - handle the processing of data subject requests for access, correction and deletion
- **INTERNAL ACCESS PROCEDURE** - develop internal procedures which adequately processes requests for information
- **DATA TRANSFERS** - manage and oversee transfers of personal information
- **TRAINING AND AWARENESS** - raise awareness of data protection laws which includes training and updating data protection policies

MANAGING COMPLIANCE

- **POLICIES AND PROCEDURES/ AGREEMENTS**
- **RETENTION PROCEDURES** - deal with retention of records and disposal in compliance with POPIA
- **CONSENT MANAGEMENT** – keeping track of consent; manage instances of refusal or withdrawal
- **DATA BREACH RESPONSE PROCEDURE**

ROLE OF INFORMATION OFFICER DURING DATA BREACHES

- Information officer needs to ensure that the organisation has adequate breach detection, investigation and internal reporting procedures in place -
  - Detect and analyse the data breach
  - Analyse what data is affected
  - Consider the contractual / legal implications of the data breach
  - Report to management per predefined escalation procedures
- Consider notification obligations
  - Information Regulator
  - Affected data subjects
  - Other legislative notification obligations

HOW TO ENSURE INFORMATION QUALITY IS MAINTAINED

- Identify categories of PI to keep updated and implement procedure to do so
- Must take **"reasonably practicable steps"** to ensure that information is complete, accurate, not misleading and updated **"where necessary"** having regard to the purpose for which it is collected/processed
- **How?**
  - Via call centre, email communications, re-application forms etc.
  - Keep data centralised so as to facilitate easy updating of personal information

DATA SUBJECT NOTIFICATION

- Data subject must be aware of -
  - Information collected
  - Purpose of the collection
  - Name and address of the responsible party
  - Whether the supply of information is voluntary or mandatory
  - Right to access, object to or rectify information
  - Intended transfers to foreign countries
  - Contact details of the Information Regulator

DEALING WITH THIRD PARTIES PROCESSING PI

RESPONSIBLE PARTY OR OPERATOR?

"Responsible party"
=
a public or private body or any other person

which, alone or in conjunction with others,

determines the purpose of and means for processing of personal information.

"Operator"
=
a person who processes personal information for a responsible party

in terms of a contract or mandate,

without coming under the direct authority of that party.

MANDATORY SECURITY MEASURES ASSESSMENTS

Section 19 requires responsible parties to:

Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control	Establish and maintain appropriate safeguards against the risks identified	**Regularly verify that the safeguards are effectively implemented**	**Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards**

NEW BUSINESS LINE OR DEVELOPMENT

- Requirement to collect and process new PI e.g. running a survey

- When you have a new business innovation or activity - which has data protection implications which did not exist at time when the initial assessment was conducted
- Anything new which requires the collection of different personal information or which processes PI in a different manner

- Examples include – a mobile app; outsourcing a business function; a marketing and advertising campaign; an information sharing arrangement

SPECIFIC RETAIL SECTOR POPIA CONSIDERATIONS

- Loyalty and reward programs
- Ecommerce and the online retail world
- Direct Marketing

CLIFFE DEKKER HOFMEYR


Q
&
A