Business Management Software

# PROTECTION OF PERSONAL INFORMATION

## Framework, Procedures, Controls & Systems

## for

## Skyetek (Pty) Ltd

(hereinafter referred to as “Skye”)

## 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.

Skye 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 Skye operates. By ensuring that it properly applies the requirements of the Act in a practical way, Skye 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 Skye employs for the lawful processing of such information as a guide to Skye 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, Skye is 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 Skye 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

Skye 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 Skye, 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

We will only transfer personal information across South African borders if the relevant situation requires trans-border processing, and will do so only in accordance with POPIA.
When our operators are located overseas, we will take steps to ensure that our operators are bound by laws, binding corporate rules or binding agreements that provide an adequate level of protection and uphold principles for the reasonable and lawful processing of personal information, in accordance with POPIA.

## 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. Skye being a responsible party has taken steps to:

- understand the data processing activities that our organisation engages in;
- training relevant staff and planning continuous updates annually to ensure that staff understand the impact of POPI on their area of focus within the organisation;
- ensure that where 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;
- evaluate the security measures in place to keep personal data secure;
- analyse 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 Skye's duties under POPI apply throughout the period that Skye is processing personal data and so do the rights of individuals in respect of that personal data. Skye will 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.
- Contact data - includes billing address, postal address, email address and telephone numbers (of billing contacts and users).
- Financial data - includes bank account and payment card details, information included in VAT certificate/TAX clearance certificates, debit order forms and bank statements for certain clients.

- Transaction data - includes details about payments to and from you and other details of products and services you have purchased from us.
- Technical data -includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website, products you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs).
- Profile data - includes your username and password, purchases or orders made by you and any requests for support, your interests, preferences, feedback, survey responses, entries to competitions or promotions, and where you have registered for training or an event.
- Usage data - includes information about how you use our website, products and services.
- Marketing and communications data - includes your preferences in receiving marketing from us and our third parties and your communication preferences.

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

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information:

- Where we need to perform the contract we have entered into with you; or
- Where it is necessary for our legitimate interests (or those of a third party); or
- Where we need to comply with a legal or regulatory obligation; or
- Where you have agreed to us processing your personal information.

The purposes for which we will use your personal information may include:

- Providing products or services and to carry out the transactions requested;
- Conducting credit reference searches or verification;
- Confirming, verifying and updating client details;
- 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, rendering the services requested and to maintain and constantly improve the relationship;
- Providing communication in respect of regulatory matters that may affect clients; and

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

- 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 Skye if certain conditions, listed below, are met, along with supporting information for the processing of personal information:

- **The client consents to the processing:** Skye clients [6] use the software provided by the contract to save client, employee and provider personal information
- **The necessity of processing:** we are required to save your company personal information and that of your employees and clients on the Skye software;
- **Processing complies with an obligation imposed by law**;
    - Legislative requirements including the Financial Advisory and Intermediary Services Act, FICA and the General Code of Conduct for FSP's require the saving of client records. This information is stored on the Skye software;
- **Processing protects a legitimate interest of the client** – it is in our client's best interest to make use of secure technology to save employee, supplier and client personal information.;
- 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 Skye 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.

We have set out below a description of all the ways we plan to use your personal information:

•To register you as a new customer

•To process and deliver your order including (a) to manage payments, fees and charges; and (b) to collect and recover money owed to us

•To manage our relationship (and, if applicable, our agreement) with you which will include: (a) updating our customer relationship management system with information about you and our dealings with you; (b) notifying you about changes to our terms or privacy notice, and (c) asking you to leave a review or take a survey

•To administer and protect our business and website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)

•To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you

•To use data analytics to improve our website, products/services, marketing, customer relationships and experiences

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

•To make suggestions and recommendations to you about goods or services that may be of interest to you

## 4.3 Disclosure of Personal Information to Associated Companies

Skye has agreements in place to ensure compliance with confidentiality and privacy conditions. Skye 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 Skye 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.

External third parties (including contractors and designated agents) - Skye uses third-party service providers to help us with the following activities: workplace technology (e.g., document management and storage), hosting, communications (including audio and video conferencing) and marketing (e.g., notifications, surveys) and who may process your personal information while assisting us with these activities. Skye will provide details of these third-party service providers on request.

## 4.4 Procedures to Protect Personal Information

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

- We have appointed an Information Protection Officer (Rob Lansdell) who is responsible for compliance with the conditions regarding the lawful processing of personal information and other provisions of POPI[7] Rob may be contacted at 0415015300 or rob@skyetek.co.za ;
- Relevant policy training is implemented at all relevant levels;
- New employees are 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 are 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 where stored on site is also governed by POPI and access to these areas is limited to authorised personnel;
- Product suppliers and other third-party service providers have been required to sign Service Level Agreements where applicable guaranteeing their commitment to the Protection of Personal Information. This is an ongoing process that is evaluated as needed;
- All electronic files and data are backed up by the Skye IT division which is also responsible for system security that protects third party access and physical threats. The IT division is responsible for Electronic Information Security.

[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

- Consent to process client information is generally obtained from our clients (or a person who has been given authorisation from the client to provide the client's personal information) during the contractual stage of the relationship.
- We ensure that there are appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.
- We have put in place procedures to deal with any suspected security compromises and will notify you and the Information Regulator of a breach where we are legally required to do so.

## 4.5 Website Disclaimer

- Skye 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.
- Skye 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 Skye 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.
Skye 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 Skye on the following email address: rob@skyetek.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. Legal Rights

You have the right to make a complaint at any time to the Information Regulator, the South African supervisory authority for data protection issues:

Website: https://www.justice.gov.za/inforeg/

Email: complaints.IR@justice.gov.za

## 6. POLICY REVIEW AND AMENDMENTS

It is a requirement of POPI to adequately protect personal information. Skye will continuously review security controls and processes to ensure that personal information is secure.
Amendments to, or a review of this policy take place at least once a year. Clients are advised to access the Skye'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.

## 7. CONCLUSION

In conclusion, these are a summary of the most important aspects of POPI compliance:

- Skye has legitimate grounds for collecting and using personal data collected and will ensure that data is not used in ways that have unjustified adverse effects on the individuals concerned;
- There is a lawful purpose for which data is being collected and the company is committed 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;
- Skye will ensure that it complies with:
    - The requirements regarding the extent of information that is collected from our clients to ensure that it is only for the intended purpose, that we collect adequate and relevant information and prevent any excessive information collection;
    - the requirements and limits imposed regarding the retention periods of personal information and the destruction processes and procedures;
    - the rights of individuals, i.e. data subjects, in terms of POPI;

- Skye has security measures in place 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;
- Skye complies with POPIA requirements when it transfers data outside the country and understands the roles, duties and responsibilities of all parties involved; and
- Skye has processes and procedures in place to ensure that data is always kept up to date and current and accurate.