PROTECTION OF PERSONAL INFORMATION

Framework, Procedures, Controls & Systems

for

Skylam 24 cc t/a Profin Financial Solutions & Profin Risk Solutions

(FSP No 10624, hereinafter referred to as the "FSP")

PHILOSOPHY

The scope of the Protection of Personal Information Act is very wide and applies to virtually everything that one might do with an individual's personal details, including details of one's employees. However, the right to privacy must be balanced against the need for the removal of unnecessary impediments to the free flow of information, including personal information.

The FSP wishes to ensure that personal data of clients is processed in accordance and adherence with the POPI Act and that the personal data is handled in accordance with POPI's data protection principles.

The application of the Act, if done in an orderly, ethical manner contributes significantly to society, the economy and the environment in which the FSP operates. By ensuring that it properly applies the requirements of the Act in a practical way, the FSP aims to guarantee the sustainable development of its business and promote the highest standard of services to clients while protecting their personal information.

PURPOSE

This policy creates an overarching framework that encompasses all aspects of the governance and compliance requirements for the business relating to the protection of personal information and sets out procedures that the FSP employs for the lawful processing of such information as a guide to the FSP and its personnel.

TABLE OF CONTENTS

1. INTRODUCTION

The Protection of Personal Information Act, No. 4 of 2013 ("the POPIA") gives effect to the constitutional right to privacy, in particular the protection against the unlawful collection, retention, dissemination and use of personal information.

An objective of POPI is to promote the right to privacy in our Constitution, protect the flow of information and at the same time expand the right of access to information. POPI determines the rights and duties that are designed to manage and safeguard personal data[1].

In terms of POPI, the justifiable needs of organisations to collect and use personal data for business and other purposes, are adjusted against the right of individuals to have their right of privacy, in the form of their personal details, acknowledged[2].

The core purpose of the Act is to ensure that individuals and juristic persons know exactly what is being done with their personal information.

In establishing adequate measures and controls to ensure compliance, Profin Financial Solutions are required to consider:

- What is done with personal information?
- How is personal information processed or shared?
- Who handles the personal information or with whom is it shared?
- What type of personal information is processed or shared?
- Why is personal information processed or shared?

POPI applies to a specific activity, namely the processing of personal data. The scope of personal information is very wide and applies to virtually everything that one might do with an individual's personal details including details of one's employees.

If information is collected or held about an identifiable individual or if the information is used, disclosed, retained or destroyed, one is likely to be processing personal data. Accordingly, if personal data is processed, POPI must be complied with and the data handled in accordance with POPI's data protection principles.

In principle, POPI:

- sets out the rules and practices which are to be followed when processing information about individuals;
- awards rights to individuals regarding their information; and
- produces an autonomous mechanism to enforce these rules, rights and practices.

[1] Sec.8 (a) & (b) of Protection of Personal Information Policy Act No. 4 of 2013
[2] Sec.9 of Protection of Personal Information Policy Act No. 4 of 2013

The introduction of the Protection of Personal Information Act (POPI) puts the onus on Profin Financial Solutions and its individuals to respect and protect the personal information they process during routine business, including personal information of customers, prospective customers, employees, and suppliers.

It is not limited to people but also applies to information about organisations, including communities and corporate entities.

2. POPI PRINCIPLES

Profin Financial Solutions complies with the eight principles as seen in POPI regarding the processing of personal information:

2.1 Consent

POPI requires for there to be a particular business purpose for the storage of personal information, such as "*where it is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party*"[3]; and explicit consent needs to be obtained from the relevant subject. When the subject is a child, this consent needs to be obtained from a competent person such as a parent or guardian.

2.2 Record Keeping

Storing an email address or cell phone number of a recipient who has opted for a newsletter is considered acceptable but recording someone's religious affinity may not be.

2.3 Collection of Data

Data should only be collected directly from the client themselves and only for a specific purpose, "*explicitly defined and … related to a function or activity of the responsible party*".[4]

2.4 Quality of Data

Personal information must be complete and accurate and be kept up-to-date and an up-to-date process must be in place, allowing individuals to request updates regarding personal information. If the personal information is no longer being used for a particular business purpose, it must be deleted or de-identified so that it cannot be associated back to an individual or Profin Financial Solutions, unless required by law.

---

[3] Sec.10(1) (b) of Protection of Personal Information Act, No. 4 of 2013

2.5 Ceased Communication

List of contacts that are no longer communicated with, must be deleted. However, email addresses or cell phone numbers of recipients who have unsubscribed from a list or complained about spam, can legitimately be retained to ensure the contacts are always filtered out of any communication.

2.6 Records

POPI requires that records be kept of what is done with the personal information. This will include all contact processing or subscriptions, when emails or SMSs were sent, or when the contact unsubscribed.

2.7 Security of Data

Always ensuring the safety, security and integrity of data is crucial to comply with POPI. Security procedures and passwords must be in place for individuals who have access to any system where data is stored. These security measures must extend to all internal processes, to ensure compliance when personal information is handled outside of the system. If security has been breached and personal information may have been accessed illegally, the Regulator and the client needs to be informed.

2.8 Offshore Data Storage

Many service providers in South Africa store their data in the USA. Under POPI, one is required to obtain consent to store personal information outside of the borders of South Africa. This is done by including a clause in your privacy statement on your website or referring to it when recipients subscribe to your newsletter. It can also be referred to in the footer of your emails to gain consent from existing subscribers.

2.9 Direct Marketing

It is now against the law to use direct marketing tactics (email and SMS marketing) to sell to a prospective customer without their consent. One may however contact a recipient once to obtain this consent (an opt-in campaign) and if they do not explicitly provide you with consent, all future communications must cease. Once a recipient opts-in, a method of unsubscribing must be provided as is the current standard practice.

3. IMPLEMENTATION OF POPI

“Processing” in terms of POPI has a wide-ranging meaning. It is intended to cover any conceivable operation on data, ranging from collecting, recording and holding, to the subsequent disclosure and eventual destruction of data. Going forward, it is of the utmost importance that any responsible party should review, on a regular basis,

its data processing activities. A responsible party being Profin Financial Solutions, should form a view and take steps to:

- fairly understand the data processing activities that an organisation engages in;

- training of relevant staff should be conducted on a continuous basis to ensure that staff are trained to understand the impact of POPI on their area of focus within the organisation;
- consider whether appropriate written contracts are in place with third parties for whom personal data is processed, or to whom the processing of personal data is outsourced;
- always evaluate the security measures in place to keep personal data secure;
- the terms under which intra-group transfers of personal data are made;
- consider, in detail, the cross-border transfer of personal data; and
- review internal procedures ensuring continued compliance with POPI and the effective and efficient handling of enquiries and complaints by individuals.

It is always important to note that the Profin Financial Solution's duties under POPI apply throughout the period that the FSP is processing personal data and so do the rights of individuals in respect of that personal data. Therefore, the FSP must comply with POPI from the moment it obtains the data, until the time when the data have been returned, deleted or destroyed. In addition, the duties extend to the way the organisation disposes of personal data when it no longer needs to keep such data. Data must be disposed of securely and in a way which does not prejudice the interests and rights of the individual concerned.

4. WHAT IS PERSONAL INFORMATION

Examples of personal information include:

- The client's identity number, name, surname, address, postal code, marital status, and number of dependants;
- The client's race, gender, sex, pregnancy, physical or mental health, well-being, religion, conscience, belief, culture, language and birth of the person;
- The client's national, ethnic or social origin;
- Description of the client's residence, business, assets, medical and financial information, banking details, criminal or employment history;
- Biometric information;
- Personal opinions, views or preferences of the person;
- Correspondence of a person which is explicitly of a private or a confidential nature, or correspondence that would reveal the contents of the original correspondence; and,
- Views or opinions of another individual about the person.

4.1 Client's Personal Information can only be used for Purpose it was collected/ agreed to[5]

This may include:

- Providing products or services to clients and to carry out the transactions requested;
- For underwriting purposes;
- Assessing and processing claims;
- Conducting credit reference searches or verification;
- Confirming, verifying and updating client details;
- For purposes of claims history;
- For the detection and prevention of fraud, crime, money laundering or other malpractices;
- Conducting market or customer satisfaction research;
- For audit and record keeping purposes;
- In connection with legal proceedings;
- Providing services to clients, to render the services requested and to maintain and constantly improve the relationship;
- Providing communication in respect of regulatory matters that may affect clients; and
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

4.2 Conditions under Which Personal Information may be Used

According to section 10 of POPI, personal information may only be processed by Profin Financial Solutions if certain conditions, listed below, are met, along with supporting information for the processing of personal information:

- The client consents to the processing: consent is obtained from client during the introductory appointment and needs analysis stage of the relationship[6];
- The necessity of processing: to conduct an accurate analysis of the client's needs for purposes of, amongst others, credit limits, insurance requirements, etc.;
- Processing complies with an obligation imposed by law;
- The Financial Advisory and Intermediary Services Act ('FAIS') requires Financial Service Provider's ('FSPs') to conduct a needs analysis and obtain information from clients about their needs to provide them with applicable and beneficial products;
- Processing protects a legitimate interest of the client – it is in the client's best interest to have a full and proper needs analysis performed to provide them with an applicable and beneficial product or service;

[5] Sec.14(1)(a(b)(c) of Protection of Personal Information Policy Act No. 4 of 2013
[6] Sec.14(1)(d) of Protection of Personal Information Policy Act No. 4 of 2013

- Processing is necessary for pursuing the legitimate interests of a third party to whom information is supplied to provide clients with products and or services or when both the FSP and any of the product suppliers require certain personal information from the clients to make an expert decision on the unique and specific product and or service required.

4.3 Disclosure of Personal Information to Associated Companies

The Profin Financial Solutions has agreements in place to ensure compliance with confidentiality and privacy conditions. The FSP may also disclose a client's information where one has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary to protect one's rights. Furthermore, the only information Profin Financial Solutions will ever disclose to third parties is aggregate information about its users. Aggregate information will not identify the website's users and will only identify the user's population in general terms.

4.4 Procedures to Protect Personal Information

The following procedures taken by FSP are in place to protect personal information:

- Appoint an Information Protection Officer whose details are readily available and who is responsible for compliance with the conditions regarding the lawful processing of personal information and other provisions of POPI[7];
- Relevant policy training needs to be implemented at all relevant levels;
- New employees should be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI[8];
- Current employees should be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;
- Archived client information should be stored on site; this is also governed by POPI, access is limited to these areas to authorised personnel;
- Product suppliers, insurers and other third-party service providers should be required to sign Service Level Agreements guaranteeing them commitment to the Protection of Personal Information; this would however be an ongoing process that is required to be evaluated as needed;
- All electronic files or data should be backed up by the IT division which should also be responsible for system security that protects third party access and physical threats. The IT division should be responsible for Electronic Information Security. Also note clients consent to the website's agreements, notices and disclosures by visiting the website and receiving electronic information or communication by electronic means and this indicates that any legal requirements has been satisfied.

[7] Sec.48(1) (a)-(d) and Section 48(2) of Protection of Personal Information Policy Act No. 4 of 2013
[8] Sec.47 of Protection of Personal Information Policy Act No. 4 of 2013

- Usually, the consent to process client information is obtained from clients (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and needs analysis stage of the relationship.

4.5 Website Disclaimer

- Profin Financial Solutions has and will continue to take reasonable care to ensure that all information, in so far as this is under its control, provided on this website is true and correct.
- Profin Financial Solutions shall not be responsible for, and therefore disclaims any liability for, any loss, liability, damage (whether direct or consequential) or expense of any nature whatsoever which may be suffered as a result of or which may be attributable, directly or indirectly, to the use of or reliance upon any information, links or service provided through this website.
- There is no warranty of any kind, expressed or implied, regarding the information or any aspect of this service. Any warranty implied by law is hereby excluded except to the extent such exclusion would be unlawful.

4.6 Links to other sites

Our website contains links to other sites. Please be aware that Profin Financial Solutions is not responsible for the privacy practices of such other sites. We encourage users to be aware when they leave our site and to read the privacy statements of each and every website that collects personally

- identifiable information. This privacy statement applies solely to information collected by this website.

4.7 Access to and Correction of Personal Information

Clients have the right to access their personal information. Clients also have the right to ask to have their information updated, corrected or deleted on reasonable grounds. Once a client objects to the processing of their personal information, one may no longer process said personal information.
Profin Financial Solutions takes all reasonable steps to confirm the clients' identity before providing details of their personal information or making changes to their personal information. If a client is unsatisfied with said information, they may notify Profin Solutions on the following email address: rob@profinbrokers.co.za

4.8 Records that Cannot be Found

Searches where records are believed to either not exist or that cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken in the attempt to locate the record.

5. POLICY REVIEW AND AMENDMENTS

It is a requirement of POPI to adequately protect personal information. The FSP will continuously review security controls and processes to ensure that personal information is secure.
Amendments to, or a review of this policy, should take place on an adhoc basis or at least once a year. Clients should be advised to access the FSP's website periodically to keep abreast of any changes. Should material changes take place, clients will be notified directly, or changes will be stipulated on the relevant website.

6. CONCLUSION

It is important that every organisation understands at minimum the following about POPI compliance:

- the legitimate grounds for collecting and using personal data collected to ensure that data is not used in ways that have unjustified adverse effects on the individuals concerned;
- the lawful purpose for which data are being collected to ensure that the data shall not be further processed in any manner that is contrary to that purpose or the purposes for which the data were collected;
- the extent of information that is required for the purpose as intended and to ensure that they collect adequate and relevant information and prevent any excessive information collection;
- the information retention periods and requirements applicable together with destruction processes and procedures;
- the rights of individuals, i.e. data subjects, in terms of POPI;
- security measures required to prevent the unauthorised or unlawful processing of personal data or access to personal data, including accidental loss or destruction or damage to personal data;
- when it becomes necessary to transfer data outside the country, to understand the roles, duties and responsibilities of all parties involved; and
- what processes and procedures should be in place to ensure that data is always kept up to date and current and accurate.