IACT AFRICA

POPI PRODUCTS AND SERVICES

The Current State of the POPI Act/ POPIA in South Africa and the Role of Biometrics

John Cato, 083-726-9228
Certified Data Protection Officer (CDPO)
johnc@iact-africa.com
www.iact-africa.com/popi.html
www.popisolutions.co.za
https://eugdprsolutions.co.za

Contents

- POPI Act Background and Overview
- Current state of the POPI Act / POPIA in SA
- Security and Risk perspectives
- The Impact of the POPI Act on Biometrics
- The Role of Biometrics in POPI Act compliance
- How does the Security industry utilising biometrics comply with the POPI Act?
- Top 10 Tips for achieving and maintaining POPI Act compliance

IACT AFRICA

POPI PRODUCTS AND SERVICES

POPI Act/POPIA Background and Overview

Background to the POPI Act

- Where did it come from?
  - UK led the way, Data Protection Act, 1984
  - EU issued a directive in 1995 (3 year window)
  - UK and others complied with the EU in 1998

Data Protection Act 1998

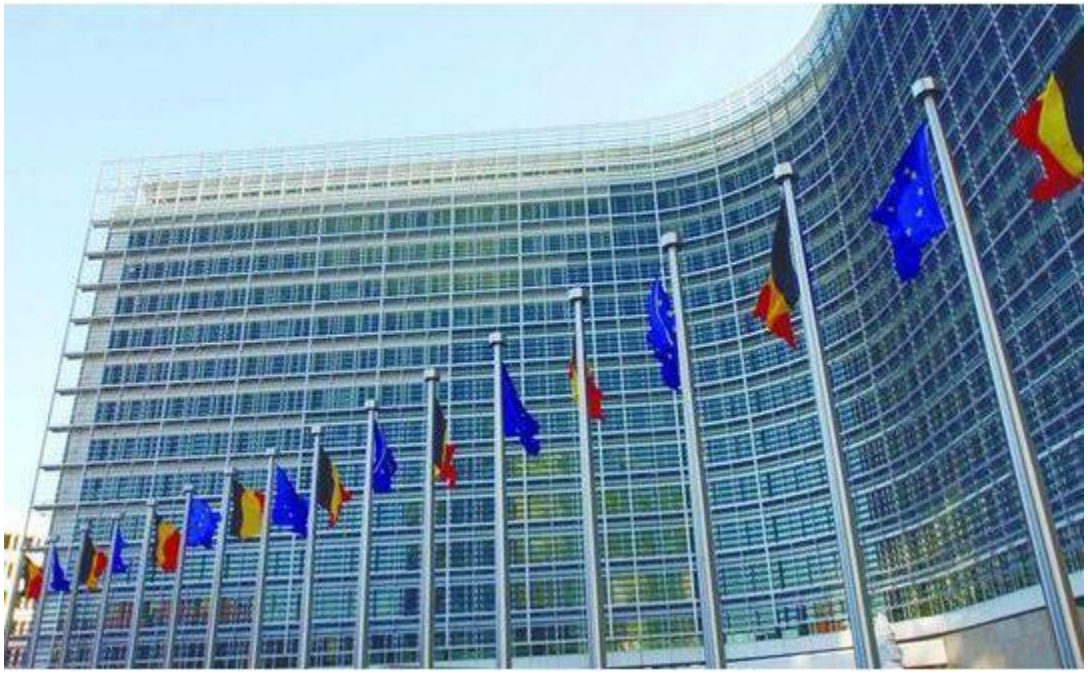
- What is the POPI Act?
  - A new (2013) law, in development for 10 years!
  - Gives us all better privacy rights as promised in the Constitution of RSA, 1994
  - A new way of thinking and acting

It is hereby notified that the President has assented to the following Act, which is hereby published for general information:–

No. 4 of 2013: Protection of Personal Information Act, 2013.

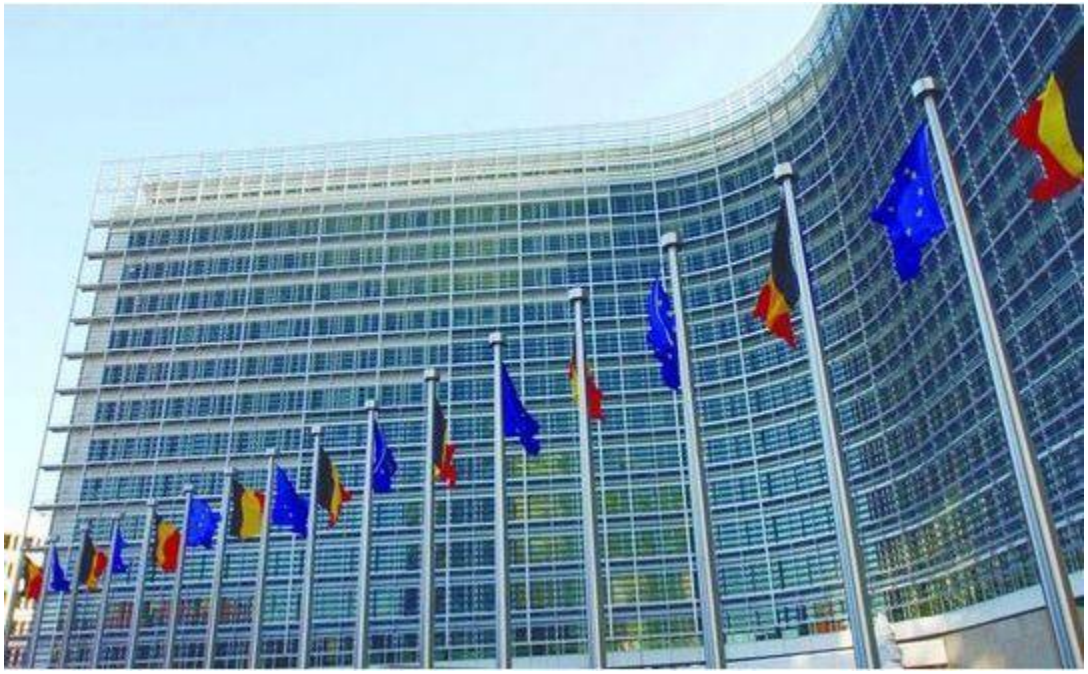
The first European Union Data Protection Directive was issued in 1995

- Privacy regulations were needed;
- POPI Act based on UK Data Protection Act;
- Alignment with international practices



EU General Data Protection Regulation (GDPR) replaces European Union Data Protection Directive

- EU GDPR was adopted on 27 April 2016
- Became effective on 25 May 2018
- Applies to all organisations outside the EU processing personal data of EU residents



The POPI Act: 8 Conditions (1)

Condition	Description
Accountability	Assigning ownership in your organisation
Processing Limitation	Processing information for lawful reasons and in a manner that does not infringe privacy (includes consent)
Purpose Specification	Only obtaining and holding personal information for a specific purpose
Further Processing Limitation	Further processing of personal information must be compatible with the purpose for which it was collected
Information Quality	Ensuring that personal information is complete, accurate and not misleading

The POPI Act: 8 Conditions (2)

Condition	Description
Openness	Informing individuals that their information has been obtained and the purpose thereof
Security safeguards	The integrity of personal information must be secured using appropriate, reasonable, technical and organisational measures
Data Subject Participation	A data subject has the right to request access to their personal information that you hold; to request the information is deleted or corrected if appropriate

Note: Consent and Purpose are key guiding principles when implementing personal information processes

The POPI Act: 6 Additional areas

- *Special Personal information*
- *Processing of personal information of children*
- *Designation and delegation of deputy Information officers*
- *Processing subject to prior authorisation*
- *Rights of data subjects regarding direct marketing*
- *Transborder information flows*

What is “Personal Information”?

“personal information” means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the 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 of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) 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 “Special Personal Information”?

Processing of special personal information

Prohibition on processing of special personal information

26. A responsible party may, subject to section 27, not process personal information concerning—

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(b) the criminal behaviour of a data subject to the extent that such information relates to—

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

WHAT IS PERSONAL INFORMATION?

Contact Details

Name
Email
Telephone
Address

History

Employment
Financial
Educational

Demographics

Age
Gender
Race
Weight

Correspondence

Private correspondence
Letters
Reports

Special Information

Religion
Ethic Origin
Trade Union
Health
Biometrics
DNA
Sexual Preferences
Criminal History

Children under 18

All information

Current status of POPI Act

....the POPI Act has been signed into law

- Under section 115 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), hereby fix 11 April 2014 as the date on which

  (a) section 1;

  (b) Part A of Chapter 5;

  (c) section 112; and

  (d) section 113,

  of the said Act come into operation.

Government Gazette

- Given under my Hand and the Seal of the Republic of South Africa at Pretoria on this seventh day of April Two Thousand and Fourteen.

....Information Regulator appointed

- On 26 October 2016, the long overdue appointment of the Information Regulator took place with Adv Pansy Tlakula being named as chair
- On 1 December 2016, the Information Regulator took up office in the Department of Justice and Correctional Services
- Responsible for regulating POPI/POPIA and PAIA laws

....Anticipated commencement of the POPI Act

- Draft POPI Act Regulations were published in September 2017
- Final POPI Act Regulations were published in the Government Gazette in December 2018
- Anticipated commencement date is Quarter Q2/Q3 2019
- Transition period (aka grace period) for compliance is expected to be 1 year

POPI Act role definitions

- Data subject: Living individual or juristic entity from whom PI is collected or about whom PI is processed
- Responsible Party: Organisation or individual processing the PI
- Operator: Service provider processing on behalf of the Responsible Party

Information Officer Responsibilities (1) (extract from POPI Act Regulations - 2018)

- A compliance framework is developed, implemented, monitored and maintained
- 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
- A manual (a PAIA manual) is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA
- The Information Officer shall upon request by any person, provide copies of the manual to any person upon the payment of a fee to be determined by the Regulator from time to time

Information Officer Responsibilities (2) (extract from POPI Act Regulations - 2018)

- The Information Officer shall upon request by any person, provide copies of the manual to any person upon the payment of a fee to be determined by the Regulator from time to time
- Internal measures are developed together with adequate systems to process requests for information or access thereto
- Internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
- Note: A Deputy Information Officer can be appointed to carry out these responsibilities

Business Reasons for complying with the POPI Act

- Business pressure is being applied by customers on service providers to demonstrate how they protect the personal information entrusted to them
- International pressure – data protection laws are becoming more prevalent in many countries, especially the EU – GDPR has global reach
- It demonstrate good governance, ethical and effective leadership
- It improves company image and gives competitive advantage
- It avoids reputational damage i.e. breaches that could be prevented

POPI Act
Risk and Security Perspectives

POPI Act Security Safeguards Condition (extract from section 19)

Security measures on integrity and confidentiality of personal information

- A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking **appropriate, *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
- Identify all reasonably foreseeable risks to PI (**See next slide**)
- The responsible party must have due regard to generally accepted information security practice and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations ***(ISO27000 series, NIST, etc.)***
- ***Written agreement*** between Responsible Party and Operator is required

POPI Act Risk Implications (extract from section 19)

In order to give effect to subsection (1), the responsible party must take reasonable measures 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; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

POPI Act Risk Management

- It is clearly stated in the POPI Act, section 109(3)(g) that fines will be higher where there is no evidence of:
  - Risk assessments completed
  - Operational policies, procedures and practices
- Management must therefore support
  - POPIA risk assessments and management
  - Development of good policies, procedures and practices
- Board/Committees/Exco must approve policies

Transborder Information Flows

Transfers of personal information outside Republic

- A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless –
  - The 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 th***at –
    - Effectively upholds principles for reasonable processing of the information ***that are substantially similar to the conditions for the lawful processing*** of personal information relating to data subject who is a natural person and, where applicable, a juristic person

Impact of POPI Act on Biometrics and the role they can play (1)

Biometric information is classed as Special Personal Information. Section 26 in the POPI Act states that Special Personal Information may not be processed unless:

- Consent is given by the data subject or;
- It is required for the establishment, exercise or defence of a right or obligation in law or;
- It is required to comply with an obligation to comply with an international public law or;
- Is processed by a body charged with applying criminal law e.g. criminal investigations

Impact of POPI Act on Biometrics and the role they can play (2)

Biometric information key risks:

- Failure to make the purpose of collecting biometric information clear to the data subject
- Failure to obtain consent for collecting biometric information from the data subject
- Technical/Data security risks (lack of technologies such as encryption, data loss prevention software, etc.)
- Service provider/operator risks – inadequate agreements
- Risk of biometric/ personal information being shared with other parties without the consent of data subjects

Impact of POPI Act on Biometrics and the role they can play (3)

Biometric technology mitigates many risks, for example:

- Time recording and Access Control systems: Manual clocking in/out processes for Staff including 'buddy clocking' – biometrics remove this risk
- Security/Access Control: Paper based Visitor books/sign-in sheets used by security companies - these can be viewed by anyone and passed on to other parties (a full book is often sold for as little as R 25) – biometrics remove this risk
- Authentication risks – unauthorised access to systems e.g. shared/lost passwords - biometrics reduce this risk
- Lost access cards - providing easy access to secure areas for unauthorised parties - biometrics remove this risk

Implementing Appropriate and Reasonable Security Measures (1)

Responsible Parties should:

- Adopt a Security Management Standard or Framework e.g:
  - ISO 27001/2 – the internal standard and code for an ISMS or;
  - NIST Cybersecurity Framework or;
  - UK Government Cyber Essentials Scheme
- Establish written agreements between the Responsible Party and Operator (service provider) in which specific commitment is obtained by the Operator to protecting personal information in accordance with the POPI Act and in which rights are included for the Responsible Party

Implementing Appropriate and Reasonable Security Measures (2)

- Ensure Cloud Service providers are certified in or aligned with a Cloud Security Standard or Framework e.g.
  - ISO 27018
  - Cloud Security Alliance (STAR program)
  - Ensure service contracts are compliant
- Operators/Processors (typically Cloud Service Providers):
  - Implement appropriate and reasonable compliance measures
  - Obtain certification in a Security standard
  - Obtain certification in a Cloud Security Standard or Framework
  - Offer compliant service contracts to clients
  - Cooperate with clients who table Responsible Party to Operator agreements

Implementing Appropriate and Reasonable Security Measures (3)

Remember:

- The required measures should be based on industry standards and frameworks, not specific security technologies
- Technologies are important but will not make you compliant on their own

How does the Security Industry Utilizing Biometrics Comply with the POPI Act? (1)

- Start a POPI Act compliance preparation project for your company as per the Top Ten Tips
- Place a focus on Security Safeguards by adopting a security standard or framework e.g. ISO27001 and demonstrate your alignment with these
- Implement policies & notices (privacy, security, etc.)
- Embed security technologies such as Encryption and Data Loss Prevention (data at rest, data in motion over networks, data in use) into all aspects of the biometric solution (from biometric devices to workstations, mobile devices and servers)

How does the Security Industry Utilizing Biometrics Comply with the POPI Act? (2)

- Replace paper based visitor books with digital solutions
- Amend systems/apps to include purpose and consent functionality
- Amend your service agreements, terms and conditions, etc. to include the rights and responsibilities of Responsibilities and Operators as appropriate
- If you are a service provider, assist your clients with appropriate notices which explain the purpose of collecting biometric and personal information and in obtaining consent from data subjects

How does the Security Industry Utilizing Biometrics Comply with the POPI Act? (3)

- Train your staff, especially those who are customer facing e.g. staff at security access points at businesses, residential estates, etc.
- Turn your compliance achievements into a business benefit – tell your customers and prospective customers about them
- Use it for competitive advantage

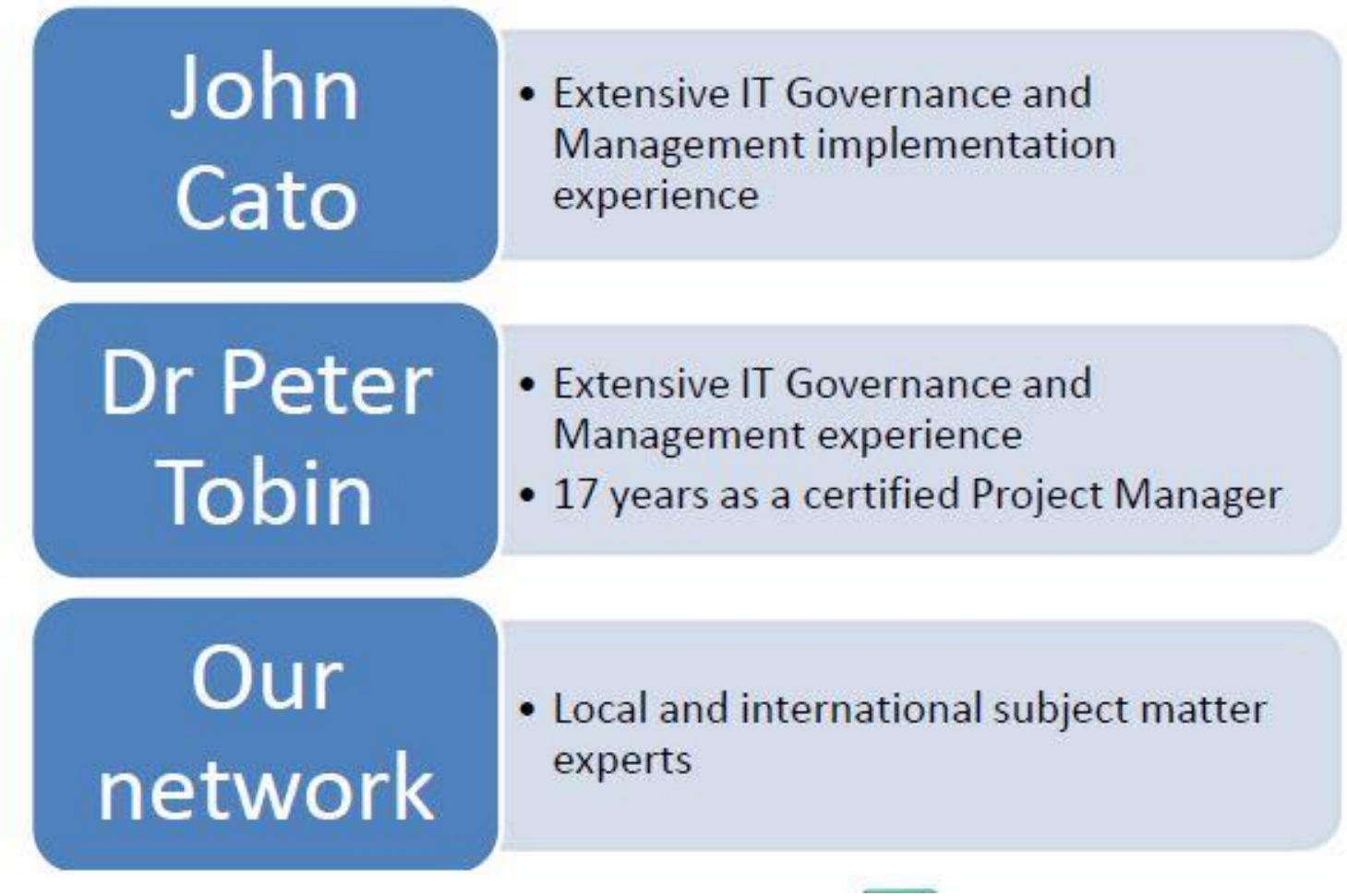
TOP TEN TIPS: becoming and remaining POPI Act (1)

1. Get approval for your POPI Act compliance project charter
2. Appoint your Information Officer
3. Assess your current status of compliance, include personal information risk assessments
4. Identify what Personal Information is processed; what records contain Personal Information; what user rights exist for your Personal Information
5. Develop & implement your POPI Act compliance privacy policy and notices (inform data subjects about the purpose of obtaining their information)

TOP TEN TIPS: becoming and remaining POPI Act compliant (2)

6. Review your website(s)
7. Review Service Provider Contracts and Implement appropriate Changes
8. Implement Personal Information management processes, including acquisition, processing, retention, security and destruction practices (include biometric processes)
9. Implement appropriate, reasonable, technical and organisation security measures which address identified risks (include biometrics risks)
10. Train staff on their role in POPI Act compliance

Who are we?

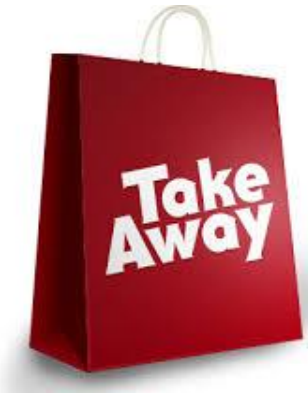


What do we offer?

A wide range of products and services with a focus on improving individual, team and organisation performance in the areas of POPI Act and EU GDPR Compliance as well as Information Security, IT Governance & Management and related topics

How can I find out more?

- Visit http://popisolutions.co.za , try our free online POPI Act Health Check and Cybersecurity Health Check
- Follow us on Twitter @sapopitalk



IACT AFRICA

POPI PRODUCTS AND SERVICES

THANK YOU