SESHEGO BENEFIT CONSULTING (PTY) LTD
2005/005855/07
AND
SESHEGO CONSULTING (PTY) LTD
2019/088330/07
("the Company")

PROTECTION OF PERSONAL INFORMATION POLICY

1. Introduction

This policy contains the guidelines to be followed by the Company after most of the remaining aspects of the Protection of Personal Information Act ("POPIA") were proclaimed by the State President with effect from 1 July 2020. This policy must become operationally effective within 12 months of 1 July 2020.

This Policy applies to all Officers of the Company, as well as all the Service Providers.

2. Purpose

The purpose of these guidelines, which have been adopted by the Company, is to protect stakeholders, and particularly clients, from harm by protecting their personal information. The aims of the guidelines are:

2.1 To introduce measures to prevent a financial exposure to the stakeholder e.g. money stolen due to inadvertent leakage of banking details and/or other sensitive information;
2.2 To prevent the stakeholder's identity being stolen;
2.3 Generally, to protect the stakeholder's privacy, which is a Companyamental human right and is also protected by the South African Constitution.

3. Definitions of the Role Players and special definitions involved in the implementation of the POPIA

3.1 **"Data Subject"** means the person to whom the information relates (in relation to the Company, this will normally be the member or the participating employer).
3.2 **"Information Officer"** means in relation to a private body (such as a company or other juristic person, including a retirement Company): the Chief Executive Officer or equivalent officer of the juristic person or any person duly authorized by that officer; or the person who is acting as such or any person duly authorised by such acting person.
3.3 **"Operator"** means the person who processes information on behalf of the responsible party, for example an IT vendor.
3.4 **"Officer/s"** means any of the Company's directors, chairperson or any other person appointed in a personal capacity by the Company to provide services to the Company.
3.5 **"Personal Information"** means Personal Information as defined in the POPIA.
3.6 **"Responsible Party"** means the person who determines why and how the information is to be processed.
3.7 **"Regulator"** means the Information Regulator, as defined in POPIA, who will have the power to investigate and if necessary fine responsible parties. Data subjects will be able to complain to the Information Regulator and the Regulator has the power to take any necessary action to protect the rights of Data Subjects. The current Information Regulator is Pansy Tlakula and the email address is inforeg@justice.gov.za.
3.8 **"Special Personal Information"** means special personal information as defined in Section 26 of the POPIA.
3.9 **"Service Provider"** means any entity or person that has been appointed by the Company to provide services to the Company in terms of an agreement.

4. What is Personal Information and what is involved in Processing of Information

4.1 Personal Information'' means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including:

4.1.1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or

social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

4.1.2. information relating to the education or the medical, financial or criminal or employment history of the person;

4.1.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;

4.1.4. the biometric information of the person;

4.1.5. the personal opinions, views, or preferences of the person;

4.1.6. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

4.1.7. the views or opinions of another individual about the person;

4.1.8. 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.

4.2 "Processing " means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

4.2.1. the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;

4.2.2. dissemination by means of transmission, distribution or making available in any other form; or

4.2.3. merging, linking as well as restriction, degradation, erasure or destruction of information.

In addition, certain information constitutes Special Information which must be treated more sensitively. All information pertaining to children is special information. Rulings from the GDPR suggest that biometric information may also be Special Information.

4.3 The Company will ensure that Personal Information is Processed lawfully and that the purpose for which it is Processed, is adequate, relevant and not excessive.

4.4 The following circumstances allows for the processing of the personal information by the Company, Officers and/or its Service Providers to be lawful:

4.4.1. To conclude or perform in terms of a contract

4.4.2. To comply with an obligation imposed by law

4.4.3. To protect the legitimate interest of the data subject

4.4.4. To perform a public law duty, as a public body

4.4.5. To pursue the legitimate interests of the responsible party or third party to whom the PI is given

4.4.6. If the data subject has consented

4.5 The Company acknowledges that obtaining consent from a Data Subject remains the most reliable form of justification for the Processing of Personal Information. The following applies

4.5.1. With regards to an employee, the employment contract provides that the employee has agreed to the right of the Company to Process such Personal Information pertaining to the employee as may be relevant to enable the Company to achieve the objectives of the Company and pay salaries in terms of the contract, subject to the provisions of the POPIA and any other applicable legislation; and

4.5.2. The Processing of certain activities of the Company and/or Service Providers will be justifiable based on the grounds that it is protecting one or other legitimate interest of a Data Subject.

4.6 The Company and/or a Service Provider shall take all reasonable steps to ensure that the Company and Data Subject's Personal Information is reliable and accurate, however it will be the Data Subject's responsibility to advise the Company and/or the Service Provider of any changes to his or her Personal Information, as and when these may occur.

5. Service Providers

5.1 The Company requires its Service Providers who are Processing Personal Information on behalf of the Company, to:

5.1.1. abide by the confidentiality principles and the principles contained in the POPIA, in particular but not limited to those principles relating to accountability, limitations on Processing of

information and purpose specification and other applicable laws governing the Processing of Personal Information, in order to ensure that all Personal Information provided to it by the Company is kept secure and confidential.

5.1.2. take reasonable steps to ensure (i) that only authorised personnel of the Service Provider has access to the Company and Data Subject Personal Information; (ii) that the Service Provider's personnel are aware of the Service Provider's obligations under the agreement with the Company and (iii) the reliability, integrity and trustworthiness of all of the Service Provider's personnel with access to the Company and Data Subject Personal Information.

5.1.3. ensure that the contract between the Company and Service Provider makes provision that (i) the Service Provider has an obligation to comply with the requirements of POPIA; (ii) has taken measures to prevent loss of, damage to or unauthorized destruction of Personal Information; (iii) has taken measures to prevent the unlawful access to or processing of Personal Information and (iv) shall not disclose the Personal Information to a third party.

5.1.4. notify the Company upon becoming aware of any breaches of the Personal Information in a timely manner.

6. Information Officer

6.1 In terms of POPIA, each organisation must appoint an Information Officer. The Company's Information Officer is the Managing Director.

6.2 An Information Officer's responsibilities include:

6.2.1. Notifying the Company upon becoming aware of any breaches of the Personal Information in a timely manner.
6.2.2. The encouragement of compliance by the Company with the Processing conditions;
6.2.3. Dealing with requests made by the Company, Regulator and/or a Data Subject pursuant to POPIA;
6.2.4. Working with the Regulator, the Operator, the Responsible Party, and the Company's Board of directors in relation to investigations conducted under POPIA in relation to the Company;
6.2.5. Otherwise ensuring compliance with the provisions of POPIA;
6.2.6. Developing, implementing, monitoring and ensuring a compliance framework;
6.2.7. Conducting and ensuring that a personal information impact assessment has been completed to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful Processing of Personal Information;
6.2.8. Developing, monitoring, maintaining and making available the Promotion of Access to Information Act ("PAIA") and POPIA manuals;
6.2.9. Developing internal measures together with adequate systems to process requests for information or access thereto;
6.2.10. Ensuring that internal awareness sessions are conducted.

6.3 The Company will be required to register the Information Officer with the Regulator. The Information Officer does not have any responsibilities and duties until the appointment is approved by the Information Regulator.

6.4 A request for access to Personal Information shall be directed to the Information Officer.

6.5 In terms of the Guidance Note issued by the Information Regulator (April 2021), the Information Officer must annually, and in terms of section 32 of PAIA, submit to the Regulator a report regarding:

6.5.1. the number of requests for access received;
6.5.2. the number of requests for access granted in full;
6.5.3. the number of requests for access granted in terms of section 46 of PAIA; the number of requests for access refused in full and refused partially and
6.5.4. the number of times each provision of PAIA was relied on to refuse access in full or partially;
6.5.5. the number of cases in which the periods stipulated in section 25(1) of PAIA were extended in terms of section 26 (1) of PAIA;
6.5.6. the number of internal appeals lodged with the relevant authority and the number of cases in which, as a result of an internal appeal, access was given to a record;
6.5.7. the number of internal appeals which were lodged on the ground that a request for access was regarded as having been refused in terms of section 27 of PAIA;
6.5.8. the number of applications to a court which were lodged on the ground that an internal appeal

was regarded as having been dismissed in terms of section 77 (7) of PAIA.

6.6 The Regulator may, annually, request an Information Officer of a private body, in terms of section 83 (4) of PAIA, to furnish the Regulator with information about requests for access to records of that body.

6.7 The Company and/or a Service Provider may not transfer Personal Information outside of South Africa unless prior permission has been obtained from the Information Officer and the transfer has complied with the requirements of POPIA.

7. Core Principles

7.1 Accountability: The Company needs to be responsible and accountable and must comply with the conditions of POPIA when processing the personal information of Data Subjects.

7.2 Limitations on Processing of Information: The following are the requirements for the processing of Data Subjects' information:

7.2.1. The Company must process personal Information lawfully and in a reasonable manner that does on infringe on the rights of the Data Subject.
7.2.2. The Company may only process Personal Information if, given the purpose for which it is processed, it is adequate, relevant and not excessive.
7.2.3. The Company may only process Personal Information with the consent of the Data Subject or if the above referenced justifications (clause 4.4) are applicable.
7.2.4. Personal information must be collected directly from the Data Subject except:
7.2.4.1. where the information is on public record or has been made public by the Data Subject;
7.2.4.2. the Data Subject has consented to collection from another source;
7.2.4.3. it is necessary to comply with a legal obligation, or legislation or legal proceedings;
7.2.4.4. it is not reasonably practical for the Company to collect the information directly from the Data Subject in the specific circumstances.
7.2.5. Processing of such Personal Information must be compatible with the original purpose for which it was collected.
7.2.6. In certain cases the consent of the Data Subject is not required, for example where Processing is necessary for the proper performance of a public law duty by a public body (for example any information relating to an individual's status with regard to Covid 19).

7.3 Purpose Specification: Personal information must be collected for a specific, explicity defined and lawful purpose related to a function or activity of the Company and the Data Subject must be made aware of the purpose for which their Personal Information is processed. The conditions applicable to the retention of Personal Information are set out in clause 10 of this policy.

7.4 Further Processing of Information: Further Processing of Information collected must be linked to the original purpose of the information being collected. The following five questions must be satisfied for further processing:

7.4.1. What is the relationship between the original purpose of processing and the intended further processing?
7.4.2. What is the nature of the information?
7.4.3. What are the consequences of further processing for the Data Subject?
7.4.4. Were there any disclaimers or *caveats* attached to the original collection of the information?
7.4.5. Is further processing connected to a contractual right or duty between the Company and the Data Subject?

7.5 All Personal Information collected must be accompanied by the Responsible Party's best endeavours to ensure the data is accurate, up to date and not misleading having regard to the purpose for which the information was processed. This also applies to back-ups.

7.6 Openness: The Company must take reasonable practical steps to ensure the Data Subject is aware of:
7.6.1. The information being collected.

7.6.2. The purpose for which information is being collected.
7.6.3. Contact details of the Information Officer for the Company.
7.6.4. Whether providing the information is voluntary or mandatory under legislation or in terms of a contract.
7.6.5. The consequences of failure to provide information.
7.6.6. Whether the Company intends to supply the information to a third party.
7.6.7. The right to lodge a complaint with the Regulator.
7.6.8. Any other information the Company deems necessary for the client.

The Data Subject must be made aware of the above before information is collected or as soon as is reasonably practical. It is not necessary to repeat the above for further collection of information from the client of the same kind. The Data Subject must be informed of the above in the privacy statement that is made available to all new members and/or existing members.

7.7 Security Safeguards:

7.7.1. The Company must take reasonable steps to ensure the confidentiality of Personal Information in its possession.
7.7.2. Personal Information may not be disclosed to a third party unless required by law or necessary for the performance of the Company's duties.
7.7.3. There must be a written contract between the Company and any third- party Operators.
7.7.4. The Company must be informed by the Operator if there have been any suspected/actual data breaches.
7.7.5. The Company makes use of the following Operators:
7.7.5.1. Accountants
7.7.5.2. IT consultants
7.7.5.3. Payroll administrators
7.7.5.4. Compliance officer

8. Processing of Special Information

8.1 The Company takes note that Processing of Personal Information which is regarded under Section 26 of POPIA as Special Personal Information is generally prohibited without the consent of the Data Subject, unless in certain circumstances specifically provided for in Section 27 - Section 35 of POPIA. Such information includes inter alia any information related to children, biometric information, criminal behaviour, race or ethnic origin, trade union membership, health or sex life and the religious or philiosophical beliefs of the Data Subject.

8.2 The Company may require access to the criminal behaviour of a Data Subject. In such case the Company shall adhere to the requirements authorizing the processing of Personal Information concerning a Data Subject's criminal behaviour as set out in Section 33 of POPIA.

8.3 The Company may process Personal Information related to children, as contemplated in Section 35 (c) of POPIA. The Company shall otherwise adhere to the provisions of Section 35 of POPIA and other relevant requirements of POPIA, and in particular if reasonably practical shall attempt to obtain the consent of a competent person before processing any Personal Information related to children.

9. Rights of the Data Subject

9.1 The Data Subject whose Personal Information the Company processes has the right to ask for any data maintained about them. They can also ask that the Company permanently delete this information, or update it. However, this does not replace the requirement to keep records for a period e.g. 5 years in terms of the FAISA and in accordance with clause 10 of this policy.

9.2 The Company maintains a manual in accordance with section 51 of the Promotion of Access to Information Act, No 2 of 2000 ("PAIA") and the POPIA. The PAIA sets out the procedural and other requirements which must be followed when there is a request for access to information. The Manual in terms of PAIA, adapted to comply with the requirements of POPIA, is available on request from the Company.

9.3 A Data Subject's Personal Information that is collected by the Company may be used for the following

reasons:

9.3.1. To comply with valid requests for information, including subject access requests and requests in terms of the Promotion of Access to Information Act 2 of 2000;

9.3.2. To comply with information requested by the Financial Sector Conduct Authority, the South African Revenue Service and any regulators or bodies lawfully requesting the information.

9.3.3. To enable the Company to achieve its objectives, which include inter alia the collection of contributions from the employer, the payment of benefits when the member exits the Company on retirement or on leaving service before retirement, or to the member's beneficiaries if the member should die while a member of the Company;

9.3.4. To enable the Company to insure risk benefits under policies in the name of the Company and the employer and the resultant medical underwriting of the risk benefits;

9.3.5. To comply with statutory and regulatory requirements in respect of the storage and maintenance of documents and information.

9.4 In making use of the Data Subject's personal information, the Company will comply with the conditions applicable to the processing of information as contemplated in the Protection of Information Act, Act 4 of 2013. The Data Subject has the following rights in relation to the Personal Information held by the Company:

9.4.1. The right to be informed that the Company is holding and using Personal Information for the specific purposes set out in clause 7 above;

9.4.2. The right of access to Personal Information held by the Company;

9.4.3. The right to rectify and/or up-date information held by the Company

9.4.4. The right to erase any Personal Information held by the Company; provided that in terms of Section 11 (b) of POPIA, the right of the Data Subject to request deletion of his Personal Information does not apply where the processing of the Data Subject's information is necessary in order to fulfil a contract to which the Data Subject is party, for example a contract between the Company, the Data Subject and another person in relation to a housing loan provided to the Data Subject with the Company acting as guarantor.

9.4.5. The right to restrict further processing of Personal Information for any purposes other than those set out in item 7 of this document;

9.4.6. The right to object, in particular, to further processing of Personal Information.

10. Security Policies

10.1 Clean desk policy: no files or other documentation should be left on Officer's desk at their place of business or in their homes. Anything constituting Personal Information should be kept under lock and key.

10.2 Unsolicited emails:

10.2.1. If an unsolicited email is from a pensioner or other fund member, or any stakeholder is received, a response advising that: Seshego is unable to assist and the email has been forwarded to the correct Operator concerned (or where applicable the respective fund's administrator); and to comply with legislation, the email will thereafter be deleted. Seshego will update their stakeholder agreements to explicitly detail what Personal Information Seshego will process and for what purpose, and anything falling outside the scope detailed in the agreement shall be handled in the abovementioned manner.

10.2.2. Should the unsolicited email contain a Curriculum Vitae ("CV") which could potentially be of value later, Seshego will advise the applicant that: the CV will be kept on our files for a maximum period of six months and on the expiry of the six-month period it will be deleted; and it is the responsibility of the applicant to advise Seshego of any changes in his or her circumstances which would require the CV to be updated.

10.3 **Underwriting**: in the event of medical underwriting being required by an insurers of a client, the process will be handled by a Seshego approved Operator, who will handle the requirements by dealing with the individual affected directly without going via a third party. The Seshego approved Operator will make summary reports available to the client after the removal of personal information i.e. names and surnames, etc.

11. Security Breach

11.1 If an Officer and/or Service Provider becomes aware of a security breach, such Officer and/or Service Provider shall immediately contact the Information Officer and advise that a security breach has occurred. The Information Officer must:

11.1.1. Establish the extent of the security breach and inform all stakeholders whose personal information might have been compromised by the breach. If the security breach arose because of an email being sent to an unintended recipient, the email transmitter is to immediately contact the recipient (both in writing and orally) and where possible request that the recipient sign an affidavit confirming that:

11.1.1.1. He or she has not relayed the email to any other party;
11.1.1.2. He or she has not printed or created a duplicate of the email;
11.1.1.3. The email has been permanently and irretrievably deleted; and
11.1.1.4. He or she will not verbally convey the contents of the email to any person.

11.1.2. Inform the stakeholders of the details and the extent to which their Personal Information may have been compromised by the security breach.
11.1.3. Inform the stakeholders of measures taken and what additional controls are being put in place, if necessary, to prevent a recurrence of the breach.
11.1.4. Inform the Regulator of the security breach as soon as possible.
11.1.5. Inform the stakeholders that if their identity has been compromised, to apply immediately for a free Protective Registration listing with Southern Africa Fraud Prevention Service (SAFPS) at protection@safps.org.za.

12. Retention of Information

12.1 The Company shall not retain Personal Information any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed unless:

12.1.1. retention of the record is required or authorized by law;
12.1.2. the directors reasonably require the record for lawful purposes related to the functions and activities of the Company;
12.1.3. retention of the record is required by a contract between the Company and its Operators, or any other party to the Company;
12.1.4. the Data Subject or a competent person (where the Data Subject is a child) has consented to the retention of the record.

12.2 The Company may retain records of Personal Information for periods in excess of those referred to in clause 11(1) for historical, statistical or research purposes if the Company has established appropriate safeguards against the record being used for any other purpose.

13. Complaints process

If a Data Subject has a privacy complaint against the Company, the Data Subject must lodge the complaint with the Company by putting the complaint in writing to the Information Officer. The Company is required to reply to the Data Subject within 30 days. If the Data Subject is not satisfied with such process, the Data Subject has the right to lodge a complaint with the Information Regulator.

JUNE 2021