GDPR – oriented privacy laws in South Africa and Mauritius

South Africa and Mauritius

PROF. SIZWE SNAIL KA MTUZE

ADV. LEBOGANG STROOM-NZAMA

22 APRIL 2021

WEBINAR

INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

Introduction

- Protection of Personal Information Act 4 of 2013 (POPIA)
- Commencement : Definition section, Section which establishes the Regulator, Sections which empowers the Minister and the Regulator to make Regulations.
- 1 June 2021
- 1 July 2021

1. Difference most relevant for companies between the POPIA and the EU GDPR

Condition	
Condition 1 Accountability	Responsible party must ensure compliance with the conditions for lawful processing.
Condition 2 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

8 (Eight) Conditions for Lawfull processing

Condition	
Condition 3 Purpose Specification	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
Condition 4 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

8 (Eight) Conditions for Lawfull processing

Condition	
Condition 5 Information Quality	Personal information must be complete, accurate, not misleading and updated.
Condition 6 Openness	Responsible party must maintain records, Notification to data subject when collecting personal information

8 (Eight) Conditions for Lawfull processing

Condition	
Condition 7 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 be done 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.
Condition 8 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.

Key Definitions Difference

ROLE PLAYER	FUNCTION
Data Subject	Person to whom information relates
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 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.
Competent Person	Any person who is legally competent to consent to any action or decision being taken in respect of a matter concerning a child

2. How the Regulators educate the business communities

- Section 40 of POPIA provides for the powers, duties and functions of the Regulator.
- To provide education by promoting an understanding and acceptance of the conditions of the lawful processing of personal information, undertaking educational programmes, making public statements and giving advice.
- Stakeholder engagements

3. Typical complaints regarding companies

- Unsolicited direct marketing – Section 69
- Breach of personal information
- Data Breaches

4. How the Regulators investigate complaints by individuals and enforce the law regarding companies

Chapter 10 – Enforcement

Section 74 – any person may submit a complaint to the Regulator in a prescribed manner.

Section 76 – Action on receipt of complaint

Section 77 – Regulator may decide to take no action on complaint

Section 79 - Pre- investigation proceedings by the Regulator

Section 80 – Settlement of complaints

Cont.

- Section 81- Investigation proceeding of the Regulator
- Section 82 – Issue of warrants
- Section 92 – Referral to the Enforcement Committee
- Section 97 – Right of Appeal
- Civil Remedies

5.How the data privacy law is being implemented by multinational companies operating in or conducting outsourcing to SA

- Section 72 - Transborder Information Flows – Transfer of personal information outside South Africa.
- No transfer unless: Third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that:

Cont.

- effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information;
- Includes provisions that are substantially similar to this section, relating to further transfer of personal information from the recipient to third parties who are in a foreign country;
- The data subject consents to the transfer;

Cont.

- The transfer is necessary for the performance of a contract between the data subject and the responsible party or for the implementation of pre-contractual measures taken in response to the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

Cont.

- The transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the consent of the data subject to that transfer; and
- If it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

- 7.Links between the data privacy regulators and other regulatory authorities in each country

- 8.Links between the data privacy regulators and other data privacy regulators in Africa, and other regions of the world

Coming into effect of POPIA

POPIA came into effect on 01 July 2020, save for sections 110 and 114(4) which will be effective from 30 June 2021.

POPIA provides for a 12 months grace period, in terms of which the responsible parties are required to put measures in place to ensure that all processing of personal information are in compliance with POPIA.

Parts of POPIA which have already entered into force and those which will enter into force on 1 July 2021

- Proclamation of certain sections of POPIA:

1 July 2021:-

- Section 2 – 38
- Section 55 – 109
- Section 111 and
- Section 114 (1)(2) and (3)

30 June 2021:-

- Section 110 and 114(4)

The Regulator's investigation of breaches

- In the South African context, the importance of observing organizational and technical measures as required by the POPIA can never be overstated considering that during the course of August 2020, the entity known as 'Experian', which is a consumer, business and credit information service agency experienced a data breach.
- The Recent Experian Data Breach – A prelimenary report has been received from the External Independent Consultant and will be shared with Experian and the Public in due course.

- Other well publicized Data Breach include the email hack on Liberty Insurance where confirmation was given that the personal information of its Clients had been breached; the ViewFines Data Breach where the driving licenses of about 943 000 (Nine hundred and forty three thousand) road users whose names, personal identity numbers and email addresses in plain text on the ViewFines website were breached; the Data Breach at the offices of the Master of the High Court and the Deeds Registrar where varied personal information is held was breached;
- The hacking of the database of Ster-Kinekor in 2017, which contained names an email addresses of members of the public that use the movie house.

SECURITY SAFEGUARDS and POPIA

- Condition seven (7) of the eight (8) conditions for processing of personal information stipulates the security measures that the responsible party must put in place to ensure the integrity and confidentiality of personal information in its possession.

- These measures are provided for in sections 19 to 22 of POPIA.

- These security safeguards, if properly applied will contribute to the prevention of data leaks, which South Africa is currently experiencing.

SECURITY SAFEGUARDS (cont.)

- The Cybercrimes Bill once it becomes law will also deal decisively with cybercrime.
  - What are the obligations of a responsible party regarding security safeguards (section 19 – 22 of POPIA)
- The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking reasonable technical and organisational measures to prevent-
  - loss of, damage to or unauthorised destruction of personal information; and
  - Unlawful access to or processing of personal information.

SECURITY SAFEGUARDS (cont.)

- This in essence requires the responsible party to not only ensure the physical security of personal information in its possession, but also to ensure that the confidentiality of such information is secured.
- The responsible party must also actively familiarise itself with the security practices and procedure applicable to its industry and assess the efficacy of its security measures on an ongoing basis.
- The responsible party. For example, it provides that the controller and processor must implement appropriate technical and organisational measurers to ensure a level or security and confidentiality of data.

SECURITY SAFEGUARDS (cont.)

- Section 19 (2) of POPIA provides that in order to give effect to section 19(1), the responsible party must take reasonable measures to:

  (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

  (b) establish and maintain appropriate safeguards against the risks identified;

  (c) regularly verify that the safeguards are effectively implemented; and

  (d)ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

- The responsible party remains accountable for the processing of personal information by its representative or operator. Hence section of POPIA provides that an operator or any one processing personal information on behalf of an operator must:

SECURITY SAFEGUARDS (cont.)

- Section 22 of POPIA provides that where the responsible party has reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by unauthorised person, the responsible party must notify:
  - the Regulator and
  - the data subject, unless the identity of such data subject cannot be established
  - The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

SECURITY SAFEGUARDS (cont.)

-The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

- The manner of notification

- The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways:

(a) Mailed to the data subject's last known physical or postal address;

(b) sent by e-mail to the data subject's last known e-mail address;

(c) placed in a prominent position on the website of the responsible party;

(d) published in the news media; or

(e) as may be directed by the Regulator.

SECURITY SAFEGUARDS (cont.)

- The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

(a) a description of the possible consequences of the security compromise;

(b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;

(c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

(d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

- The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

Guidelines on the Registration of IO and the duties of IO under section 55 of POPIA

- The Information Officers and Deputy Information Officers are required, in terms of Section 55(2) of POPIA, to take up their duties only after being registered with the Regulator.

- The Information Officers of public and private bodies must perform their duties and responsibilities in terms of both PAIA and POPIA.

- The Regulator has published a Guidance Note on Information Officers and Deputy Information Officers on the website.

- An online portal for registration of information officers is being developed and registration is expected to take place on 1 May 2021.

- The development of Codes of Conduct i.t.o Section 60

- The Guidelines to develop Code of Conduct has been issues and published on the website.
- A standards for making and dealing with complaints under approved codes of conduct.
- A checklist that accompanies the Guideline to develop Codes of Conduct.

- The Credit Bureau Association (CBA) Notice on the website on receipt of the Code and invites written comments.


Thank
You
Merci
Obrigado
Asante
Multumesc
Spasibo
Maake
Grazie
Arigato
Vinaka
Dank Je
Matondo
Kiitos
Welalin
Juspaxar
Mamana
Kia Ora
www.shutterstock.com - 584483197

QUESTIONS ???