BRAKECORE SUPPLY COMPANY (PTY) LTD

POPIA
PROTECTION OF PERSONAL INFORMATION ACT
&
(PAIA)
THE PROMOTION OF ACCESS TO INFORMATION ACT

POLICY

Date of Issue: 18 May 2021

TABLE OF CONTENTS

PART 1: GENERAL PRINCIPLES

1 POLICY STATEMENT

1.1 The purpose of this Policy is to develop and secure sound and sustainable management of the processing of Personal Information and, where relevant, Special Personal Information within the Company by establishing principles, norms, standards and other requirements to –

1.1.1 regulate the processing of Personal Information and, where relevant, Special Personal Information in a manner which complies with the provisions of the Act and gives effect to the right to privacy as envisaged in section 14 of the Constitution of the Republic of South Africa Act, No 108 of 1996, subject to justifiable limitations;

1.1.2 govern the manner in which Personal Information is collected, stored, recorded and transferred regardless of the form or medium thereof.

1.1.3 regulate and prescribe the retention of Records and the periods thereof; and

1.1.4 ensure compliance with all other relevant legislation which governs the processing of Personal Information.

1.2 Employees and other parties who are bound by or otherwise required to recognise and abide by this Policy who compromise or violate the provisions of this Policy could significantly damage the Company s' interests, including its relationships with third parties and its reputation, and expose it to un-intended consequences, risks and liabilities. Accordingly, any violation of this Policy will be subject to appropriate action by the Company, including *inter alia* possible termination of employment or damages claims, should circumstances so require.

2 DEFINITIONS

In this Policy, unless otherwise indicated by the context, the following terms shall have the meaning ascribed to them –

2.1.1 "**Act**" means the Protection of Personal Information Act, No 4 of 2013, as amended from time to time;

2.1.2 "**Business Day**" means a day which is not a gazetted public holiday, a Saturday or a Sunday;

2.1.3 "**CIPC**" means the Companies and Intellectual Property Commission established in terms of section 185 of the Companies Act;

2.1.4 "**Companies Act**" means the Companies Act, No 71 of 2008, as amended from time to time;

2.1.5 "**Company**" means Brakecore Supply Company registration number 1996/014634/07 and its subsidiaries from time to time;

2.1.6 "**Consent**" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information;

2.1.7 "**Data Subject**" means the person to whom the Personal Information relates;

2.1.8 "**Deputy Information Officers**" means those persons contemplated in paragraph 7.2.2;

2.1.9 "**Employees**" means individuals employed by the Company;

2.1.10 "**Information Officer**" means the individual contemplated in paragraph 7.2.1;

2.1.11 "**Operator**" means a person who processes Personal Information for the Company in terms of a contract or mandate, without coming under the direct authority of the Company;

2.1.12 "**PAIA**" means the Promotion of Access to Information Act, No 2 of 2000, as amended from time to time;

2.1.13 "**Personal Information**" means personal information as defined in the Act as contemplated in paragraph 10.1;

2.1.14 "**Policy**" means the policy set out in this document and includes all annexures hereto (if any) and any sub-policies prepared from time to time;

2.1.15 "**processing**" means processing as contemplated in paragraph 4.3;

2.1.16 "**public body**" means public body as defined in the Act;

2.1.17 "**Record**" means a record as defined in the Act and currently comprising of any recorded information –

2.1.17.1 regardless of form or medium, including any of the following –

2.1.17.1.1 writing on any material;

2.1.17.1.2 information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

2.1.17.1.3 label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

2.1.17.1.4 book, map, plan, graph or drawing;

2.1.17.1.5 photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.1.17.2 in the possession or under the control of a responsible party;

2.1.17.3 whether or not it was created by a responsible party; and

2.1.17.4 regardless of when it came into existence;

2.1.18 "**Regulator**" means the information regulator established in terms of section 39 of the Act;

2.1.19 "**Responsible Party**" bears the definition accorded to it in section 1 of the Act;

2.1.20 "**South Africa**" means the Republic of South Africa;

2.1.21 "**Special Personal Information**" means Personal Information concerning –

2.1.21.1 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; or

2.1.21.2 the criminal behaviour of a Data Subject to the extent that such information relates to -

2.1.21.2.1 the alleged commission by a Data Subject of any offence; or

2.1.21.2.2 any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings; and

2.1.21.2.3 any Personal Information concerning a child being a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

2.2 The words "**include**" and "**including**" mean "include without limitation" and "including without limitation". The use of the words "**include**" and "**including**" followed by a specific example or examples shall not be construed as limiting the meaning of the general wording preceding it.

2.3 Words and expressions defined in any paragraph shall, unless the application of any such word or expression is specifically limited to that paragraph, bear the meaning assigned to such word or expression throughout this Policy.

2.4 Unless otherwise provided, defined terms appearing in this Policy in title case shall be given their meaning as defined, while the same terms appearing in lower case shall be interpreted in accordance with their plain English meaning.

2.5 A reference to any statutory enactment shall be construed as a reference to that enactment as at the date of issue or date of revision as the case may be and as amended or substituted from time to time.

2.6 Unless specifically otherwise provided, any number of days prescribed shall be determined by excluding the first and including the last day.

2.7 Where figures are referred to in numerals and in words, and there is any conflict between the two, the words shall prevail, unless the context indicates a contrary intention.

2.8 In this Agreement the words "**paragraph**" or "**paragraphs**" and "**annexure**" or "**annexures**" refer to paragraphs of and annexures to this Policy.

3 INTRODUCTION

3.1 During the course and scope of its activities the Company obtains Personal Information from a variety of sources including Employees, and various third parties who may engage with the Company from time to time.

3.2 The Act governs the processing of Personal Information, including but not limited to Special Personal Information and imposes certain obligations on the Company in relation to this information and the manner in which it is processed.

3.3 Accordingly, the Company wishes to govern, regulate and administer the processing of Personal Information through this Policy in order to comply with the provisions of the Act.

3.4 Employees, volunteers and board and committee members of the Company shall be bound by, observe and implement this Policy at all times.

4 BACKGROUND TO THE ACT

4.1 The Act aims to give effect to the constitutional right to privacy by safeguarding Personal Information when processed by a Responsible Party. The Act sets forth various provisions which will, *inter alia*, regulate the way Personal Information may be processed.

4.2 The Act will apply to the processing of Personal Information entered in a Record by a Responsible Party by making use of automated or non-automated means, where the Responsible Party is either domiciled in the Republic or makes use of the automated or non-automated means in the Republic, unless those means are used only to forward Personal Information within the Republic.

4.3 For the purposes of the Act, "processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

4.3.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

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

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

4.4 The Act prescribes certain conditions for the lawful processing of Personal Information which can be summarised as follows –

4.4.1 *Condition 1: Accountability*: The Responsible Party (i.e. in this instance, the Company) must ensure that measures are taken which give effect to the conditions set out in the Act.

4.4.2 *Condition 2: Processing Limitation*: Personal Information must be processed lawfully and in a reasonable manner that does not infringe the privacy of a Data Subject. Personal information may only be processed if, given the purpose for which it is processed, the processing is adequate, relevant and not excessive. Further, subject to certain exceptions, personal information may only be processed with the Consent of a Data Subject and must be collected directly from a Data Subject.

4.4.3 *Condition 3: Purpose Specification:* Personal Information must be collected for a specific, explicitly defined and legitimate purpose. Personal Information may also not be kept for longer than is necessary for achieving the purpose for which it is collected or subsequently processed.

4.4.4 *Condition 4: Further Process Limitation:* Personal Information must not be further processed in a way incompatible with a purpose for which it has been collected in the first instance.

4.4.5 *Condition 5: Information Quality:* The Responsible Party must take reasonable practical steps to ensure that the Personal Information is complete, accurate, not misleading, and updated where necessary.

4.4.6 *Condition 6: Openness:* The Responsible Party must maintain the documentation for all processing operations in accordance with its responsibility referred to in sections 14 and 51 of PAIA. Further, if Personal Information is collected, the Responsible Party must take reasonably practicable steps to ensure that the Data Subjects are, *inter alia*, aware of the information being collected and the purpose for such collection.

4.4.7 *Condition 7: Security Safeguards*: Appropriate technical and organisational measures must be taken to secure the integrity of Personal Information by safeguarding against

the risk of loss or damage or destruction of Personal Information and against the unauthorised or unlawful access to, or processing of Personal Information.

4.5 We will refer to these conditions where relevant herein and particularly the applicability thereof to the activities of the Company.

5 PURPOSE

5.1 The Company is exposed to Personal Information in its day-to-day activities. Our Employees in particular, need to be able to trust us with the information they provide to us. The Company must, accordingly, respect and protect the integrity of the Personal Information it holds by, in particular, treating it with care and keeping it confidential.

5.2 The goal of this Policy is to ensure that Personal Information is processed and recorded in accordance with the provisions of the Act, whilst still enabling the Company to use the Personal Information for lawful and legitimate purposes in the furtherance of its business aims and objectives.

6 APPLICATION, COMMENCEMENT AND OBJECTIVES

6.1 Application

6.1.1 This Policy applies to the processing of all Personal Information by or on behalf of the Company, by all Employees, officials, agents, and representatives of the Company. The processing of Personal Information must comply with the provisions of this Policy read in conjunction with the Act.

6.1.2 This Policy prevails over all other policies of the Company pertaining to the processing of Personal Information. All persons involved in the processing and recording of Personal Information shall –

6.1.2.1 comply with the relevant provisions of the Act as read with this Policy;

6.1.2.2 interpret and apply this Policy congruently with any other policies of the Company to the extent that such congruency is possible; and

6.1.2.3 apply this Policy in preference to any other policies of the Company in the event that ambiguity and/or conflict and/or vagueness exists between this Policy and other policies of the Company.

6.1.3 The Company must, however, use its best endeavours to ensure that all other policies confirm and are aligned with the terms and conditions set out herein where relevant.

6.2 Commencement

This Policy shall come into effect on **21 May 2021**

6.3 **Objectives**

6.3.1 The objectives of this Policy are to ensure that the processing of Personal Information by the Company –

6.3.1.1 complies with all applicable legislation, including the Act; and

6.3.1.2 occurs in a manner that facilitates and enhances the ability of the Company to achieve its objectives but with due regard to safeguarding the interests of Data Subjects in relation to their Personal Information.

6.3.2 This Policy also strives to ensure that consistency is achieved and maintained in relation to the processing of Personal Information throughout the Company at all times.

7 OVERSIGHT AND RESPONSIBILITIES

7.1 **General**

7.1.1 The Board is generally responsible for the management oversight and control of the activities of the Company.

7.1.2 The management team is, however, responsible for day to day management.

7.1.3 The management team shall ensure that the terms and conditions set out in this Policy are observed at all times by introducing and maintaining the appropriate procedures and deploying the appropriate resources to achieve this.

7.2 **Information Officer and Deputy Information Officers**

7.2.1 The Information Officer for the Company is Jonathan Humphrey (HR Manager).

7.2.2 The following positions and the persons who hold such positions from time to time are designated Deputy Information Officers, namely –

7.2.2.1 Glenda Coetzer (Admin Manager)

The Information Officer will be deemed to have delegated, on a revocable basis, aspects of his/her authority to the Deputy Information Officers in respect of the following matters –

7.2.2.2 to provide general guidance on the processing and recording of Personal Information in accordance with this Policy as read with the Act;

7.2.2.3 to encourage the compliance by the Company as well as all Employees, with the conditions for the lawful processing of Personal Information;

7.2.2.4 dealing with requests made to the Company pursuant to the Act as well as this Policy;

7.2.2.5 working with the Regulator in respect of any investigations conducted pursuant to the Act in relation to the Company;

7.2.2.6 to otherwise ensure compliance by the Company, as well as all Employees, with the provisions of the Act and this Policy; and

7.2.2.7 to generally implement all processing activities in accordance with this Policy as read with the Act.

7.2.3 The Information Officer and Deputy Information Officers shall only be required to perform the functions contemplated in paragraph 0 upon being registered with the Regulator.

8 REPORTING

8.1 Information Officer's Report

8.1.1 The Information Officer shall submit a report on the implementation of this Policy to the management team on the request of the management team. Such report shall deal, *inter alia*, with –

8.1.1.1 the Company's compliance of the provisions of this Policy;

8.1.1.2 the implementation of relevant security safeguards for the protection of the Personal Information as contemplated in paragraph 14;

8.1.1.3 any security compromises in which there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by an unauthorised third party;

8.1.1.4 any complaints received in respect of the processing of Personal Information as well as any unauthorised use of the Personal Information of a Data Subject by anyone in the Company; and

8.1.1.5 any and all other matters as may be appropriate and/or necessary to be addressed in the report contemplated in this paragraph 8.1.

8.1.2 The Deputy Information Officers and/or the Information Administrators, in accordance with the provisions of paragraph 14.4, shall immediately report any compromises in the Company s' security safeguards in writing to the Information Officer, whereupon the Information Officer shall be obliged to immediately report same to the management team.

9 ETHICAL OBLIGATIONS AND STANDARDS

9.1 Employees shall be obliged to observe the following duties so as to act in the best interests of the Company and in due cognisance of the right to privacy of Data Subjects at all times during the processing of Personal Information and after the completion thereof –

9.1.1 Employees shall not exceed the powers conferred upon them in terms of the Act, this Policy and their respective employment agreements;

9.1.2 Employees shall not exercise their powers for an improper or collateral purpose by abusing their positions as employees or office bearers of the Company in order to derive personal or private benefit or advantage; and

9.1.3 Employees shall avoid a conflict between the interests of the Company and their personal or private interests or benefit.

9.2 In the event that an Employee breaches any terms or conditions of this Policy, the Company shall be entitled, without prejudice to any of its rights in terms of this Policy or at law, to take such action against such Employee in terms of the Disciplinary Code and Procedure which the Company may have in place or the relevant code of conduct or behaviour that applies to such Employee.

PART 2: PROCESSING AND RECORDING

10 GENERAL

10.1 Personal Information is defined by the Act as information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing, juristic person, including, but not limited to –

10.1.1 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;

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

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

10.1.4 the biometric information of the person;

10.1.5 the personal opinions, views or preferences of the person;

10.1.6 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;

10.1.7 the views or opinions of another individual about the person; and

10.1.8 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.

10.2 Subject to the provisions of the Act, Personal Information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address and telephone number and does not include information made lawfully available to the general public.

10.3 **Collection of Personal Information**

10.3.1 Subject to the provisions of paragraph 10.4 as read with the Act, Personal Information must be collected directly from the Data Subject. This includes all Personal Information required from all Employees and persons applying for such positions.

10.3.2 Any request (which will include, but not be limited to all application forms as well as other information requests, in whatsoever medium or format) to a Data Subject for Personal Information must be in writing and contain at least the following –

10.3.2.1 details pertaining to the Personal Information being collected and, where the Personal Information is not collected from the Data Subject, the source from which it is collected;

10.3.2.2 the name and address of the Company;

10.3.2.3 the purpose for which the Personal Information is being collected;

10.3.2.4 whether or not the supply of the Personal Information by that Data Subject is voluntary or mandatory;

10.3.2.5 the consequences of failure to provide the Personal Information;

10.3.2.6 any particular law authorising or requiring the collection of the Personal Information;

10.3.2.7 whether the Personal Information will or may be transferred to a third party residing outside of South Africa and the level of protection afforded to the Personal Information by that non-resident third party;

10.3.2.8 the recipient or category of recipients of the Personal Information;

10.3.2.9 the nature or category of the Personal Information;

10.3.2.10 the existence of the right of access to and the right to rectify the Personal Information collected;

10.3.2.11 the existence of the right to object to the processing of Personal Information; and

10.3.2.12 the existence of the right to lodge a complaint to the Regulator and the contact details of the Regulator.

10.4 Notwithstanding the provisions of paragraph 10.3.1, Personal Information need not be collected directly from the Data Subject in the event that –

10.4.1 the Personal Information is derived from a public record or has been deliberately made public by the Data Subject. A public record is defined in the Act as a Record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body. Examples of public records include deeds office records and CIPC records;

10.4.2 the Data Subject or, where the Data Subject is under the age of 18, his or her parent and/or guardian has consented to the collection of the Personal Information from another source;

10.4.3 the collection of Personal Information from another source would not prejudice a legitimate interest of the Data Subject;

10.4.4 the collection of the Personal Information from another source is necessary –

10.4.4.1 to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

10.4.4.2 to comply with an obligation imposed by law or enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, No 34 of 1997;

10.4.4.3 for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

10.4.4.4 in the interest of national security; or

10.4.4.5 to maintain the legitimate interests of the Company or of a third party to whom the information is supplied;

10.4.5 the collection would prejudice the lawful purpose thereof; or

10.4.6 it is not reasonably practical in the circumstances of the particular case.

10.5 **Requests for Personal Information**

Any person who receives a written request from a Data Subject to obtain a Record or description of the Personal Information held by the Company about the Data Subject, shall be required to –

10.5.1 obtain a certified copy of the proof of identification of that Data Subject; and

10.5.2 refer such request to the Information Officer who must deal with such request in the manner and form prescribed in terms of the Act, as well as PAIA**.**

10.6 **Correction of Personal Information**

10.6.1 A Data Subject is entitled to provide the Company with a written request to –

10.6.1.1 correct or delete the Personal Information about the Data Subject in the possession or control of the Company which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

10.6.1.2 destroy or delete a Record of Personal Information about the Data Subject that the Company is no longer authorised to retain.

10.6.2 Within 20 business days (or if this period is not reasonable, then such extended period as may be reasonable in the circumstances) of receipt of the written request contemplated in paragraph 10.6.1, the relevant person so designated by the Information Officer shall –

10.6.2.1 correct the Personal Information;

10.6.2.2 destroy or delete the Personal Information;

10.6.2.3 provide the Data Subject, subject to his or her satisfaction, with credible evidence in support of the Personal Information; or

10.6.2.4 where agreement cannot be reached between the Company and the Data Subject concerned, and if the Data Subject so requests, take such steps, as are reasonable in the circumstances, to attach to the Personal Information in such a manner that it will always be read with the Personal Information, an indication that a correction of the Personal Information has been requested but not been made.

10.6.3 In the event of the Information Officer having taken steps as contemplated in paragraphs 10.6.1 and 10.6.2, where such steps have resulted in a change to the Personal Information of the Data Subject, and where the changed Personal Information has an impact on decisions that have been or will be taken in respect of the Data Subject in question, the Information Officer must, if reasonably practicable, and within 10 business days (or if such period is not reasonable then such extended period as may be reasonable in the circumstances) of such amendment taking place, inform each person or body to whom the Personal Information has been disclosed of the steps taken.

11 PROCESSING OF PERSONAL INFORMATION

The Company has a general and overriding duty to ensure that, at the time of determining the purpose and means of processing of any Personal Information of a Data Subject, as well as during the processing of the aforesaid, the provisions contemplated in this paragraph 11 as read with the Act, are complied with.

11.1 Consent, Justification and Objection

11.1.1 For Personal Information to be lawfully processed by the Company, one of the following requirements must be complied with, namely that –

11.1.1.1 the Consent of the Data Subject to such processing must be obtained, or in the case of the Data Subject being under the age of 18, the parent and/or guardian of such Data Subject must provide his or her Consent to the processing;

11.1.1.2 the processing of the Personal Information is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party;

11.1.1.3 the processing complies with an obligation imposed by law on the Company;

11.1.1.4 the processing protects a legitimate interest of the Data Subject.

11.1.1.5 the processing is necessary for the proper performance of a public law duty by a public body; or

11.1.1.6 the processing is necessary for pursuing the legitimate interests of the Company or a third party to whom the Personal Information is supplied.

11.1.2 The Consent contemplated in paragraph 11.1.1.1 may be withdrawn by the Data Subject or, where relevant, the parent and/or guardian of the Data Subject, at any time. Such withdrawal shall be made in writing to the Information Officer.

11.1.3 The withdrawal of Consent as contemplated above shall not affect the lawfulness of the processing of the Personal Information either in terms of paragraphs 11.1.1.2 to 11.1.1.6 or which took place prior to the Company receiving notification of such withdrawal.

11.1.4 Except where such processing is required in terms of legislation, the Data Subject may, at any time, object to the processing of Personal Information in terms of paragraphs 11.1.1.2 to 11.1.1.6, on reasonable grounds relating to his or her particular situation. Such notice of objection is to be made in writing to the Information Officer. Where the Company receives notice of such objection as contemplated herein, the Company may no longer process the Personal Information of the objecting Data Subject.

11.2 **Further processing**

11.2.1 Further processing of Personal Information must be in accordance with the purpose for which the information was collected. Where this is not the case, the Consent of the Data Subject to such further processing must be obtained.

11.2.2 In assessing whether further processing is compatible with the purpose of collection, the Company shall take account of –

11.2.2.1 the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

11.2.2.2 the nature of the information concerned;

11.2.2.3 the consequences of the intended further processing for the Data Subject;

11.2.2.4 the manner in which the Personal Information has been collected; and

11.2.2.5 any contractual rights and obligations between the parties.

11.2.3 Notwithstanding the provisions of paragraph 11.2.1, in the event of –

11.2.3.1 the information being available in or derived from a public record or having deliberately been made public by the Data Subject;

11.2.3.2 the further processing being necessary: (i) to avoid prejudice to the maintenance of the law by any public body; (ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue; (iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or (iv) in the interests of national security;

11.2.3.3 the further processing being necessary to prevent or mitigate a serious and imminent threat to public health, public safety or the life or health of the Data Subject; or

11.2.3.4 the Personal Information being used for historical, statistical or research purposes and the Company ensures that the further processing is carried out solely for such purpose and will not be published in an identifiable form,

the further processing of such Personal Information may take place without the Consent of the Data Subject or his or her parent and/or guardian, where applicable.

11.3 **Restrictions**

11.3.1 Th Company shall be required to place restrictions on the processing of Personal Information in the event of –

11.3.1.1 the accuracy of the Personal Information being contested by the Data Subject, for a period to verify the accuracy of the information;

11.3.1.2 the Company no longer requiring the Personal Information for achieving the purpose for which it was collected or subsequently processed, but such information is being retained for purposes of proof;

11.3.1.3 the processing being unlawful and the Data Subject, opposing the destruction or deletion thereof, requesting for the restriction of the use of the Personal Information; or

11.3.1.4 the Data Subject requests to transmit the personal data into another automated processing system.

11.3.2 Where a restriction as contemplated in this paragraph 11.3 has been placed on the processing of the Personal Information of a Data Subject, such information may, with the exception of storage, only be processed for the purposes of proof, or with the Data Subject's Consent or, where relevant, the Consent of the Data Subject's parent and/or guardian, or for the protection of the rights of another natural or legal person, or where such processing is in the public interest.

11.3.3 Where the processing of Personal Information has been restricted as contemplated in this paragraph 11.3, the Company must inform the Data Subject before lifting the restriction.

12 RETENTION AND RECORD KEEPING

12.1 The Act requires that the Company only retains Records for as long as 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 authorised by law. In this regard the minimum retention schedule attached hereto sets out the various minimum retention periods for certain records prescribed by law;

12.1.2 the Company reasonably requires the Record for lawful purposes related to its function or activities;

12.1.3 retention of the Record is required by a contract between the parties thereto; or

12.1.4 the Data Subject, or his or her parent or legal guardian where relevant, has consented to the retention of the Record.

12.2 Personal Information collected in accordance with paragraph 10 shall be retained –

12.2.1 in the case of Employees for the duration of the Employee's employment and for a period of not more than **[10]** years thereafter, provided that in the case of information relating to any remuneration including benefits received by former Employees will, if this is in the interest of the former Employee, be retained for an indefinite period;

12.2.2 in the case of any other person including applicants for employment, for a period of **[1]** years after receipt of the Personal Information; or

12.2.3 until such Personal Information is superseded, in which case any obsolete Personal Information shall be destroyed.

12.3 After expiration of the periods contemplated in paragraph 12.1, the Company shall be required to destroy, delete or de-identify the Record of Personal Information as soon as reasonably possible thereafter provided that the Company will be entitled to retain Records of Personal Information for periods in excess of those contemplated in paragraph 12.2 above for historical, statistical or research purposes provided that the Company has established appropriate safeguards against the records being used for any other purpose.

13 SPECIAL PERSONAL INFORMATION

No person shall be entitled to process the Special Personal Information of a Data Subject, unless –

13.1 the Data Subject has provided his or her Consent to the processing of such information;

13.2 processing is necessary for the establishment, exercise or defence of a right or obligation in law;

13.3 processing is for historical, statistical or research purposes to the extent that –

13.3.1 the purpose serves a public interest and the processing is necessary for the purpose concerned;

13.3.2 it appears to be impossible or would involve a disproportionate effort to ask for Consent;

and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;

13.3.3 information has deliberately been made public by the Data Subject; or

13.3.4 the necessary authorisations have been complied with.

PART 3: INFORMATION SECURITY SUPERVISION

14 IMPLEMENTATION OF SECURITY SAFETYGUARDS

14.1 **General**

14.1.1 The Company strives to ensure the security, integrity and privacy of personal information submitted. The Company will review and update its security measures in accordance with future legislation and technological advances. Unfortunately, no data transmission can be guaranteed to be totally secure, however, the Company will endeavour to take all reasonable steps to protect the Personal Information collected.

14.1.2 The Company 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 –

14.1.2.1 loss of, damage to or unauthorised destruction of Personal Information; and

14.1.2.2 unlawful access to or processing of Personal Information.

14.1.3 The Company has done and will from time to time ensure that it takes reasonable steps to –

14.1.3.1 identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

14.1.3.2 establish and maintain appropriate safeguards against the risks identified;

14.1.3.3 regularly verify that the safeguards are effectively implemented; and

14.1.3.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

14.1.4 In implementing the above measures, the Company will have due regard to generally accepted information security practices and procedures which may apply to it generally.

14.2 **Information Security**

14.2.1 The Company is committed to ensuring information security and in particular ensure that the incidence of unauthorised access to or transmission of Personal Information is minimised.

14.2.2 The following measures have or will be introduced by the Company and must, where relevant be adhered to –

14.2.2.1 all documents containing Personal Information must be securely stored and access thereto controlled in an appropriate manner. No documentation containing Personal

Information must be left unattended or unsecured or otherwise in plain sight or otherwise in an environment with ease of access;

14.2.2.2 all computers and other electronic devices including particularly mobile devices which are capable of storing or accessing data must be secured with passwords which are to be updated on a regular basis;

14.2.2.3 [as far as possible and unless there is good reason not to do so, all information and particularly Personal Information must be loaded onto and accessed from the Company central information systems and not be housed or stored on local devices including computers and other electronic devices; and]

14.2.2.4 [data transmission, such as sending and receiving messages like e-mails must be conducted by the relevant Company information systems provided if this involves the transmission of Personal Information as these systems and transmission are encrypted. No non-Company assigned e-mail addresses may be used to transmit any Personal Information.]

14.3 **Information processed by Operators**

14.3.1 An Operator or anyone processing Personal Information on behalf of the Company must –

14.3.1.1 process such information only with the knowledge or authorisation of the Company; and

14.3.1.2 treat Personal Information which comes to their knowledge as confidential and must not disclose it,

unless required by law or in the course of the proper performance of their duties.

14.3.2 The Company shall always ensure that, in terms of a written contract between the Company and the Operator, the Operator which processes Personal Information for the Company establishes and maintains the security measures referred to in paragraph 14.1.

14.3.3 The Operator must notify the Company immediately where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person.

14.3.4 Notwithstanding anything to the contrary herein contained, under no circumstances must any Operator be allowed to process any Personal Information unless there is a written contract signed by both parties which deals comprehensively with the matters contemplated in this Policy.

14.4 **Security Compromises**

14.4.1 In the event of there being reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by an unauthorised person and accordingly, resulting in a compromise of the security safeguards of the Company , the Information Officer upon, notification of such compromise as contemplated in paragraph 8.1.2, shall immediately upon receipt of such notification report same to]the[management body].

14.4.2 The Information Officer shall be required to notify both the Regulator and the Data Subject concerned within 5 business days of the management team being informed of the compromise as contemplated in paragraph 14.4.1.

14.4.3 The notification to the Data Subject must be in writing and must either –

14.4.3.1 be mailed to the Data Subject's last known physical or postal address; or

14.4.3.2 be sent by email to the Data Subject's last known email address; or

14.4.3.3 be placed in a prominent position on the website of the Company; or

14.4.3.4 be published in the news media; or

14.4.3.5 as directed by the Regulator.

14.4.4 The notification contemplated in paragraph 14.4.2 must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including –

14.4.4.1 a description of the possible consequences of the security compromise;

14.4.4.2 a description of the measures that the Company intends to take or has taken to address the security compromise;

14.4.4.3 a recommendation with regard to the measures to be taken by the Data Subject to mitigate the possible adverse effects of the security compromise; and

14.4.4.4 if known to the Company, the identity of the unauthorised third party who may have accessed or acquired the Personal Information.

15 REGULATOR

15.1 The Regulator is a juristic person established in terms of section 39 of the Act. The power, duties and functions of the Regulator are –

15.1.1 to provide education by –

15.1.1.1 promoting an understanding and acceptance of the conditions for the lawful processing of Personal Information and of the objects of those conditions;

15.1.1.2 undertaking education programmes, for the purpose of promoting the protection of Personal Information, on the Regulator's own behalf or in co-operation with other persons or authorities acting on behalf of the Regulator;

15.1.1.3 making public statements in relation to any matter affecting the protection of the Personal Information of a Data Subject or of any class of Data Subjects;

15.1.1.4 giving advice to Data Subjects in the exercise of their rights; and

15.1.1.5 providing advice, upon request or on its own initiative, to a Minister or a public or private body on their obligations under the provisions, and generally on any matter relevant to the operation, of the Act;

15.1.2 to monitor and enforce compliance by –

15.1.2.1 public and private bodies with the provisions of the Act;

15.1.2.2 undertaking research into, and monitoring developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the Personal Information of Data Subjects are minimised, and reporting to the Minister the results of such research and monitoring;

15.1.2.3 examining any proposed legislation, including subordinate legislation, or proposed policy of the Government that the Regulator considers may affect the protection of the Personal Information of Data Subjects, and reporting to the Minister the results of that examination;

15.1.2.4 reporting upon request or on its own accord, to Parliament from time to time on any policy matter affecting the protection of the Personal Information of a Data Subject, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the Personal Information of a Data Subject;

15.1.2.5 submitting a report to Parliament, within 5 months of the end of its financial year, on all its activities in terms of this Act during that financial year;

15.1.2.6 conducting an assessment, on its own initiative or when requested to do so, of a public or private body, in respect of the processing of Personal Information by that body for the purpose of ascertaining whether or not the information is processed according to the conditions for the lawful processing of Personal Information;

15.1.2.7 monitoring the use of unique identifiers of Data Subjects, and reporting to Parliament from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the Personal Information of a Data Subject;

15.1.2.8 maintaining, publishing and making available and providing copies of such registers as are prescribed in this Act;

15.1.3 examine any proposed legislation that makes provision for the –

15.1.3.1 collection of Personal Information by any public or private body; or

15.1.3.2 disclosure of Personal Information by one public or private body to any other public or private body, or both, to have particular regard, in the course of that examination, to the matters set out in section 44(2), in any case where the Regulator considers that the information might be used for the purposes of an information matching programme;

15.1.4 report to the Minister and Parliament the results of that examination;

15.1.5 to consult with interested parties by –

15.1.5.1 receiving and inviting representations from members of the public on any matter affecting the Personal Information of a Data Subject;

15.1.5.2 co-operating on a national and international basis with other persons and bodies concerned with the protection of Personal Information; and

15.1.5.3 acting as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of the protection of the Personal Information of a Data Subject;

15.1.6 to handle complaints by –

15.1.6.1 receiving and investigating complaints about alleged violations of the protection of Personal Information of Data Subjects and reporting to complainants in respect of such complaints;

15.1.6.2 gathering such information as in the Regulator's opinion will assist the Regulator in discharging the duties and carrying out the Regulator's functions under the Act;

15.1.6.3 attempting to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation; and

15.1.6.4 serving any notices in terms of the Act and further promoting the resolution of disputes in accordance with the prescripts of the Act;

15.1.7 to conduct research and to report to Parliament –

15.1.7.1 from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the Personal Information of a Data Subject; and

15.1.7.2 on any other matter, including necessary legislative amendments, relating to protection of Personal Information that, in the Regulator's opinion, should be drawn to Parliament's attention;

15.1.8 in respect of codes of conduct to –

15.1.8.1 issue, from time to time, codes of conduct, amend codes and to revoke codes of conduct;

15.1.8.2 make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct; and

15.1.8.3 consider afresh, upon application, determinations by adjudicators under approved codes of conduct;

15.1.8.4 to facilitate cross-border co-operation in the enforcement of privacy laws by participating in any initiative that is aimed as such co-operation; and

15.1.9 in general to –

15.1.9.1 do anything incidental or conducive to the performance of any of the preceding functions;

15.1.9.2 exercise and perform such other functions, powers and duties as are conferred or imposed on the Regulator by or under the Act or any other legislation;

15.1.9.3 require the responsible party to disclose to any person affected by a compromise to the integrity or confidentiality of Personal Information, such compromise in accordance with section 22; and

15.1.9.4 exercise the powers conferred upon the Regulator by the Act in matters relating to the access of information as provided by PAIA.

15.2 The contact details of the Regulator may be obtained from the Information Officer during normal working hours.

PART 4: IMPLEMENTATION AND AMENDMENTS

16 DELEGATIONS

No decision making contemplated in this Policy may be delegated to an advisor or consultant of the Company.

17 AMENDMENTS TO POLICY

17.1 No additions, amendments or deviations from this Policy shall be valid unless approved by the management team.

17.2 Changes or suggestions to amend the Policy shall be done in writing stating the rationale and, where possible, proposed recommendations to amend the Policy. Such recommendations shall be submitted to the Information Officer.

17.3 When deemed necessary in the opinion of the Information Officer and after giving due consideration to the merits and de-merits of the proposals to amend this Policy, the Information Officer shall, where appropriate, submit such recommendations to the management team for its decision. The management team shall thereupon be empowered to accept the proposal or alternatively, accept the proposal subject to conditions that the management team may impose or alternatively, reject the proposal. In making its decision, the management team shall be required to take into consideration the provisions of the Act together with any amendments thereto.

17.4 Where any provision of the Act has been amended, the management team shall be required to convene a meeting to determine whether the aforesaid amendments have an impact on the Policy. Where it is decided that the amendment to the Act has an impact on the Policy, the management team shall be required to amend the Policy to align it with the provisions of the Act as well as the amendments thereto.

18 COMMUNICATION WITH THE COMPANY

18.1 All correspondence about this Policy or any matter arising from or related to the implementation of this Policy, shall be addressed to the Information Officer.

18.2 The Information Officer shall be obliged to inform the management team of any matters of significance in relation to the implementation or otherwise of this Policy.

19 COMBATING ABUSE OF THE POLICY

19.1 The Information Officer shall take all reasonable steps to prevent the abuse of the provisions of this Policy and when justified shall –

19.1.1 take appropriate steps against such person, provided that such steps shall at all times comply with the relevant laws and processes of the Company; or

19.1.2 in consultation with the management team may issue a complaint to the Regulator in the manner prescribed by the Act.

19.2 The Information Officer shall inform the management team of any actions taken in terms of this paragraph 19.

POL 5.2-016 BSC (POPIA & PAIA)

	NAME	DESIGNATION	SIGNATURE	DATE
COMPILED BY:	**J HUMPHREY**	**HR MANAGER**		**2 JUNE 2021**
REVIEWED BY:	**T V D MERWE**	**FINANCIAL MANAGER**		**2 JUNE 2021**
APPROVED BY:	**D MORGAN**	**C.E.O**		**2 JUNE 2021**

END.