TOMLINSON & ASSOCIATES

PROTECTION OF PERSONAL INFORMATION POLICY

Policy statement and manual of Protection of Personal, Information and the Retention of Documents for Tomlinson & Associates (Pty) Ltd. (hereinafter referred to as the “Company” (Registration number: FSCA Number: 3952)

INDEX

1. INTRODUCTION 3
2. PERSONAL INFORMATION COLLECTED 3
3. THE USAGE OF PERSONAL INFORMATION 3
4. DISCLOSURE OF PERSONAL INFORMATION 4
5. SAFEGUARDING CLIENT INFORMATION 4
6. ACCESS AND CORRECTION OF PERSONAL INFORMATION 5
7. AMENDMENTS TO THIS POLICY 5
8. POLICY ON THE RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS 5
8.1 Purpose 5
8.2 Scope and Definitions 6
8.3 Access to Documents 6
8.4 Disclosure to 3rd Parties 7
8.5 Storage of Documents 7
8.6 Electronic Storage 7
8.7 Destruction of Documents 8
9. EMPLOYEE'S ACKNOWLEGEMENT OF RECEIPT .... **Error! Bookmark not defined.**

1. INTRODUCTION

1.1 TOMLINSON & ASSOCIATES is a company functioning within the financial services sector, that is obligated to comply with The Protection of Personal Information Act 4 of 2013. POPI requires THE COMPANY to inform their clients and employees / members as to the manner in which their personal information is used, disclosed and destroyed. The Company is committed to protecting its clients and employee's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws. The Policy sets out the manner in which the Company deals with their clients and employees / members' personal information as well as stipulates the purpose for which said information is used. The Policy is made available by request from the Company.

2. PERSONAL INFORMATION COLLECTED

2.1 Section 9 of POPI states that "Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."

2.2 The Company collects and processes employee's / members personal information pertaining to the employees / members fund and financial needs. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, the Company will inform the employee / member / fund as to the information required and the information deemed optional. Examples of personal information we collect include, but is not limited to:

2.2.1 The employee's / members Identity number, name, surname, address, postal code, marital status, and number of dependants;

2.2.2 Description of the employee's / members residence and business

2.2.3 Employment history

2.2.4 Any other information required by the Company or suppliers in order to provide employees / members with suitable assessment and requirement of needs.

2.3 The Company aims to have agreements in place with all product suppliers and third-party service providers to ensure a mutual understanding with regards to the protection of the employees / members personal information. The Company suppliers will be subject to the same regulations as applicable to the Company. With the employees / members / funds consent, the Company may also supplement the information provided with information the Company receives from other providers in order to offer a more consistent and personalised experience in the employees / members interaction with the Company. For purposes of this Policy, employees / members / fund includes potential and existing employees / members or funds.

3. THE USAGE OF PERSONAL INFORMATION

3.1 The Employees / members' Personal Information will only be used for the purpose for which it was collected and as agreed.

3.2 This may include:

3.2.1 Providing products or services to carry out the transactions requested;

3.2.2 Confirming, verifying and updating employee / members details;

3.2.3 Conducting employee / member or fund research;

3.2.4 For audit and record keeping purposes;

3.2.5 In connection with legal proceedings;

3.2.6 Providing the Company's services to employees / members / fund, to render the services requested and to maintain and constantly improve the relationship;

3.2.7 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

3.3 According to section 10 of POPI, personal information may only be processed if certain conditions, listed below, are met along with supporting information for the Company processing of Personal Information:

3.3.1 The employee / member / fund consents to the processing: - consent is obtained from employee / member / fund during the introductory, appointment and needs analysis stage of the relationship or as required;

3.3.2 The necessity of processing: in order to conduct an accurate analysis of the employees / members / fund's needs;

3.3.3 Processing complies with an obligation imposed by law on the Company;

3.3.4 Processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom information is supplied — in order to provide TOMLINSON & ASSOCIATES employees / members and funds with products and or services both TOMLINSON & ASSOCIATES and any of our product suppliers require certain personal information from the clients and employees / members in order to make an expert decision on the unique and specific product and or service required.

4. DISCLOSURE OF PERSONAL INFORMATION

4.1 The Company may disclose an employee's / member's personal information to any of the The Company approved product supplier or third-party service providers whose services or products clients require use of. The Company has agreements in place to ensure compliance with confidentiality and privacy conditions.

4.2 The Company may also share employees / members personal information with and obtain information about employees / members from third parties for the reasons already discussed above.

4.3 The Company may also disclose a candidate's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect the Company's rights.

5. SAFEGUARDING CLIENT INFORMATION

5.1 It is a requirement of POPI to adequately protect personal information. The Company will continuously review its security controls and processes to ensure that personal information is secure.

5.2 The Company's Information Officer is Cindy James whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI.

5.3 This Policy has been put in place throughout the Company and training on this policy and the POPI Act has been conducted by the Company.

5.4 Every employee currently employed by the Company has signed an addendum to their Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;

5.5 The Company's archived client and candidate information is stored off site through Office 365 Cloud which is also governed by POPI, access to retrieve information is limited to authorised personal.

5.6 The Company's product suppliers, insurers and other third-party service providers will be required to sign a Service Level Agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.

6. ACCESS AND CORRECTION OF PERSONAL INFORMATION

6.1 Clients / Employees / Members and Funds have the right to access the personal information the Company holds about them. Clients also have the right to ask the Company to update, correct or delete their personal information on reasonable grounds. Once a client / employee / member / fund objects to the processing of their personal information, the Company may no longer process said personal information. The Company will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

6.1.1 The details of TOMLINSON & ASSOCIATES 'S Information Officer and Head Office are as follows:

Information Officer CINDY JAMES
Telephone Number (011) 463 9499
E-Mail Address cindy@tmcons.co.za

Postal Address: 125 4th Street, Parkmore, Sandton
Physical Address: 125 4th Street, Parkmore,Sandton

7. AMENDMENTS TO THIS POLICY

7.1 Amendments to, or a review of this Policy, will take place on an ad hoc basis or at least once a year. Clients / employees / members / funds are advised to access the Company's website periodically to keep abreast of any changes. Where material changes take place, clients and candidate's will be notified directly or changes will be stipulated on the TOMLINSON & ASSOCIATES website.

8. POLICY ON THE RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS

8.1 Purpose

8.1.1 To exercise effective control over the retention of documents and electronic transactions:

8.1.1.1 as prescribed by legislation; and

8.1.1.2 as dictated by business practice.

8.1.2 Documents need to be retained in order to prove the existence of facts and to exercise rights the Company may have. Documents are also necessary for defending legal action, for establishing what was said or done in relation to business of the Company and to minimize the Company's reputational risks.

8.1.3 To ensure that the Company's interests are protected and that the Company's and employees / members / funds rights to privacy and confidentiality are not breached.

8.1.3.1 Queries may be referred to the Information Officer.

8.2 Scope and Definitions

8.2.1 All documents and electronic transactions generated within and/or received by the Company.

8.2.2 Definitions:

i. Clients and Employees / members / funds includes, but are not limited to, shareholders, debtors, creditors as well as the affected personnel and/or departments related to a service division of the Company.
ii. Confidential Information refers to all information or data disclosed to or obtained by the Company by any means whatsoever.
iii. Constitution: Constitution of the Republic of South Africa Act, 108 of 1996.
iv. Data refers to electronic representations of information in any form.
v. Documents include books, records, accounts and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro- mechanically or optically, or in any other form.
vi. ECTA: Electronic Communications and Transactions Act, 25 of 2002.
vii. Electronic communication refers to a communication by means of data messages.
viii. Electronic signature refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.
ix. Electronic transactions include e-mails sent and received.
x. PAIA: Promotion of Access to Information Act, 2 of 2000.

8.3 Access to Documents

All Company and client information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances (also see clause 20 b) below):

a. where disclosure is under compulsion of law;

b. where there is a duty to the public to disclose;

c. where the interests of the Company require disclosure; and

d. where disclosure is made with the express or implied consent of the client.

8.4 Disclosure to 3rd Parties

8.4.1 All employees / members / funds have a duty of confidentiality in relation to the Company, clients and employees / members / funds.

8.4.1.1 Information on clients and employees / members: Our clients' and employees / members' right to confidentiality is protected in the Constitution and in terms of ECTA. Information may be given to a 3rd party if the client or candidate has consented in writing to that person receiving the information.

8.4.1.2 Requests for company information:

8.4.1.2.1 These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Company, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

8.4.1.2.2 In terms hereof, requests must be made in writing on the prescribed form to the Information Officer in terms of PAIA. The requesting party must state the reason for wanting the information and has to pay a prescribed fee.

8.4.1.2.3 Confidential company and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Company must be kept strictly confidential at all times.

8.4.1.3 The Company views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

8.5 Storage of Documents

8.5.1 Hard Copies

8.5.1.1 Documents are stored in lockable storage at Tomlinson & Associates' office.

8.5.2 The FSCA requires a retention period of 5 years for the documents mentioned below:

8.5.2.1 adequate storage and filing systems for the safe-keeping of records, business communications and correspondence;

8.5.2.2 systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information, including:

8.5.2.2.1 electronic data security and internal and external cybersecurity;

8.5.2.2.2 system application testing;

8.5.2.2.3 back-up and disaster recovery plans and procedures for systems and electronic data

8.6 Electronic Storage

8.6.1 The internal procedure requires that electronic storage of information: important documents and information must be referred to and dis cussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.

8.6.2 Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

8.7 Destruction of Documents

8.7.1 Documents may be destroyed after the termination of the retention periods listed above.

8.7.2 Each department is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file.

8.7.3 After completion of the process the Principal Advisor and Information Officer shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by Registration.

8.7.4 The documents are then made available for collection by the removers of the Company's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.

8.7.5 Documents may also be stored off-site, in storage facilities approved by the Company.

8.7.6 The Company makes use of Metrofile for the storage of documentation both in hard copy and electronically (scanned and indexed). In addition, the outsourced function or activity must –

8.7.6.1 ensure that the person to whom the function or activity has been outsourced –

8.7.6.1.1 has the ability, capacity, and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally;

8.7.6.1.2 is able to carry out the outsourced services effectively, to which end the FSP must establish methods for assessing the standard of performance of that person;

8.7.6.2 have a written contract that governs the outsource arrangement and which clearly provides for all material aspects of the outsourcing arrangement, including:

8.7.6.2.1 addressing the rights, responsibilities, and service-level requirements of all parties;

8.7.6.2.2 providing for access by the Company and the Registrar to the person's business and information in respect of the outsourced function or activity;

8.7.6.2.3 addressing sub-outsourcing; and

8.7.6.2.4 addressing confidentiality, privacy and the security of information of the Company and clients of the Company.

8.7.6.3 properly supervise the carrying out of the outsourced functions, and adequately manage the risks associated with the outsourcing, including any risks to the Company's clients;

8.7.6.4 take appropriate action if it appears that the person may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements;

8.7.6.5 retain the necessary expertise to supervise the outsourced functions effectively and manage the risks associated with the outsourcing;

8.7.6.6 be able to terminate the arrangement for outsourcing where necessary without detriment to the continuity and quality of its provision of financial services to clients;

8.7.6.7 establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities;

8.7.6.8 have effective access to data related to the outsourced activities, including any data relating to the Company's clients, as well as to the business premises of the person; and ensure that the outsourcing arrangement does not

8.7.6.8.1 compromise the fair treatment of or continuous and satisfactory service to the Company's clients; or

8.7.6.8.2 result in key decision-making responsibilities being removed from the Company.