Walter Tullis & Associates CC
FSP 8264 AUTHORISED FINANCIAL SERVICE PROVIDER 1996/037234/23
3D Bureau du Paul, 9 Corridor Crescent
Route N4 Business Park, Ben Fleur Ext 11
Emalahleni
tulliswt@iafrica.com
☎ (013) 690 1600 🖷 0866 300 410
Postnet Suite 280
Private Bag X7214
Emalahleni, 1035

POPIA

Protection of Personal Information Act

Act - https://popia.co.za/

Introduction

- POPIA **took effect on July 1, 2020**.
- POPIA **enforcement is scheduled to begin July 1, 2021**.
- **POPIA applies to any company or organization processing personal information in South Africa**, who is domiciled in the country, or not domiciled but making use of automated or non-automated means of processing in the country.
- **Transfers of personal information outside of South Africa is prohibited** by POPIA (with exceptions).
- **POPIA creates nine actionable rights for South African citizens** (data subjects), including but not limited to the right to access, right to correction and right to deletion.
- **POPIA also creates eight conditions for lawful data processing**, in which the consent of the data subject is central. It is up to websites, companies and organizations ("responsible parties") to prove that their processing is lawful, e.g. that correct consents have been obtained from users.
- **POPIA defines consent as any voluntary, specific and informed expression of will**.
- **POPIA defines processing as collection, receipt, recording, organization, storage, merging, linking**, and more.
- **POPIA defines personal information** broadly as any information relating to not only a living person, but also a company or legal entity.

POPIA creates nine actionable rights for SA citizens

Rights of data subjects

5. A data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3, including the right—

(a) to be notified that—
  (i) personal information about him, her or it is being collected as provided for in terms of section 18; or
  (ii) his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;

(b) to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of section 23;

(c) to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24;

(d) to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)*(a)*;

(e) to object to the processing of his, her or its personal information—
  (i) at any time for purposes of direct marketing in terms of section 11(3)*(b)*; or
  (ii) in terms of section 69(3)*(c)*;

(f) not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1);

(g) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71;

(h) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74; and

(i) to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99.

POPIA creates eight conditions for lawful data processing

CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

Part A

Processing of personal information in general

Condition 1

Accountability

8. Responsible party to ensure conditions for lawful processing

Condition 2

Processing limitation

9. Lawfulness of processing
10. Minimality
11. Consent, justification and objection
12. Collection directly from data subject

Condition 3

Purpose specification

13. Collection for specific purpose
14. Retention and restriction of records

Condition 4

Further processing limitation

15. Further processing to be compatible with purpose of collection

Condition 5

Information quality

16. Quality of information

Condition 6

Openness

17. Documentation
18. Notification to data subject when collecting personal information

Condition 7

Security safeguards

19. Security measures on integrity and confidentiality of personal information
20. Information processed by operator or person acting under authority
21. Security measures regarding information processed by operator
22. Notification of security compromises

Condition 8

Data subject participation

23. Access to personal information
24. Correction of personal information
25. Manner of access

Member: W.T. Tullis
Bachelor of Commerce (Economics)
Diploma in Financial Planning Diploma in Insurance
Certified Financial Planner Fellow of the Institute of Life and Pension Advisers Associate of the Insurance Institute of South Africa
Member: L Tullis
N Dip Electrical Engineering & Computer Systems

Purpose of the Popi Act

The purpose of the Popi Act is to:

- Protect your constitutional right to privacy by safeguarding your personal information when it is processed by a responsible party, subject to justifiable limitations to balance your right to privacy against other rights and particularly the right of access to information and protecting important interests, including the free flow of information
- Regulate the way personal information is processed by establishing conditions in line with international standards that prescribe the minimum requirements for lawful processing of your personal information
- Provide rights and remedies to protect your personal information from processing that is not in line the Act and
- Establish voluntary and compulsory measures, including the establishment of an Information Regulator to ensure to promote, enforce and fulfil your rights.

These are your rights

According to section 5, your rights are to:

- have your personal information processed according to the conditions for the lawful processing of personal information
- establish whether a responsible party holds your personal information and request access to it
- request, where necessary, the correction, destruction or deletion of your personal information
- object on reasonable grounds to processing of your personal information
- object to the processing of your personal information at any time if it is used for direct marketing
- refuse that your personal information is processed for direct marketing using unsolicited electronic communications
- refuse to be subject to a decision based solely on automated processing of your personal information to provide a profile of you
- complain to the Regulator about the alleged interference with the protection of your personal information
- institute civil proceedings if somebody interferes with the protection of your personal information.

Exclusions

According to section 6 of the act, it does not apply to the processing of personal information in the course of a purely personal or household activity or when it is done by or on behalf of a public body that involves national security, including the identification of financing terrorist and related activities, defence or public safety or to prevent or detect unlawful activities and prosecute offenders.

Conditions for legitimate use

The protection of your personal information form part of eight different conditions that will ensure your rights are protected, namely accountability, limited use, purpose specification, limited further use, information quality, openness, security safeguards and data subject participation.

Exemptions

The Regulator can grant an exemption for processing personal information even if it is in breach of a condition if it is in the public interest or it has a clear benefit for you and others that outweighs the chance of interference.
Public interest includes national security, the prevention, detection and prosecution of offences, important economic and financial interests, compliance with legal provisions, historical, statistical or research activity or freedom of expression.

Children

The personal information of children may not be used without consent. It can only be used if it is necessary to establish, exercise or defend a legal right or obligation, comply with international public law, for historical, statistical or research purposes, has been made public already with consent.

Direct marketing

Section 69 of the act provides that processing of personal information for direct marketing is prohibited unless you gave permission or are a client of the entity. Entities can also only ask you once for permission.
If you are a client your information can only be used if it was obtained when you gave it while buying a product or service or for direct marketing. You must also get the opportunity to object free of charge to the use of your information gathered during direct marketing.
Communication for direct marketing must identify the entity and give an address where you can ask for the communication to be stopped.

Where to complain:

Visit the Regulator's website on www.justice.gov.za/inforeg/index.html or send email to inforeg@justice.gov.za.

Physical and digital records:

Secure retention and destruction of physical PI records or deletion of electronic records are important steps to comply with the POPI Act. They also reduce the chances of data breaches taking place.

PI is only considered destroyed or deleted if it cannot be reconstructed in an intelligible form. Data breaches, particularly identity theft, often result when PI is incorrectly destroyed or deleted.
Certain business practices may lead to the insecure destruction of physical records. For example, criminals who 'dumpster dive' may find documents with PI that are routinely thrown out with ordinary refuse.

Securely destroying digital records may pose challenges, as multiple copies of PI may exist on your systems or devices, such as laptops and cell phones. All these records need to be deleted. It is therefore important to implement correct policies or practices in your business to destroy and delete PI. Your employees should also be trained accordingly.

Legitimate reasons to retain PI:

Section 14 of the POPI Act states that *"records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected."* So, PI must be destroyed as soon as reasonably possible after you no longer have any legal justification to retain it. Underestimating this obligation can cause considerable practical problems if not tackled systematically.
However, there are legitimate reasons to retain personal information. These are:

- If **required or authorised by law**. Labour legislation, the Companies Act and many financial services laws require you to retain PI.
- If you reasonably need the record for **lawful purposes related to its functions or activities,** such as contracts with clients that specify the terms of service or product offering. You can keep this PI only for as long as a legal liability or claim relating to the contract is possible.
- If a **contract** between parties requires retaining a record. The contract must specify the retention requirement and ideally the applicable time periods.
- If the data subject **consents** to the retention. Consent must be voluntary, specific and informed; it must never be assumed. To be able to make an informed decision, the data subject must be informed why retention is required and for how long.
- Records are often retained for **historical, statistical or research purposes.** This is a wide allowance that the regulator and courts will probably interpret this conservatively, given the nature and purpose of the act. You should be able to justify for what specific and reasonable historical, statistical or research purposes the retention is necessary.
- Safeguards should also be put in place to prevent the records from being used for any other purpose. If possible, it is advisable to 'de-identify' the PI. This entails destroying any information that: (1) identifies the data subject; (2) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (3) can be linked by a reasonably foreseeable method to other information that identifies the data subject.
- If PI is used **to make a decision about a data subject,** for example, if the data subject qualifies for a particular product or will be employed. This PI must be retained for any period required or prescribed by law or a code of conduct. If no period is prescribed, the period that will afford the data subject a reasonable opportunity to request access to the record applies, taking into account the intended use of the PI.

Destruction or deletion of PI

PI data is a crucial component of any business, and it is important to have a policy in place on how employees should treat this. Here are some practical tips to keep in mind when drafting such a policy:

- In essence, it should address how employees may obtain, create (for example unique identifiers), store, transmit, protect and destroy or delete PI.

- It must be simple, practical and easily executable. Employees should not be expected to spend excessive time sorting and managing PI records alongside their other duties.
- You need to identify what PI should be collected, where to store it and how to keep it secure. You also should assign a retention period to the PI when it is collected. Responsible parties operating in the financial services industry should give careful consideration to the retention periods that FICA and FAIS legislation require.
- Ideally you would have several retention periods to suit the different purposes for which the PI is used and the type of PI that need to be retained. When the longest allowed retention period expires, you no longer have a reason to keep the PI and all records of it should be destroyed or de-identified.
- You can securely destroy physical records by implementing a process, for example, shredding paper documents correctly on site. There should also be a policy to minimise the printing of records.
- When dealing with digital or electronic records, consider emails and the risks involved. Email should preferably not be a system of record keeping. Emails that need to be deleted should be fully deleted and not accessible in a deleted items folder.
- Also consider electronic PI that has been stored in a cloud or back-up. Records in the cloud should all be deleted or de-identified. Access to PI on servers or back-ups should be conservatively and responsibly managed.

Stakeholders in the financial services industry have concerns regarding what the reasonable retention periods for certain PI should be. It is foreseen that an industry specific code of conduct will be approved by the Regulator to help clarify the practical challenges and uncertainties relating to PI.
While retaining PI longer than you are legally allowed violates the POPI Act, compliance should not be your only consideration when managing PI. It is pointless to keep data that is not needed, cannot be retrieved efficiently or could be accidently accessed while you incur costs in attempting to securely store it. A data breach could affect a lot of PI data and negatively impact your business reputation.

Furthermore, as your clients trust you to manage their financial future, they also trust you to responsibly manage their PI. If you would like to discuss how to manage your clients' PI in line with the POPI Act requirements, please contact your Masthead consultant.