Privacy and Cybersecurity

Ridwaan Boda
Head of Technology, Media and Telecommunications Law
Member of the United Nations Global Pulse Privacy Advisory Group

Overview

- Status of POPI
- Overview of key concepts
- The POPI draft Regulations
- Elements of Proactive Compliance
- Implementing POPI
- GDPR – more of a concern than POPI?
- Cybersecurity Bill

Protection of Personal Information Bill

- 20 August 2013 - National Assembly passed the Protection of Personal Information Bill [B9D of 2009]
- 19 November 2013 - Signed into law by the President
- Section 115 - Act will come into force on a date to be determined by the President by proclamation in the Gazette
- 11 April 2014 - Regulations, Regulator and definitions

Protection of Personal Information Bill

- 24 July 2015: Parliament calls for nominations for candidates for five positions within the Regulator
- 13 April 2016: The Portfolio Committee on Justice and Correctional Services ("**the Committee**") shortlists 10 candidates for positions within the Regulator
- 17 May 2016: The Committee recommends that Adv. Pansy Tlakula be appointed as chairperson and four other candidates as members of the Regulator
- 1 December: Regulator appointed
- Regulations published recently in late 2017
- transitional period of 1 year

what is “personal information”?

information relating to an identifiable:

- living natural person
- existing juristic person as far as applicable

personal information

- race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture and birth
- education or medical, financial, criminal or employment history
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assigned to the person
- biometric information

personal information

- personal opinions, views or preferences
- the views or opinions of another individual about the person
- correspondence sent by the person that is implicitly or explicitly of a private/confidential nature
- the name of the person if it appears with other personal information relating to the person, or if the disclosure of the name itself would reveal information about the person

what is “processing”?

any activity concerning personal information, e.g.

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use
- dissemination by means of transmission, distribution or making available in any other form
- merging, linking, restriction, degradation, erasure or destruction of information

what processing activities are covered?

- processing of personal information by public and private bodies:
  - entered into a “record” – if recorded by non-automated means, it must form part of a **filing system** ; AND
  - by or on behalf of a responsible party that is:
    - domiciled in South Africa
    - not domiciled in South Africa, using automated or non-automated means situated in South Africa, unless only used to forward personal information through the Republic

POPI does not regulate:

- pure household or personal activities
- information that has been de-identified
- information by or on behalf of a public body - national security, defence or public safety, or prevention, investigation or proof of offences, the prosecution or the execution of sentences
- processing for purely journalistic purposes if subject to a code of ethics that provide adequate safeguards for protection

the 8 processing conditions

- **accountability.** Data controllers and responsible parties must comply with these eight principles
- **processing limitation.** Data should only be obtained by limited and lawful processing that does not unnecessarily infringe privacy
- **purpose specification.** The purpose for which personal data is collected must be specific, explicitly defined and lawful
- **further processing limitation.** Further processing must be compatible with the purpose for which data is collected

the 8 protection conditions (continued)

- **information quality.** Reasonably practicable steps to ensure personal information is complete, accurate, not misleading and updated
- **openness.** Notify the Regulator that it processes personal information where pre-approval is required and advise the data subject of certain mandatory information in regard to the collection
- **security safeguards.** The integrity and confidentiality of the personal information must be secured.
- **data subject participation.** The data subject has certain access rights , including a right to request its deletion

The draft POPI Regulations

- Comments by 7 November 2017
- Covers, inter alia:
  - Direct marketing
  - Request for deletion / correction of records
  - Duties of the information officer
  - Procedural matters

Elements of Proactive Compliance

- Understand the law – executive buy-in; initial training and awareness
- Appoint / reconsider / outsource role of information officer
- Implement Risk Management Framework (eg POPI Toolkit)
- Ongoing awareness, training and monitoring
- In addition, specific interventions required including:
  - Privacy By Design / Privacy Engineering
  - Privacy Impact Assessments and Data Flow Diagrams
  - Data Ethics Councils

POPI toolkit

- A copy of POPI and a copy of PAIA
- PAIA Manual as amended by POPI
- Personal Information Sharing Policy
- Global Data Protection Policy (“Binding Corporate Rules”)
- Website Privacy Policy
- Security Compromises Policy
- Subject Access Request Policy

POPI toolkit

- Compliance Self-Audit Assessment
- Model Data Processor / Operator contract
- Model clauses for contracts (including employment contracts and model consent clauses)
- Data Retention Policy
- BYOD Policy
- CCTV Policy
- Cookie Policy
- Sample posters for awareness programme
- List of Do's and Dont's

Practical Implementation

- Information Officer
- Information Audit
- “Touchpoints”
- Privacy Impact Assessments
- Privacy by Design
- Cybersecurity
- Stronger Contractual Frameworks
- Ethics Review Board

GDPR

- POPI not the only concern
- On May 25, 2018 the new set of privacy rules formed by the General Data Protection Regulation (GDPR) take effect.
- Every organization — regardless of its location — doing business with the EU market will need to make changes to its oversight, technology, processes, and people to comply with the new GDPR rules.
- Time is running out!

Cybercrimes and Cybersecurity Bill

- Bill in its second draft
- submitted to National Assembly on 21 February 2017
- public hearings held earlier this year; further hearings scheduled for later this year
- no timeline at this stage for finalisation of Bill

chapters in the Bill

- chapter 1 - definitions
- chapter 2 - cybercrimes
- chapter 3 - malicious communication
- chapter 4 - jurisdiction
- chapter 5 - powers to investigate, search and access or seize
- chapter 6 - mutual assistance
- chapter 7 - 24/7 point of contact
- chapter 8 - evidence
- chapter 9 - obligations of electronic communications service providers and financial institutions
- chapter 10 - structures to deal with cyber security
- chapter 11 - critical information infrastructure protection
- chapter 12 - agreements with foreign states
- chapter 13 – general provisions

aims of the Bill

- create cybercrime offences
- prescribe penalties for cybercrimes
- criminalise distribution of harmful data messages
- provide interim protection orders
- regulate jurisdiction for cybercrimes
- regulate power to investigate
- regulate aspects of mutual legal assistance
- establish 24/7 point of contact
- provide for proof of certain facts by affidavit
- impose obligations on electronic communications service providers and financial institutions to assist to investigate & report cybercrimes

aims continued

- provide for establishment of structures - promote cybersecurity & build capacity
- regulate the identification and declaration of critical information infrastructures
- creates measures to protect critical information infrastructures
- provide that the Executive may enter into agreements with foreign States to promote cybersecurity

cybercrimes

- cybercrimes detailed
  - s 2 - unlawful securing of access
  - s 3 - unlawful acquiring of data
  - s 4 - unlawful acts in respect of software and hardware tools
  - s 5 - unlawful interference with data or computer program
  - s 6 - unlawful interference - computer data storage medium or computer system
  - s 7 - unlawful acquisition, possession, provision, receipt or use or password, access codes or similar data or devices
  - s 8 - cyber fraud
  - s 9 - cyber forgery and uttering
  - s 10 - cyber extortion
  - s 11 - aggravated offences
  - s 12 – attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence
  - s 13 - theft of incorporeal
  - s 14 - penalties
  - s 15 - competent verdicts

Ridwaan Boda rboda@ensafrica.com

thank you

AFRICA

Contact

Ridwaan Boda

Director – ENSafrica

rboda@ensafrica.com

+27 (0)83 345 1119