POPIA (Protection of Personal Information Act) Policy

Privacy Policy in terms of the Protection of Personal Information Act, No. 4 2013 (South Africa)

The President of the Republic of South Africa has indicated that the Protection of Personal Information Act 4 of 2013 will come into force on 1 July 2020. Due to the wide definition of personal information, the commencement of POPI will have far reaching implications for responsible parties.

1. Purpose

POPIA requires the Company to inform their clients as to how their Personal Information is used, disclosed and destroyed. The Company guarantees its commitment to comply with the law in respect of the data it holds about individual, follow good practice, protect staff and other individuals and protect the organisation from the consequences of a breach of its responsibilities. The Company will protect their client's privacy and ensuring their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

2. Definition of Personal Information

Information relating to identifiable individuals, in terms of the Protection of Personal Information Act, 2013 (hereinafter POPI Act). Such information includes but is not limited to:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, belief, culture, language and birth of the person;
- Information relating to the education or the medical, financial, criminal or employment history of the person;
- The e-mail address, physical address and telephone number of the person; ∞ the biometric information of the person;
- The personal opinions, views or preferences of the person; and

- 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.

3. Policy statement

The Company will:

- Comply with both the law and good practice;
- Respect individuals' rights;
- Be open and honest with individuals whose data is held; and
- Provide training and support for staff who handle personal data, so that they can act confidently and consistently.

The Company recognises that its first priority under the POPIA is to avoid causing harm to individuals, this means keeping information securely in the right hands, and retention of good quality information. Secondly, the Company will give individuals as much choice as is possible and reasonable over what data is held and how it is used.

4. Key risks

The Company has identified following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately);
- Failure to offer choice about data use when appropriate;
- Breach of security by allowing unauthorised access;
- Harm to individuals if personal data is not up to date;
- Data Operator contracts; and
- Information Officer Responsibilities.

5. Information Officer Responsibilities

As per Condition 1, and Chapter 5, Part B, the Information Officer has the following responsibilities:

- Developing, publishing and maintaining a POPI Policy which addresses all relevant provisions of the POPI Act, including but not limited to the following:

  - Reviewing POPIA and periodic updates as published;
  - Ensuring that POPIA induction training takes place for all staff;
  - Ensuring that periodic communication awareness on POPIA responsibilities takes place;
  - Ensuring that Privacy Notices for internal and external purposes are developed and published;
  - Handling data subject access requests;
  - Approving unusual or controversial disclosures of personal data;
  - Ensuring that appropriate policies and controls are in place for ensuring the Information Quality of personal information;
  - Ensuring that appropriate Security Safeguards in line with the POPIA for personal information are in place;
  - Handling all aspects of relationship with the Regulator as foreseen in the POPI Act; and
  - Provide direction to any Deputy Information Officer if and when appointed appointment.

The appointment of the Information Officer will be authorised by the CEO/MD/Director. Consideration will be given an annual basis of the re-appointment or replacement of the Information Officer; the need for any Deputy to assist the Information Officer.

6. Processing limitation

The scope of this aspect of the policy is defined by the provisions of POPIA, Condition 2. The key elements are:

6.1 Fit for a purpose:

Fit for purpose refers to the nature of the information collected and whether this information is specific and relevant for the intended purpose and not excessive. In simple words, if you are not actually using the information you collect then do not collect it.

6.2 Collection of information:

The method of information collection must be lawful and it should not infringe the privacy of the data subject. Practically this means that companies need to assess the processes they use for the collection of personal information.

6.3 Consent from data subject:

The data subject has to consent to the processing of personal information by the responsible party. The onus rests on the responsible party to provide proof of such consent. Furthermore, the data subject may withdraw consent at any time in which case the responsible party must stop processing this information. The data subject can also request that the responsible party destroy all such personal information. Effective controls will likely require, at a minimum, a register to be maintained.

6.4 Sourced directly from the data subject:

The final section of this condition relates to the collection of personal information directly from the data subject. Personal information must always be collected from the data subject, unless otherwise provided. There will be certain exceptions to the rule as in the case of conveyance. In this instance law firms will typically receive information pertaining to the bond transaction from the bank rather than the data subject. Law firms will need to be clear of their responsibility in terms of working with the information sourced from the bank.

7. Purpose specification

The '**purpose specification** principle', that is, the principle that a citizen needs to be informed why the personal data is being collected and the specific **purposes** for which it will be processed and kept, is a central protection for a citizen in data protection law.

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 3. The key elements of this condition are:

7.1 Collection for specific purpose:

Personal information should only be collected to fulfil a specific purpose. In addition to this, and barring the special conditions set in section 18 (4), the data subject must be made aware of the purpose for which the information is to be collected and processed and of course just what this information encompasses.

7.2 Retention and restriction of records:

As a general rule, the information collected should only be retained for as long as it is required for the completion of the task, however, records can be kept for statistical, historical or research purposes. In such instances, the onus rests on the responsible party to have appropriate safeguards in place to protect the information.

At the time when the information is no longer required the information must be de-identified or destroyed.

8. Further processing limitation

The scope of this aspect of the policy is defined by the provisions of POPIA, Condition 4. The fundamental principle underlying this condition is that the purpose for the further processing must be compatible with the original specified purpose.

The responsible party must determine whether there is alignment and in doing so should consider the following factors:

- The relationship between the purpose of the further processing and the purpose for which the information was originally collected;
- The nature of the information collected;
- The consequences that further processing will have for the data subject;
- The manner in which the information has been collected, and
- Any contractual rights and obligations between the parties.

In addition to the considerations above, there are circumstances under which further processing will be considered to be "not incompatible":

- The data subject has consented to the further processing of the information;
- The information is available in or derived from a public record or has deliberately been made public by the data subject;
- Further processing is necessary due to reasons relating to other legal processes, SARS, national security,
- The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to:

  (i) public health or public safety, or
  (ii) the life or health of the data subject or another individual.

- The information is used for historical, statistical or research purposes (with consent) and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or
- The further processing of the information is in accordance with an exemption granted under section 37.

9. Information quality

The scope of this aspect of the policy is defined by the provisions of POPIA, Condition 5. This condition is one of the broader conditions in the bill and simply states that the responsible party should ensure that the information collected or processed is accurate. In regard to the quality and completeness of the data, the responsible party should still collect and process information within the boundaries of the purpose specification.

The first step is to confirm that there are controls in place to ensure that those conditions relating to purpose specification (Condition 3 and Condition 4) are complied with. This will identify the correct information which you need to collect. Once collected, the next step is to implement controls which will ensure that the information is validated, ensuring the information quality. You

will further require a business process to flag when this information must be checked for validity including updates to the information. Typically this would be if information is only at some time after it was collected.

Data quality plays a major role during the data collection process, as it is at this point that data quality issues can be encountered and also corrected. Good collection practice will reduce the reliance on corrective controls. It should be noted that data collection is not always a manual process. Though this condition in the bill comprises only a few lines, the implementation of this should be carefully considered as data quality can be impacted at any point where a change to the data record is effected – from where it is collected initially and anywhere where it is exchanged from one system or department to another.

10. Openness

The scope of this aspect of the policy is defined by the provisions of POPIA, Condition 6.

There are two elements to this condition:

10.1 Notification to the Regulator:

The responsible party must inform the Regulator of its intention to process personal information before commencing with the processing of personal information intended to serve a single or different related purposes. However, compliance is not required if the responsible party compiles, or has compiled, a PAIA (Process of Access to Information Act) manual which includes the information as stipulated in section 58 of this bill and summarized as follows:

- The name and address of the responsible party;
- The purpose of processing;
- A description of the categories of recipients to whom the personal information may be supplied;
- Planned trans-border flows of personal information;
- A general description of the information security measures to be implemented by the responsible party to ensure the confidentiality, and

- Integrity and availability of information which is to be processed.

10.2 Notification to the Data Subject.

When personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of:

- The information being collected and if not directly from the data subject, the source from which it is collected;
- The name and address of the responsible party;
- The purpose for which the information is being collected;
- Whether or not supply of this information by the data subject is voluntary or mandatory;
- The consequences of failure to provide such information;
- Any particular law which authorizes or requires the collection of the information;
- The intention of the responsible party to transfer the information to a third country or international organization and the level of protection provided to this information by that country or organization;
- Any further information necessary to enable processing in respect of the data subject to be reasonable, taking into account the specific circumstances in which the information is to be (or not to be) for example:

  - Recipient or category of recipients of the information,
  - nature or category of the information,
  - existence of the right of access to and right to rectify the personal information collected,
  - the existence of the right to object to the processing of the information,
  - the right to lodge a complaint to the Information Regulator and contact details.

The data subject should be made aware of the above information prior to collection or in the instance where the information is collected from a source other than the data subject, as soon as reasonably practicable after the personal information is collected.

11. Security safeguards

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 7, Section 19 to 22.

This is the one point no firm can get away from, it's the one condition you cannot "make disappear" through specific clauses in the consent form received from the data subject.

The condition as per the law states:

"19. (1) 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—"

"technical measures" means information as it exists needs to be protected using technical means. Most of these are in all probability are already in place. These measures are to the likes of:

- Antivirus or Anti Phishing software;
- Firewalls on your network infrastructure;
- Unique and strong passwords on all computers, and
- Disk encryption (storing information on a computer or hard drive in a format that is not readable by someone without the computer password) for hard drives.

Avoiding negligence is what links the technical to the "organizational measures". It is therefore imperative for the Company to prove that they have implemented "reasonable organizational measures".

The organizational measures can be summarized as a set of business processes that the firm follows to ensure the confidentiality, integrity and availability of information is protected at all times.

12. Data Subject participation

The scope of this aspect of the policy is defined by the provisions of POPIA, Condition 8, Section 23 to 25.

The responsible party needs to facilitate data subject interaction with the personal information they hold. The Company will have to be able to allow for a Data Subject to interact with the personal information you possess. The Data Subjected interaction is in the form of a request; a request to either access, corrects or destroys the information.

Fees for access and procedures for access to personal information will be handled in compliance with the PAIA.

It is the Company's responsibility to provide proof of their actions. This identifies the requirement to keep an audit trail of all actions that were done on information.

13. Processing of special personal information

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Part B, sections 26 to 33.

The Company may not process personal information concerning:

- 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.
- The criminal behaviour of a data subject to the extent that such information relates to:

  - The alleged commission by a data subject of any offence, or
  - Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

The prohibition on processing personal information, does not apply if:

- Carried out with the consent of the data subject;
- It is obliged by law;
- It is necessary for to comply with an obligation of international public law;
- For historical data, statistical and research purposes;
- Information has deliberately been made public by the data subject, or
- Provisions of Sections 28 to 33 are (as the case may be) complied with.

14. Trans-border data flows

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Chapter 9, Section 72.

Section 72 does not prohibit cross-border data flows; rather it acts as an enabler and protector of personal information by providing a set of five (5) conditions / considerations which a responsible party needs to apply:

1. **The third party (recipient) is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection;**
2. d**ata subject consents to the transfer;**
3. **Transfer is necessary for the performance of a contract between data subject and responsible party,**
4. **Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject; or**
5. **Transfer is for the benefit of the data subject.**

At least one (1) of the five (5) conditions must be met and only then may the responsible party transfer a data subject's personal information outside of South Africa.

15. Training and acceptance of responsibilities

Information is contained in this policy document and other materials and/or training will be made available by / to the Information Officer.

Appointed employees will sign acceptance of this policy once they have had a chance to understand the policy and their responsibilities in terms of the policy / POPIA.

16. Policy review

An annual review will be completed prior to the policy anniversary date. The Information Officer will ensure relevant stakeholders are consulted as part of the annual review to be completed prior to the policy anniversary date.