PSYCHOLOGY IN PUBLIC SERVICE division

PiPS

DEMYSTIFYING THE POPIA ACT

Barry Viljoen Clinical Psychologist
PS0128767

PsySSA
Psychological Society of South Africa

Overview of the Act

- The Protection of Personal Information Act (or POPI Act) is South Africa's equivalent of the EU GDPR.
- A COMBINAION OF THE POPIA (Personal Information) and PAIA Act (Access to Information)
- As the information office you become responsible for both of these
- Information Regulator has the power to regulate both these laws
- It sets some conditions for responsible parties (called controllers in other jurisdictions) to lawfully process the personal information of data subjects (both natural and juristic persons).
- The POPI Act does not stop you from processing and does not require you to get consent from data subjects to process their personal information.
- Whoever decides why and how to process personal information is responsible for complying with the conditions.
- There are eight general conditions and three extra conditions. The responsible party is also responsible for a failure by their operators (those who process for them) to meet the conditions.

Purpose

- **To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith.**

Legislative Underpinnings

- section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy;
- the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information;
- the State must respect, protect, promote and fulfil the rights in the Bill of Rights
  - consonant with the constitutional values of democracy and openness, the need for economic and social progress, within the framework of the information society, requires the removal of unnecessary impediments to the free flow of information, including personal information;
  - regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests,

- The POPI Act is important because it protects data subjects from harm, like theft and discrimination.
- The risks of non-compliance include reputational damage, fines and imprisonment, and paying out damages claims to data subjects.
- The biggest risk, after reputational damage, is a fine for failing to protect account numbers.

- The biggest impact is on organisations that process lots of personal information, especially *special personal information*, *children's information,* and *account numbers*.
- The most affected industries are financial services, healthcare, and marketing.

Concepts

- IR: Information Regulator
- IO: Information Officer
- D-IO: Deputy Information Office
- PAIA: Promotion of Access to Information Act
- Operator: A third party that handles personal information that the Practice would otherwise handle (Data Processor)
- Responsible Party: The Practice and all its staff contractors

Important Considerations

- Remember this hasn't taken the place of health laws, where in place.
- The protection and of disclosure to health is still in place
- POPIA makes it possible for this consent to be given verbally, however the national health act does not allow for this, without written consent
- Law (However we need to let people know that we are doing this in accordance with the law)
- Court order
- Between professionals within patient's interest (No consent required and necessary)(Patient entitled to a copy of letter of referral)

Medical Schemes Regulation (Medical Schemes Act)

- Only a general right to patient information if there is a manged care agreement between he provider and the scheme/administrator/ MCO
- Regulation 15A & J
- All accounts to a scheme must include an ICD Code (ie. Diagnostic/health condition code, patient must be informed)

What is personal information

- Race; gender; sex; pregnancy; marital status; nationality; ethnic or social origin ; colour; sexual orientation; age; physical or mental health; well-being; disability; conscience; belief; culture; lanaugue and birth
- Education; medical; finical; criminal or employment history
- Id number; symbol; email address; physical address; telephone number
- Blood type or any other biometric information
- Personal opinions, view or preferences
- The views or opinions of another individual about a person
- The name of a person if it appears with other personal information
- A child who is subject to parental control in terms of the law (Special Personal information)(Extra precautions required)
- A data subjects religious or philosophical beliefs

Processing

- Any activity or operation involving Personal Information, whether automated or not. It includeds the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of information.
- Ie. data bases; payroll etc.

POPI: Special Information (health and biometric

- Processing of this information is, in general, prohibited, unless consent has been provided; the data is necessary to exercise a right or fulfil a legal obligation; and sufficient guarantees for induvial
- Section 32 excludes from the prohibition: medical professionals and healthcare facilities, insurance companies and medical schemes/administrators deal with authorisations relating to health, but requires that information only be processed under a contractual duty of confidentiality, unless here is a legal duty to process information

Conditions for lawful processing

- Accountability – responsibility to ensure compliance
- Processing limitation – Lawful (information to be kept as long as you need it)
- Purpose specification – purpose specific and explicitly defined
- Further processing limitation – only if it formed part of originally obtained
- Information quality – responsible party to take steps to ensure info is complete, accurate, not misleading and updated
- Openness – Notifying data subjects, such as if the data-collection is mandatory or voluntary
- Security safeguards – list of measures that should be taken to prevent loss, damage, unauthorised and unlawful access.

- Step 1 Appoint IO and deputy (CEO)
- Responsible for the development and implementation of a Compliance Framework
- A personal information impact assessment
- Internal awareness sessions should be conducted regarding the
- Internal measure and adequate systems to process requests for information or access thereto must be developed
- Internal measures and adequate systems to process requests of the information

The IO must be trained

- They are the main contact with the information regulator and the public
- They are responsible for compliance with the POPI At and Regs and PAIA and Regs
- Both POPI and PAIA must be implemented

Step 2: PAIA Compliance

- Revamp/ update/ create a new PAIA Manual, use template
- Make sure the IO/ D-Ios know how PAIA works:
- Requester Form- check what right person wants to protect by accessing the info
- Check if they want info you must refuse
- Write back to say that you will supply by a date (you have 30 days)
- Disclose/ decline then before the 30 days

Impact Assessment

- List all sources of personal information
- If we have this, do we have more than we need?
- Measure the information and how that measures up against the Conditions of Processing

Security

- Breaches must be reported to the IR and you must inform those affected
- Ensure integrity and confidentiality
- Through appropriate, reasonable technical and organisational measures
- Prevent Loss/Damage/ Unauthorised destruction/Unlawful Access

Check/implement Policies contracts

- Check which Policies/ SOPs do you have in the Practice and are they all POPI aligned?
- Check which contracts you have
- Draft your POPI Policy/ Framework based on your analysis in Step 3 and 4
- Do I need more policies to govern this

Rights of data

- Notification when personal information is being collected
- Notified if there has been an unlawful access or acquisition of their personal information
- Request a record of your Personal Information
- Request the correction, deletion and or destruction of your Personal Information
- Object to the processing of Personal Information
- Exercise the right to withdraw the consent to processing, if voluntarily given
- Not to be subjected to automated decision-making on the personal information in contravention of section 71, POPI Act
- Submit a complaint to Information Regulator
- Institute civil proceedings

Consent to disclosure

- We use this when a patient wants you to disclose to their employer or issue a report to an insurer or submit chronic forms to a medical scheme or if a former partner is to be given information
- We need to ask the patient to complete this and to be specific with who, for what reason and for how long this information is to be shared
- Copy to patient and practice file

Report on disclosures

- This is done when disclosures are made that are not the regular, such as ICD 10 codes on scheme account or UIF to SARS
- Or say a patient has consented to whole file to attorney
- This should be done by completing the information so that there is an easy record of disclosures of personal information

Retention, archiving and destruction

- According to the act we must keep information as long as we need it.
- We need to decide how long we need this information for and to put that into our policy
- We need to be clear with when records are going to be archived
- When documents are to be destroyed and to have proof that these were destroyed

Section 34 Prohibition on processing personal information of children

- A responsible party may, subject to section 35, not process personal information concerning a child.

Section 35 General authorisation concerning personal information of children

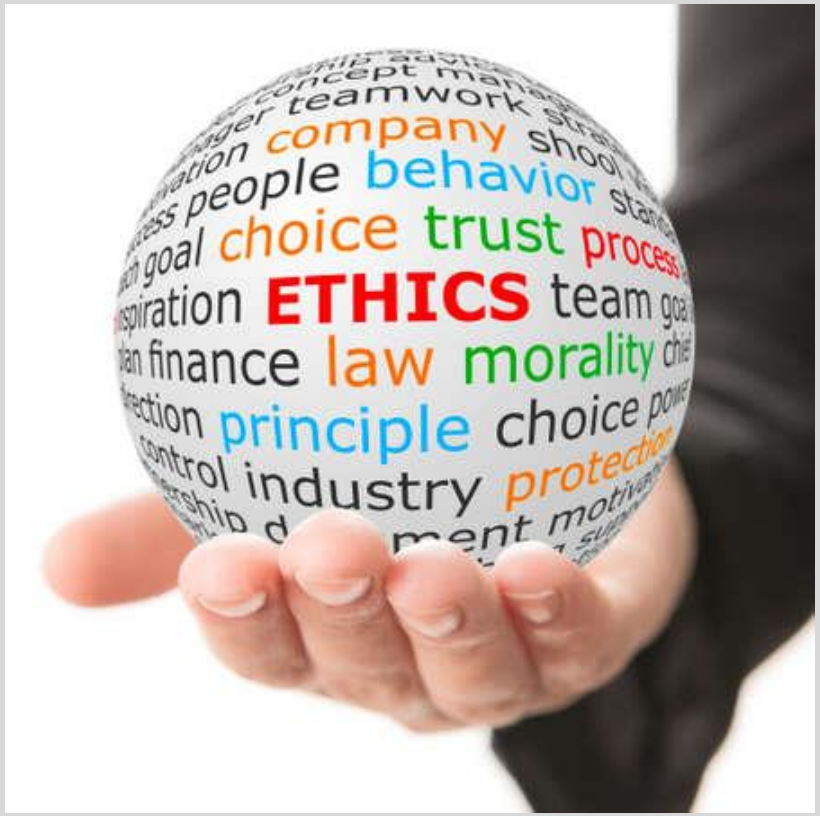
1. The prohibition on processing personal information of children, as referred to in section 34, does not apply if the processing is—
    1. carried out with the prior consent of a competent person;
    2. necessary for the establishment, exercise or defence of a right or obligation in law;
    3. necessary to comply with an obligation of international public law;
    4. for historical, statistical or research purposes to the extent that—
        1. the purpose serves a public interest and the processing is necessary for the purpose concerned; or
        2. it appears to be impossible or would involve a disproportionate effort to ask for consent,
        3. and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
    5. of personal information which has deliberately been made public by the child with the consent of a competent person.
2. The Regulator may, notwithstanding the prohibition referred to in section 34, but subject to subsection (3), upon application by a responsible party and by notice in theGazette, authorise a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.
3. The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2), including conditions with regard to how a responsible party must—
    1. upon request of a competent person provide a reasonable means for that person to—
        1. review the personal information processed; and
        2. refuse to permit its further processing;
    2. provide notice—
        1. regarding the nature of the personal information of children that is processed;
        2. how such information is processed; and
        3. regarding any further processing practices;
    3. refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and
    4. establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children

Section 4 Lawful processing of personal information

1. The conditions for the lawful processing of personal information by or for a responsible party are the following:

    1. "**Accountability**", as referred to in section 8;
    2. "**Processing limitation**", as referred to in sections 9 to 12;
    3. "**Purpose specification**", as referred to in sections 13 and 14;
    4. "**Further processing limitation**", as referred to in section 15;
    5. "**Information quality**", as referred to in section 16;
    6. "**Openness**", as referred to in sections 17 and 18;
    7. "**Security safeguards**", as referred to in sections 19 to 22; and
    8. "**Data subject participation**", as referred to in sections 23 to 25.

◦


company
people
behavior
goal
choice
trust
ETHICS
team
finance
law
morality
principle
choice
control
industry
protection

References

- Adams, R., Adeleke, F., Anderson, D., Bawa, A., Branson, N., Christoffels, A., De Vries, J., Etheredge, H., Flack-Davison, E., Gaffley, M., Marks, M., Mdhluli, M., Mahomed, S., Molefe, M., Muthivhi, T., Ncube, C., Olckers, A., Papathanasopoulos, M., Pillay, J., … Ramsay, M. (2021a). POPIA Code of Conduct for Research (with corrigendum). *South African Journal of Science*, *117*(5/6). https://doi.org/10.17159/sajs.2021/10933
- Bronstein, V., & Nyachowe, D. T. (2023). Streamlining regulatory processes for health researchers: To what extent does POPIA apply? *South African Medical Journal*, 30–33. https://doi.org/10.7196/SAMJ.2023.v113i8.781
- Da Veiga, A., Abdullah, H., Eybers, S., Ochola, E., Mujinga, M., & Mwim, E. (2024). Evaluating Data Privacy Compliance of South African E-Commerce Websites Against POPIA. *Journal of Information Systems and Informatics*, 6(4). https://doi.org/10.51519/journalisi.v6i4.917

- Jones, B. (2022a). IS POPIA BAD BUSINESS FOR SOUTH AFRICA? COMPARING THE IS POPIA BAD BUSINESS FOR SOUTH AFRICA? COMPARING THE GDPR TO POPIA AND ANALYZING POPIA'S IMPACT ON GDPR TO POPIA AND ANALYZING POPIA'S IMPACT ON BUSINESSES IN SOUTH AFRICA BUSINESSES IN SOUTH AFRICA IS POPIA BAD BUSINESS FOR SOUTH AFRICA? COMPARING THE GDPR TO POPIA AND ANALYZING POPIA'S IMPACT ON BUSINESSES IN SOUTH AFRICA. *Penn State Journal of Law & International Affairs*. https://elibrary.law.psu.edu/jlia/vol10/iss1/11
- Kumalo, M. O., & Botha, R. A. (2024). *POPIA Compliance in Digital Marketplaces: An IGOE Framework for Pattern Language Development* (pp. 331–346). https://doi.org/10.1007/978-3-031-64881-6_19
- Thaldar, D., Edgcumbe, A., & Donnelly, D.-L. (2023). How to interpret core concepts in POPIA? Recommendations on the draft Code of Conduct for Research. *South African Journal of Science*, *119*(7/8). https://doi.org/10.17159/sajs.2023/15062
- Thaldar, D., Townsend, B., Thaldar, D., & Townsend, B. (2021). *Exempting Health Research from the Consent Provisions of POPIA*. https://doi.org/10.17159/1727